TSUKUBA J. MATH.
Vol. 15 No. 1 (1991), 185—192

A REMARK ON ARTIN-SCHREIER CURVES WHOSE HASSE-WITT MAPS ARE THE ZERO MAPS

By

Susumu IROKAWA and Ryuji SASAKI

1. Introduction

Let X be a complete non-singular algebraic curve over an algebraically closed field k of positive characteristic p. Let $F:\mathcal{O}_X\rightarrow\mathcal{O}_X$ be the Frobenius homomorphism $F(\alpha)=\alpha^{p}$, and denote the induced p-linear map $H^{1}(X, \mathcal{O}_X)\rightarrow H^{1}(X, \mathcal{O}_X)$ again by F, which is called the Hasse-Witt map. The dimension of the semi-simple subspace $H^{1}(X, \mathcal{O}_X)_s$ of $H^{1}(X, \mathcal{O}_X)$ is denoted by $\sigma(X)$ and called the p-rank of a curve X, which is equal to the p-rank of the Jacobian variety of X.

Let $\pi: X\rightarrow Y$ be a p-cyclic covering of complete non-singular curves over k. Then the Deuring-Šafarevič formula is the following:

$$\sigma(X)-1+r=p(\sigma(Y)-1+r) \tag{1.1}$$

where r is the number of the ramification points with respect to π (see Subrao [10], Deuring [3], Šafarevič [8]).

An algebraic curve X, which is not birationally equivalent to $\boldsymbol{P}^{1}$, is called an Artin-Schreier curve if there is a p-cyclic covering $\pi: X\rightarrow\boldsymbol{P}^{1}$. Then the p-rank $\sigma(X)$ of X is immediately known by the above formula, however the rank of the Hasse-Witt map is not known. In this article, we shall prove the following.

THEOREM. *Let X be an Artin-Schreier curve defined over an algebraically closed field k, of positive characteristic p. Then the Hasse-Witt map of X is the zero map if and only if X is birationally equivalent to the complete non-singular algeraic curve defined by the equation*

$$y^{p}-y=x^{l}$$

for some divisor l ($l\geqq 2$) of $p+1$.

The Jacobian variety of a curve X is isomorphic to the product of supersingular ellitic curves if and only if the Cartier operator is the zero map

Received March 1, 1990. Revised May 8, 1990.

(Nygaard [7]). Since the Cartier operator is the transpose of the Hasse-Witt map, our theorem gives the Artin-Schreier curves whose Jacobian variety is isomorphic to the product of super-singular elliptic curves.

2. Basic for $H^0(X, \Omega_X)$

Let X be an Artin-Schreier curve, hence there is a p-cyclic coverning $\pi: X \to \boldsymbol{P}^1$. Let $\mathbf{k}(X)$ and $\mathbf{k}(\boldsymbol{P}^1)$ denote the function fields, and we regard $\mathbf{k}(\boldsymbol{P}^1)$ as contained in $\mathbf{k}(X)$. The fields $\mathbf{k}(X)$ and $\mathbf{k}(\boldsymbol{P}^1)$ can be expressed in the following:

$$\mathbf{k}(X)=k(x, y) \quad \text{and} \quad \mathbf{k}(\boldsymbol{P}^1)=k(x)$$

where

$$y^p-y=f(x), \qquad f(x)\in k(x).$$

Moreover, we can assume that $f(x)$ satisfies the following conditions:

$$f(x)=\frac{G(x)}{(x-\alpha_1)^{e_1}\cdots(x-\alpha_n)^{e_n}} \tag{2.1}$$

where

(1) $G(x)$ is a polynomial in $k[x]$,

(2) e_i's are positive integers prime to p,

(3) $\alpha_i\neq\alpha_j$ if $i\neq j$ and $G(\alpha_i)\neq 0$ for $i=1, \cdots, n$,

(4) $\deg G(x)-(e_1+\cdots+e_n)=e_0$ is a positive integer relatively prime to p.

Then the points of $\boldsymbol{P}^1$ which ramify in $\pi: X\to\boldsymbol{P}^1$ are exactly $\{\alpha_1, \cdots, \alpha_n, \infty\}$. If we denote by $P_1, \cdots, P_n$ and P_0 the points in X lying over $\alpha_1, \cdots, \alpha_n$ and ∞, then the divisor of the differential dx on X is given by

$$\operatorname{div}(dx)=\sum_{i=1}^{n}(e_i+1)(p-1)P_i-(2p-(e_0+1)(p-1))P_0. \tag{2.2}$$

Hence the genus $g(X)$ of X is given by the formula

$$2g(X)-2=\deg(\operatorname{div}(dx))=\sum_{i=1}^{n}(e_i+1)(p-1)-2p. \tag{2.3}$$

In the sequel, for a real number, a, we denote by $[a]$ the largest integer not exceeding a. Further we denote by $|S|$ the cardinality of a finite set S.

We define finite sets of differentials;

$$H_0=\{y^r x^b dx \mid (e_0+1)(p-1)-re_0-(b+2)p\geqq 0,$$
$$0\leqq b\leqq e_0-2,\ 0\leqq r\leqq p-1\}$$

and for each $i=1, \cdots, n$,

$$H_i=\left\{\frac{y^r dx}{(x-\alpha_i)^a} \mid (e_i+1)(p-1)-re_i-ap\geqq 0,\ 1\leqq a\leqq e_i,\ 0\leqq r\leqq p-2\right\}.$$

Then we have the following;

LEMMA.

1) $|H_0|=\frac{1}{2}(e_0-1)(p-1)$

2) $|H_i|=\frac{1}{2}(e_i+1)(p-1)$

3) $|H_0|+|H_1|+\cdots+|H_n|=g(X)$

4) $\bigcup_{i=1}^{n} H_i$ *forms a basis for* $H^0(X, \Omega_X)$.

PROOF. By the conditions defining the set $|H_0|$, we have

$$\frac{(e_0-b-1)p-1}{e_0}-1\geqq r\geqq 0\,. \tag{2.4}$$

For each b with $0\leqq b\leqq e_0-2$, the number of r satisfying (2.4) is given by

$$\varphi(b)=\left[\frac{(b_0-e-1)p-1}{e_0}\right].$$

Hence we have

$$|H_0|=\sum_{b=0}^{e_0-2}\varphi(b)=\sum_{b=0}^{e_0-2}\left[\frac{(e_0-b-1)p-1}{e_0}\right].$$

Since $(p, e_0)=1$, the set $\{(e_0-1)p, (e_0-2)p, \cdots, 1\cdot p, 0\}$ gives a complete set of representatives of $\boldsymbol{Z}$ modulo $e_0\boldsymbol{Z}$, hence so does $\{(e_0-1)p-1, (e_0-2)p-1, \cdots, 1\cdot p-1, 0-1\}$. Therefore we have

$$\begin{aligned}\frac{0}{e_0}+\frac{1}{e_0}+\cdots+\frac{e_0-2}{e_0}&=\sum_{b=0}^{e_0-2}\left\{\frac{(e_0-b-1)p-1}{e_0}-\left[\frac{(e_0-b-1)p-1}{e_0}\right]\right\}\\&=(e_0-1)\frac{(e_0-1)p-1}{e_0}-\frac{p}{e_0}\sum_{b=0}^{e_0-2}b-|H_0|.\end{aligned}$$

It follows that

$$\begin{aligned}|H_0|&=(e_0-1)\frac{(e_0-1)p-1}{e_0}-\frac{(p+1)(e_0-1)(e_0-2)}{2e_0}\\&=\frac{1}{2e_0}(e_0-1)\{2(e_0-1)p-2-(p+1)(e_0-2)\}\\&=\frac{1}{2}(e_0-1)(p-1)\,.\end{aligned}$$

This completes the proof of 1).

As the equality in 2) is proved in the same way, we shall omit its proof. 3) is a direct consequence of 1), 2) and (2.3).

As is easily seen, the divisors of the rational functions x, y and $x-\alpha_i$ on X, are given by

$$\operatorname{div}(x)=(x)_0-pP_0\,,$$

$$\operatorname{div}(y)=(y)_0-\sum_{i=0}^{n} e_iP_i\,,$$

$$\operatorname{div}(x-\alpha_i)=p(P_i-P_0)\,,$$

where $(x)_0$ and $(y)_0$ are the divisors of zeros of x and y, respectively. It follows that

$$\operatorname{div}\left(\frac{y^r dx}{(x-\alpha_i)^a}\right)=r(y)_0+\sum_{i=1}^{n}\{(e_i+1)(p-1)-re_i-ap\}P_i$$
$$+\{(e_0+1)(p-1)-re_0+(a-2)p\}P_0$$

and

$$\operatorname{div}(y^r x^b dx)=r(y)_0+b(x)_0+\sum_{i=1}^{n}\{(e_i+1)(p-1)-re_i\}P_i$$
$$+\{(e_0+1)(p-1)-re_0-(b+2)p\}P_0\,.$$

Thus we see that every element in H_i $(0\leqq i\leqq n)$ is a holomorphic 1-form. The elements in $\bigcup_{i=0}^{n} H_i$ are linearly independent over k, since otherwise $[k(x, y): k(x)]$ would be smaller than p. Thus, by 3), we get 4).

3. Proof of the theorem

We adopt the same notation as before. Let $C: H^0(X, \Omega_X)\to H^0(X, \Omega_X)$ be the Cartier operator of X. (For the definition and properties of C, we refer to Cartier [1], [2] and Seshadri [9].) Then it satisfies

$$C((f_0{}^p+f_1{}^p x+\cdots+f_{p-1}{}^p x^{p-1})dx)=f_{p-1}dx\,, \tag{3.1}$$

because x is a separable element of $k(x, y)$ over k and any element f in $k(x, y)$ can be uniquely written in the form

$$f=f_0{}^p+f_1{}^p x+\cdots+f_{p-1}{}^p x^{p-1}\,.$$

Since the Cartier operator is the transpose of the Hasse-Witt map $F: H^1(X, \mathcal{O}_X)\to H^1(X, \mathcal{O}_X)$, it suffices to determine Artin-Schreier curves whose Cartier operator is the zero map.

Now we shall prove the "if" part. Let X be the curve defined by

$$y^p-y=x^l$$

where l is a divisor of $p+1$ and $l \geqq 2$. By the Lemma in the section 2, we can write a basis for $H^0(X, \Omega_X)$ in the following way;

$$dx,\ xdx,\ \cdots,\ x^{s_0}dx\,,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$y^r dx,\ y^r xdx,\ \cdots,\ y^r x^{s_r}dx\,,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

where $0 \leqq r \leqq p-(r+1)/l-1$ and $s_r=[l-1-((r+1)l+1)/p]$. Then we have

$$l-2 \geqq s_0 \geqq s_1 \geqq \cdots .$$

Since $y^r=(y^p-x^l)^r$, we have

$$C(y^r x^b dx)=C\Big(\sum_{k=0}^{r}\binom{r}{h} y^{p(r-h)}(-x^l)^k x^b\, dx\Big)$$
$$=\sum_{h=0}^{r}\binom{r}{h}^{1/p}(-1)^{h/p}y^{r-h}C(x^{lh+b}dx),$$

where $\binom{r}{h}$ is the binomial coefficient. To prove that C is the zero map, it is sufficient to show

$$C(x^{lh+b}dx)=0$$

for all r, b and h satisfying

$$0 \leqq r \leqq p-1, \quad 0 \leqq h \leqq r \quad \text{and} \quad 0 \leqq b \leqq s_r\,.$$

By (3.1), $C(x^{lh+b}dx) \neq 0$ if and only if $lh+b \equiv -1 \pmod p$. Suppose there exist h and b satisfying

$$0 \leqq h \leqq r \leqq p-1, \qquad 0 \leqq b \leqq s_r$$

and

$$lh+b=ip-1$$

for some $i>0$. Let $p+1=lm$. Then we have

$$lh+b=i(lm-1)-1=ilm-i-1<ilm$$

and

$$i=\frac{lh+b+1}{p} \leqq \frac{l(p-1)+l-1}{p}<l\,.$$

hence

$$h \leqq im-1 \quad \text{and} \quad i \leqq l-1\,. \tag{3.2}$$

If $h=im-t$, $t \geqq 1$, then $r \geqq im-t=h$; hence

$$b=lt-i-1\leqq s_r\leqq s_{im-1}$$
$$=\left[l-1-\frac{(im-t+1)l+1}{p}\right]\leqq l-2\,.$$

By (3.2), we have $t=1$. Then,

$$lh+b\leqq(im-1)l+s_{im-1}$$
$$=(im-1)l+\left[l-1-\frac{iml+1}{p}\right]$$
$$\leqq(im-1)l+l-i-2=iml-i-2$$
$$<iml-i-1=ip-1\,.$$

This is a contradiction. Thus we have $C(x^{lh+b}dx)=0$.

Next we shall prove the "only if" part. Let X be an Artin-Schreier curve whose Hasse-Witt map is the zero map; hence the p-rank $\sigma(X)$ is zero. Then by (1.1), we see that X is defined by an equation

$$y^p-y=f(x)\,,$$

where

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\,,\qquad \text{for } n\geqq 2 \text{ and } (n,\,p)=1\,.$$

As above,

$$H_0=\{y^r x^b dx\,|\,(e_0+1)(p-1)-re_0-(b+2)p\geqq 0\,,$$
$$0\leqq b\leqq e_0-2,\ 0\leqq r\leqq p-1\}$$

forms a basis for $H^0(X,\,\Omega_X)$. Since

$$C(y^r x^b dx)=C((y^p-f)^r x^b dx)$$
$$=\sum_{h=0}^{r}\binom{r}{h}^{1/p}(-1)^{h/p}y^{r-h}C(f^h x^b dx)\,,$$

we have

$$C(f^h x^b dx)=0 \tag{3.3}$$

for all h, r and b satisfying $0\leqq h\leqq r\leqq p-1$, $0\leqq b\leqq n-2$ and

$$(n+1)(p-1)-(b+2)p-rn\geqq 0\,. \tag{3.4}$$

By (3.3) with $r=0$, we have

$$C(dx)=C(xdx)=\cdots=C(x^{s_0}dx)=0$$

where $s_0=[n-1-(n+1)/p]$. Since $C(x^{p-1}dx)=dx$, we must have $[n-1-(n+1)/p]\leqq p-2$. It follows that $n\leqq p+1$ noticing that $(p,\,n)=1$. Assume $n\leqq p$; hence $n\leqq p-1$. Then there exists $l\geqq 1$ such that

$$ln+1 \leqq p < (l+1)n+1 .$$

Again by $(p, n)=1$, we have

$$ln+1 \leqq p \leqq (l+1)n-1 . \tag{3.5}$$

Therefore we have

$$\deg(f^l)=ln ,$$
$$\cdots\cdots\cdots\cdots ,$$
$$\deg(f^l x^{s_l})=ln+\left[n-1-\frac{(l+1)n+1}{p}\right]=(l+1)n-3 .$$

Suppose $p-1=ln+b$, $0 \leqq b \leqq s_l$. Then we have $f^l x^b = x^{p-1}+g(x)$ where $g(x)$ is polynomial in $k[x]$ of degree $\leqq p-2$; hence we have

$$C(f^l x^b dx)=dx .$$

This contradicts to (3.3). Therefore we have

$$p-1 \geqq ln+s_l+1=ln+n-2 . \tag{3.6}$$

By (3.5) and (3.6), we have

$$p-1=(l+1)n-2 , \qquad i.e.\ p+1=(l+1)n .$$

Thus in any case we have

$$p+1=ln \tag{3.7}$$

for some $l \geqq 1$. Since $(n, p)=1$, we can write

$$f=x^n+a_i x^i+\cdots+a_0$$

with $i \leqq n-2$ and

$$f^l=x^{ln}+la_i x^{i+(l-1)n}+\cdots+a_0{}^l . \tag{3.8}$$

(1) Assume $n \geqq 3$ and $l \geqq 2$. If $1 \leqq i \leqq n-2$, then

$$0 \leqq n-i-2 \leqq n-3=s_l=\left[n-1-\frac{(l+1)n+1}{p}\right]$$

and

$$i+(l-1)n+n-i-2=ln-2=p-1 .$$

By (3.3), we have

$$C(f^l x^{n-i-2} dx)=(la_i)^{1/p} dx=0 .$$

Hence f must be of the form

$$f(x)=x^n+a_0 .$$

(2) Assume $n \geqq 4$ and $l=1$. If $2 \leqq i \leqq n-2$, then

$$0 \leqq n-i-2 \leqq n-4=s_l=\left[n-1-\frac{2n+1}{p}\right]$$

and

$$i+n-i-2=n-2=p-1\,.$$

By the same reason as above, we have

$$f(x)=x^n+a_l x+a_0\,.$$

(3) If $n=2$, then we have

$$f(x)=x^2+a_0\,.$$

(4) If $n=3$ and $l=1$, then we have $p=2$ and

$$f(x)=x^3+a_1 x+a_0\,.$$

On the other hand, the curves defined by

$$y^p-y=x^{p+1}+ax+b\,,\qquad (a,b\in k)\,,$$

are isomorphic to each other and all the curves defined by

$$y^p-y=x^n+a\,,\qquad (a\in k)\,,$$

are isomorphic to each other. This completes the proof.

References

[1] P. Cartier, Questions de rationalite des diviseurs én géometrie algbrique, Bull. Soc. math. France **86** (1958), 177-251.

[2] P. Cartier, Une nouvelle opération sur les formes differntials, Compt. Rend. Paris **244** (1957), 426-428.

[3] M. Deuring, Automorphismen und Divisorenklassen der Ordnung 1 in algebraischen Funktionenkörpern, Math. Ann. **113** (1936), 208-215.

[4] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionen-Körper, insbesondere bei endlichem Könstantenkörper, J. reine angrew. Math. **172** (1935), 37-54.

[5] H. Hasse and E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p, Mh. Math. Phys. **43** (1936), 477-492.

[6] M.L. Madan, On a theorem of M. Deuring and I.R. Šafarevič, Manuscripta math. **23** (1977), 91-102.

[7] N.O. Nygaard, Slopes of powers of frobenius on crystalline cohomology, Ann. Sci. Ecole Norm. Sup. **14** (1981), 369-401.

[8] I.R. Šafarevič, On p-extensions, Amer. Math. Soc. Trans. Series II vol. **4** (1954), 59-71.

[9] C.J. Seshadri, L'operation de Cartier. Applications, in "Séminaire C. Chevalley, E.N.S. 1958/59", Secrétariat Math. Paris 1960.

[10] D. Subrao, The p-rank of Artin-Schreier curves, Manuscripta math. **16** (1975), 169-193.

Susumu Irokawa
Institute of Mathematics
University of Tsukuba
Ibaraki 305
Japan

Ryuji Sasaki
Department of Mathematics
College of Science and Technology,
Nihon University
Kanda, Tokyo 101
Japan