TOKYO J. MATH.
VOL. 34, NO. 2, 2011

On the Deuring-Shafarevich Formula

Daisuke SHIOMI

Nagoya University

(Communicated by M. Kurihara)

Abstract. In this paper, we will give a new proof of the Deuring-Shafarevich formula, which asserts a relation between the p-ranks of Jacobi varieties. We analyze the zeta functions of global function fields to prove the formula, without using tools of the algebraic geometry.

1. Introduction

Let K be a function field with one variable over a field F of characteristic $p > 0$. Let g_K be the genus of K. Fix an algebraic closure $\bar{F}$ of F. It is known that the p-primary subgroup of Jacobian of $K\bar{F}$ is isomorphic to the direct sum of λ_K copies of $\mathbf{Q}_p/\mathbf{Z}_p$, where $0 \leq \lambda_K \leq g_K$. The integer λ_K is called the Hasse-Witt invariant of K. The following relation for Hasse-Witt invariants is called the Deuring-Shafarevich formula.

THEOREM 1.1. *Let K be a function field with one variable over an algebraic closure F of characteristic $p > 0$. Let L/K be a cyclic extension of degree p. Then,*

$$\lambda_L - 1 = p(\lambda_K - 1) + i_{L/K}(p-1)\,, \tag{1}$$

where $i_{L/K}$ is the number of primes of K ramifying in L/K.

The above formula was first stated by Deuring [De] when $i_{L/K} \geq 1$. However, his proof contained some mistakes. In 1954, by studying the rank of Hasse-Witt matrix, Shafarevich [Sha] proved the formula in the case of $i_{L/K} = 0$. Subrao [Su] finally gave a complete proof by using Artin-Schreier curves. Up to now, several proofs have been given (cf. [Cr], [Ma]).

In this paper, we will give a new proof of the Deuring-Shafarevich formula when F is a finite field. We analyze the zeta functions of global function fields to prove the formula, without using tools of the algebraic geometry. Let K be a global function field over a finite field $\mathbf{F}_q$ of characteristic $p > 0$. Then we will show the following formula.

Received February 26, 2010; revised Janurary 26, 2011
2010 *Mathematics Subject Classification*: 14H40, 11M38

THEOREM 1.2. *Let L/K be a geometric cyclic extension of degree p. Let λ_L and λ_K be Hasse-Witt invariants of L and K, respectively. Let S_K be the set of all primes of K. Then*

$$\lambda_L - 1 = p(\lambda_K - 1) + \sum_{P \in S_K} (e_P - 1) \deg_K P \,, \tag{2}$$

where e_P is the ramification index of P in L/K, and $\deg_K P$ is the degree of P.

We shall call a function field K supersingular if $\lambda_K = 0$ (Note that some authors use the word "supersingular" in a different sense.). This means that the Jacobian of $K\bar{\mathbf{F}}_q$ has no p-torsion points, where $\bar{\mathbf{F}}_q$ is an algebraic closure of $\mathbf{F}_q$. As an application of the above formula, we will construct an infinite family of supersingular function fields (see Proposition 4.1).

REMARK 1.1. By a standard argument of specialization, we can deduce Theorem 1.1 from Theorem 1.2 (cf. [K-M], [Suw]). We give a sketch of the proof.

1. Let $\pi : Y \to X$ be a cyclic covering of degree p of smooth projective curves over an algebraic closed field k of characteristic p. Then there are sub $\mathbf{F}_p$-algebra A of k of finite type, and a cyclic covering $\Pi : \mathcal{Y} \to \mathcal{X}$ of degree p of smooth projective curves over A such that $\Pi \otimes_A k = \pi$.
2. There is a non-empty open subset U of Spec$A$ such that for each geometric point s of U, the p-ranks of Jacobian of $\mathcal{Y}_s$ and $\mathcal{X}_s$ equal to those of Y and X, respectively.
3. On the other hand, by applying the semi-continuity theorem for the sheaf $\Omega_{\mathcal{Y}/\mathcal{X}}$ of relative differential of $\mathcal{Y}/\mathcal{X}$, we can take a non-empty open subset V such that for each geometric point s of V, the ramification data of $\mathcal{Y}_s/\mathcal{X}_s$ equals to that of Y/X.

It follows that Theorem 1.2 leads Theorem 1.1.

2. Preparation

Let K be a global function field over a finite field $\mathbf{F}_q$. The zeta function of K is defined as

$$\zeta(s, K) = \prod_{P:\text{prime}} \left(1 - \frac{1}{NP^s}\right)^{-1},$$

where P runs through all primes of K, and NP is the number of elements of the residue class field of P. Let g_K be the genus of K. Then there is a polynomial $Z_K(X)$ with integral coefficients of degree $2g_K$, satisfying

$$\zeta(s, K) = \frac{Z_K(q^{-s})}{(1 - q^{1-s})(1 - q^{-s})}.$$

Since we see that $Z_K(0) = 1$, we have

$$Z_K(X) = \prod_{i=1}^{2g_K} (1 - \pi_{i,K} X)$$

where $\pi_{i,K}$ is an algebraic integer. Let $\bar{Z}_K(X) \in \mathbf{F}_p[X]$ be the reduction of $Z_K(X)$ modulo p. It is well-known that

$$\lambda_K = \deg \bar{Z}_K(X) \tag{3}$$

(see [Ro] Proposition 11.20). In particular, $\bar{Z}_K(X) = 1$ if and only if K is supersingular.

Let $\mathbf{Q}_p$ denote the p-adic field. Fix an algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$, an algebraic closure $\bar{\mathbf{Q}}_p$ of $\mathbf{Q}_p$, and an embedding $\sigma : \bar{\mathbf{Q}} \to \bar{\mathbf{Q}}_p$. By this embedding, we regard $\bar{\mathbf{Q}} \subseteq \bar{\mathbf{Q}}_p$. We fix also a p-adic valuation ord_p of $\bar{\mathbf{Q}}_p$ with $\mathrm{ord}_p(p) = 1$. Let T_K denote the set of all $\pi_{i,K}$ satisfying $\mathrm{ord}_p(\pi_{i,K}) = 0$. By the equality (3), we can see that ${}^{\#}T_K = \lambda_K$. We can take a positive integer d_K such that $\gcd(d_K, p) = 1$, and $\mathrm{ord}_p((\pi_{i,K})^{d_K} - 1) > 0$ for all $\pi_{i,K} \in T_K$ (see [Ro] p.171). Then we have the following result.

PROPOSITION 2.1. *Let m be a positive integer with $d_K|m$. Then we have*

$$\sum_{i=1}^{2g_K} (\pi_{i,K})^{mp^s} \longrightarrow \lambda_K \quad (s \to \infty)$$

in $\bar{\mathbf{Q}}_p$.

PROOF. From the definition of d_K, we have

$$\begin{cases} (\pi_{i,K})^{mp^s} \longrightarrow 1 \quad (s \to \infty) & \text{if } \pi_{i,K} \in T_K, \\ (\pi_{i,K})^{mp^s} \longrightarrow 0 \quad (s \to \infty) & \text{otherwise,} \end{cases}$$

in $\bar{\mathbf{Q}}_p$. Since ${}^{\#}T_K = \lambda_K$, we obtain the Proposition 2.1. □

3. A Proof of Theorem 1.2

Let L/K be a geometric cyclic extension of degee p. Let S_L and S_K be sets of all primes of L and K, respectively. Let $I_K (\subseteq S_K)$ be the set of all primes of K ramifying in L/K.

LEMMA 3.1. *Let m be a positive integer such that* $\deg_K P|m$ *for all $P \in I_K$. Then, for each integer $s \geq 0$, we have*

$$\sum_{\substack{\mathcal{P} \in S_L \\ \deg_L \mathcal{P}|mp^s}} \deg_L \mathcal{P} \equiv p \sum_{\substack{P \in S_K \\ \deg_K P|mp^s}} \deg_K P - \sum_{P \in S_K} (e_P - 1) \deg_K P \mod p^{s+1},$$

where e_P is the ramification index of P in L/K.

PROOF. Let $P \in S_K$. Then we have the following three cases:
(i) $e_P = 1,\ f_P = 1,\ g_P = p$ if P is decomposed completely in L/K,
(ii) $e_P = 1,\ f_P = p,\ g_P = 1$ if P inerts in L/K,
(iii) $e_P = p,\ f_P = 1,\ g_P = 1$ if P ramified in L/K,

where f_P is the relative degree of P in L/K, and g_P is the number of primes of L lying over P. It follows that

$$\sum_{\substack{\mathcal{P}\in S_L \\ \deg_L \mathcal{P}|mp^s}} \deg_L \mathcal{P} = p \sum_{\substack{P\in S_K \\ \deg_K P|mp^s}} \deg_K P - p \sum_{\substack{P\in S_K \\ P \text{ inerts} \\ \deg_K P=mp^s}} \deg_K P$$
$$+(1-p) \sum_{\substack{P\in S_K \\ P \text{ is ramified} \\ \deg_K P|mp^s}} \deg_K P\,.$$

By the choice of m, we have

$$(1-p) \sum_{\substack{P\in S_K \\ P \text{ is ramified} \\ \deg_K P|mp^s}} \deg_K P = -\sum_{P\in S_K} (e_P-1)\deg_K P\,.$$

These imply the conclusion. □

Let $Z_K(X),\ Z_L(X)$ be the polynomials corresponding to the zeta functions for K and L, respectively. We put

$$Z_K(X) = \prod_{i=1}^{2g_K}(1-\pi_{i,K}X) \quad (\pi_{i,K}\in \mathbf{C})\,,$$
$$Z_L(X) = \prod_{i=1}^{2g_L}(1-\pi_{i,L}X) \quad (\pi_{i,L}\in \mathbf{C})\,.$$

It is well-known that

$$q^N + 1 - \sum_{i=1}^{2g_K}(\pi_{i,K})^N = \sum_{\substack{P\in S_K \\ \deg_K P \mid N}} \deg_K P\,,$$
$$q^N + 1 - \sum_{i=1}^{2g_L}(\pi_{i,L})^N = \sum_{\substack{\mathcal{P}\in S_L \\ \deg_L \mathcal{P} \mid N}} \deg_L \mathcal{P}\,,$$

for all positive integer N (cf. [Ro] p.56). Let m be a positive integer such that $d_K \mid m$, $d_L \mid m$, $\deg_K P|m$ for all $P \in I_K$. By Lemma 3.1, we have

$$q^{mp^s} + 1 - \sum_{i=1}^{2g_L}(\pi_{i,L})^{mp^s} \equiv p\{q^{mp^s} + 1 - \sum_{i=1}^{2g_K}(\pi_{i,K})^{mp^s}\}$$
$$- \sum_{P\in S_K}(e_P-1)\deg_K P \mod p^{s+1}\,,$$

for each positive integer s. From Proposition 2.1, we complete the proof of Theorem 1.2.

4. Examples of supersingular function fields

In this section, we will construct supersingular function fields by using cyclotomic function fields. For definitions and properties of cyclotomic function fields, see [Ha], [Ro].

Let p be a prime. Let k be a field of rational functions over a finite field $\mathbf{F}_q$ with $q = p^e$ elements. Fix a generator T of k, and let $A = \mathbf{F}_q[T]$ be the polynomial subring of k. For a monic polynomial m, we denote the m th cyclotomic function field by K_m.

PROPOSITION 4.1. *Let Q be a monic polynomial of degree one. Then K_{Q^n} is supersingular for any positive integer n.*

PROOF. For any positive integer n with $n \geq 2$, the field K_{Q^n} is an abelian extension over $K_{Q^{n-1}}$ of degee $q = p^e$. Hence we can construct a sequence of field extensions:

$$K_{Q^{n-1}} = K_{Q^{n-1},0} \subseteq K_{Q^{n-1},1} \subseteq \cdots \subseteq K_{Q^{n-1},e} = K_{Q^n} ,$$

satisfiying $[K_{Q^{n-1},i} : K_{Q^{n-1},i-1}] = p$ for $i = 1, 2, ..., e$. By Proposition 2.2 in [Ha], only one prime is ramified in $K_{Q^{n-1},i}/K_{Q^{n-1},i-1}$ and its degree is one. Hence, by Theorem 1.2,

$$\lambda_{K_{Q^{n-1},i}} = p \times \lambda_{K_{Q^{n-1},i-1}} \tag{4}$$

for any n and i. On the other hand, using the Riemann-Hurwitz formula, we find that the genus of K_Q is zero. Hence $\lambda_{K_Q} = 0$. By equation (4), we obtain Proposition 4.1. □

REMARK 4.1. If Q is not a monic polynomial of degree one, then the Proposition 4.1 does not work. For example, let $q = 3$ and $Q = T^2 + 1 \in \mathbf{F}_3[T]$. Then we see that $Z_{K_Q}(X) = 1 - 2X^2 + 9X^4$. By equation (3), we have $\lambda_{K_Q} = 2$.

Let Q be a monic polynomial of degree one. By the above proposition, we have $\bar{Z}_{K_{Q^n}}(X) = 1$. Let $h_{K_{Q^n}}$ be the order of the divisor class group of K_{Q^n} of degree zero. By an analytic class number formula, we have $Z_{K_{Q^n}}(1) = h_{K_{Q^n}}$. Thus we have the following Corollary.

COROLLARY 4.1. *Let Q be a monic polynomial of degree one. Then we have $h_{K_{Q^n}} \equiv 1 \mod p$ for all $n \geq 1$.*

The above corollary was first showed by Guo and Shu [G-S] studying a congruence of an analytic class number formula.

ACKNOWLEDGEMENTS. The author would like to thank Prof. Yasutaka Ihara and Prof. Akio Tamagawa for their valuable comments. The author also wish to thank the referee for many helpful suggestions.

References

[Cr] CREW, RICHARD M., Etale p-covers in characteristic p, Compositio Math. **52** (1984), no. 1, 31–45.

[De] M. DEURING, Automorphismen und Divisorenklassen der Ordnung ι in algebraischen Funktionenkörpern, Math. Ann. **113** (1937), 208–215.

[Ha] HAYES, D. R., Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[G-S] GUO, L. and SHU, L., Class numbers of cyclotomic function fields., Trans. Amer. Math. Soc. 351 (1999), no. **11**, 4445–4467.

[K-M] KATZ, M. and MESSING, W., Some consequences of the Riemann hypothesis for varieties over finite fields. Invent. Math. **23** (1974), 73–77.

[Ma] MADAN, MANOHAR L., On a theorem of M. Deuring and I. R. Shafarevich., Manuscripta Math. **23** (1977), no. 1, 91–102.

[Ro] ROSEN, MICHAEL, *Number Theory in Function Fields*, Springer-Verlag, Berlin, 2002.

[Sha] I. R. SHAFAREVICH, On p-Extensions, Amer. Math. Soc. Trans. Series II, **4** (1954), 59–71.

[Su] SUBRAO, DORÉ, The p-rank of Artin-Schreier curves, Manuscripta Math. **16** (1975), no. 2, 169–193.

[Suw] Sur l'image de l'application d'Abel-Jacobi de Bloch, Bull. Soc. Math. France 116 (1988), no. **1**, 69–101.

Present Address:
GRADUATE SCHOOL OF MATHEMATICS,
NAGOYA UNIVERSITY,
CHIKUSA-KU, NAGOYA, 464–8602 JAPAN.
e-mail: m05019e@math.nagoya-u.ac.jp