An ordinary cyclotomic function field

By D. Shiomi

1 Introduction

Let $\mathbb{F}_q$ be the field with q elements of characteristic p. Let $k = \mathbb{F}_q(T)$ be the rational function field over $\mathbb{F}_q$, and $A = \mathbb{F}_q[T]$ the associated polynomial ring. Let $m \in A$ be a monic polynomial. Let K_m, K_m^+ be the m-th cyclotomic function field, and its maximal real subfield (see subsection 2.1). The aim of this paper is to study the structure of the Jacobians of K_m, K_m^+.

For a global function field K over $\mathbb{F}_q$, we denote by J_K the Jacobian of $K\bar{\mathbb{F}}_q$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. For a prime l, it is well-known that the l-primary subgroup $J_K(l)$ of J_K is isomorphic to the following group

$$J_K(l) \simeq \begin{cases} \bigoplus_{i=1}^{2g_K} \mathbb{Q}_l/\mathbb{Z}_l & \text{if } l \neq p, \\ \\ \bigoplus_{i=1}^{\lambda_K} \mathbb{Q}_p/\mathbb{Z}_p & \text{if } l = p, \end{cases}$$

where g_K is the genus of K, and λ_K is called the Hasse-Witt invariant of K. In general, λ_K satisfies with $0 \leq \lambda_K \leq g_K$. In particular, we shall call K supersingular if $\lambda_K = 0$, and ordinary if $\lambda_K = g_K$. For more details of the Jacobian, see [Ro1], [Mi].

Let g_m, g_m^+ be the genuses of K_m, K_m^+, respectively. Kida-Murabayashi gave explicit formulas for g_m, g_m^+ for all monic polynomial m (cf. [K-M]). Hence we obtain the l-ranks ($l \neq p$) of J_{K_m}, and $J_{K_m^+}$.

On the other hand, it is more difficult problem to construct an explicit formula for Hasse-Witt invariants. Let λ_m, λ_m^+ be the Hasse-Witt invariants of K_m, K_m^+, respectively. In the previous paper [Sh2], the author completely determined $m \in A$ satisfying $\lambda_m = 0$ (and $\lambda_m^+ = 0$).

In this paper, we shall consider the ordinary case. Assume that $m \in A$ is a monic irreducible polynomial of degree d. We set

$$s_i(n) = \sum_{a \in A(i)} a^n,$$

where $A(i)$ is the set of monic polynomials of degree i. For $1 \leq n \leq q^d - 2$, we define $B_n(u)$ as follows

$$B_n(u) = \begin{cases} \sum_{i=0}^{d-2} \left(\sum_{j=0}^{i} s_j(n) \right) u^i & \text{if } n \equiv 0 \mod q-1, \\ \\ \sum_{i=0}^{d-1} s_i(n) u^i & \text{if } n \not\equiv 0 \mod q-1. \end{cases} \tag{1}$$

Let $\mathcal{R}_m = A/mA$, and $\bar{f}(u) \in \mathcal{R}_m[u]$ be the reduction of $f(u) \in A[u]$ modulo m. Now we state our main result in this paper.

Theorem 1.1. *Let $m \in A$ be a monic irreducible polynomial of degee d. Then we have the following results.*

1. *K_m is ordinary if and only if*

$$\deg \bar{B}_n(u) = \begin{cases} \left[\frac{l(n)}{q-1}\right] - 1 & \textit{if } n \equiv 0 \mod q-1, \\ \\ \left[\frac{l(n)}{q-1}\right] & \textit{if } n \not\equiv 0 \mod q-1 \end{cases} \tag{2}$$

   for all $1 \leq n \leq q^d - 2$.

2. *K_m^+ is ordinary if and only if*

$$\deg \bar{B}_n(u) = \left[\frac{l(n)}{q-1}\right] - 1 \tag{3}$$

   for all $1 \leq n \leq q^d - 2$ $(n \equiv 0 \mod q-1)$.

Here $[x]$ is the maximal integer satisfying $[x] \leq x$, and $l(n) = a_0 + a_1 + \cdots + a_{d-1}$ if $n = a_0 + a_1 q + \cdots + a_{d-1} q^{d-1}$ $(0 \leq a_i \leq q-1)$.

Assume that $q \neq p$. By using Theorem 1.1, we will completely determine a monic irreducible polynomial m such that K_m is ordinary (see Corollary 3.1). On the other hand, in the case $q = p$, it is more difficult problem to determine such m. In section 4, we shall give some examples of ordinary cyclotomic function fields.

Remark 1.1. The above polynomial $B_n(u)$ is closely related to characteristic p zeta function (cf. [Go1]).

2 Preparations

2.1 Cyclotomic function fields

In this subsection, we shall provide basic facts about cyclotomic function fields. For details, see [Ha], [Ro1], [Go1].

Let $\bar{k}$ be an algebraic closure of k. For $x \in \bar{k}$ and $m \in A$, we define the following action

$$m * x = m(\varphi + \mu)(x),$$

where φ, μ are $\mathbb{F}_q$-linear isomorphisms of $\bar{k}$ defined by $\varphi : x \mapsto x^q$, and $\mu : x \mapsto Tx$, respectively. By this action, $\bar{k}$ becomes A-module. This A-module is called the Carlitz module. For a monic polynomial $m \in A$, we set

$$\Lambda_m = \{x \in \bar{k} \ : \ m * x = 0\}.$$

Let $K_m = k(\Lambda_m)$, which is called the m-th cyclotomic function field. One shows that K_m/k is a Galois extension, and have the group isomorphism

$$\mathrm{Gal}(K_m/k) \simeq (A/mA)^{\times}, \tag{4}$$

where $\mathrm{Gal}(K_m/k)$ is the Galois group of K_m/k. We regard $\mathbb{F}_q^{\times} \subseteq (A/mA)^{\times}$, and let K_m^+ be the intermediate field of K_m/k corresponding to $\mathbb{F}_q^{\times}$. The field K_m^+ is called the maximal real subfield of K_m. Let P_∞ be the prime of k with the valuation ord_∞ satisfying $\mathrm{ord}_\infty(1/T) = 1$. Then P_∞ splits completely in K_m^+/k, and any prime of K_m^+ over P_∞ is totally ramified in K_m/K_m^+. Hence we have

$$K_m^+ = k_\infty \cap K_m,$$

where k_∞ is the associated completion of k by P_∞.

2.2 Zeta functions

In this subsection, we shall study the zeta function of cyclotomic function fields. For more references, see [G-R], [Ro1].

For a global function field K over $\mathbb{F}_q$, we define the zeta function of K by

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

where $\mathcal{P}$ runs through all primes of K, and $\mathcal{N}\mathcal{P}$ is the number of elements of the reduce class field of $\mathcal{P}$. Then $\zeta(s, K)$ converges absolutely for $\mathrm{Re}(s) > 1$.

Theorem 2.1. *Let g_K be the genus of K. Then there is a polynomial $Z_K(u) \in \mathbb{Z}[u]$ of degree $2g_K$ satisfying*

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

Now we focus on the cyclotomic function field case. Let $m \in A$ be a monic polynomial of degree d. Let $\zeta(s, K_m)$, $\zeta(s, K_m^+)$ be zeta functions of K_m, and K_m^+, respectively. By Theorem 2.1, there are polynomials $Z_m(u)$, and $Z_m^{(+)}(u)$ such that

$$\zeta(s, K_m) = \frac{Z_m(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}, \tag{5}$$

$$\zeta(s, K_m^+) = \frac{Z_m^{(+)}(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}. \tag{6}$$

Let X_m be the group of primitive Dirichlet characters modulo m, and X_m^+ is the subgroup of X_m defined by

$$X_m^+ = \{\chi \in X_m : \chi(a) = 1 \text{ for all } a \in \mathbb{F}_q^\times\}.$$

By the same arguments in subsection 2.2 in [Sh1], we have

$$\zeta(s, K_m) = \Big\{ \prod_{\chi \in X_m} L(s, \chi) \Big\} (1 - q^{-s})^{-[K_m^+ : k]}, \tag{7}$$

$$\zeta(s, K_m^+) = \Big\{ \prod_{\chi \in X_m^+} L(s, \chi) \Big\} (1 - q^{-s})^{-[K_m^+ : k]}. \tag{8}$$

Here an L-function $L(s, \chi)$ is defined by

$$L(s, \chi) = \sum_{a: monic} \frac{\chi(a)}{N(a)^s},$$

where a runs through all monic polynomials of A, and $N(a) = q^{\deg a}$. Let χ_0 be the trivial character. We can check that

$$L(s, \chi) = \begin{cases} 1/(1 - q^{1-s}) & \text{if } \chi = \chi_0, \\ \sum_{i=0}^{d-1} s_i(\chi) q^{-si} & \textit{otherwise}, \end{cases}$$

where $s_i(\chi) = \sum_{\substack{a:monic \\ \deg(a)=i}} \chi(a)$ for $i = 0, 1, ..., d-1$. We set

$$\Phi_\chi(u) = \begin{cases} \left(\sum_{i=0}^{d-1} s_i(\chi)u^i\right)/(1-u) & \text{if } \chi \in X_m^+ \setminus \{\chi_0\}, \\ \sum_{i=0}^{d-1} s_i(\chi)u^i & \text{if } \chi \in X_m^-, \end{cases}$$

where $X_m^- = X_m \setminus X_m^+$. From equations (5) (6) (7) (8), we obtain the following result.

Proposition 2.1.

$$(1)\ \ Z_m(u) = \prod_{\substack{\chi \in X_m \\ \chi \neq \chi_0}} \Phi_\chi(u), \tag{9}$$

$$(2)\ Z_m^{(+)}(u) = \prod_{\substack{\chi \in X_m^+ \\ \chi \neq \chi_0}} \Phi_\chi(u). \quad . \tag{10}$$

Remark 2.1. Assume that $\chi \in X_m^+ \setminus \{\chi_0\}$. Noting that $\sum_{i=0}^{d-1} s_i(\chi) = 0$, we have

$$\Phi_\chi(u) = \sum_{i=0}^{d-2} \left(\sum_{j=0}^{i} s_j(\chi)\ \right) u^i. \tag{11}$$

In particular, $\Phi_\chi(u)$ is a polynomial.

2.3 The Hasse-Witt invarinat

Our goal in this subsection is to express λ_m and λ_m^+ in terms of $B_n(u)$. To do this, we will study a relation between $B_n(u)$ and $Z_m(u)$ (and $Z_m^{(+)}(u)$). For more information, see chapter 8 of [Go1].

Let $m \in A$ be a monic irreducible polynomial of degree d. We denote the p-adic field by $\mathbb{Q}_p$. Fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, and an embedding $\sigma : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$. By this embedding, we regard $\bar{\mathbb{Q}} \subseteq \bar{\mathbb{Q}}_p$. Let ord_p the p-adic valuation of $\bar{\mathbb{Q}}_p$ with $\mathrm{ord}_p(p) = 1$. We set

$$M = \mathbb{Q}_p(W),$$

where W is the group of $(p^{de}-1)$-th roots of unity (we assume $q = p^e$). Let $\mathcal{O}_M$ be the valuation ring of M. Since $M/\mathbb{Q}_p$ is unramified, the residue class field $\mathcal{F}_M = \mathcal{O}_M/p\mathcal{O}_M$ consists of p^{de} elements. We notice that the image of $\chi \in X_m$ is contained in $\mathcal{O}_M$. Hence we see that

$$\Phi_\chi(u) \in \mathcal{O}_M[u] \quad (\text{ for } \ \chi \in X_m \setminus \{\chi_0\} \ ).$$

Notice that $\mathcal{R}_m$ and $\mathcal{F}_M$ are finite fields with same cardinality. Hence $\mathcal{R}_m$ is isomorphic to $\mathcal{F}_M$, and fix an isomorphism $\phi : \mathcal{R}_m \to \mathcal{F}_M$. This map derives the group isomorphism $\phi_0 : (A/mA)^\times \to \mathcal{F}_M^\times$, and the ring isomorphism $\phi_* : \mathcal{R}_m[u] \to \mathcal{F}_M[u]$. Since p is prime to ${}^\# W$ (= the cardinality of W), we have the following isomorphism

$$\psi : W \longrightarrow \mathcal{F}_M^\times \ \ (\zeta \to \zeta \mod p\mathcal{O}_M \ ).$$

Put $\omega = \psi^{-1} \circ \phi_0$. Then ω is a generator of X_m. Hence we have

$$X_m = \{\omega^n \mid n = 0, \ 1, \ 2, ..., \ q^d - 2\}.$$

We see that $\omega^n \in X_m^+$ if $n \equiv 0 \mod q-1$, and $\omega^n \in X_m^-$ if $n \not\equiv 0 \mod q-1$. We notice that

$$\phi(a^n \mod mA) \equiv \omega^n(a \mod mA) \mod p\mathcal{O}_p$$

for $a \in A$ $(0 \leq \deg(a) < d)$, and $n = 0, 1, ..., q^d - 2$. Hence, by the definition of $B_n(u)$, we obtain

$$\phi_*(\bar{B}_n(u)) = \bar{\Phi}_{\omega^n}(u),$$

where $\bar{\Phi}_\chi(u)$ is the reduction of $\Phi_\chi(u)$ modulo $p\mathcal{O}_M$. From Proposition 2.1, we obtain the following results.

Proposition 2.2.

$$(1) \ \phi_*\Big(\prod_{n=1}^{q^d-2} \bar{B}_n(u)\Big) = \bar{Z}_m(u), \tag{12}$$

$$(2) \ \phi_*\Big(\prod_{\substack{n=1 \\ n\equiv 0 \mod q-1}}^{q^d-2} \bar{B}_n(u)\Big) = \bar{Z}_m^{(+)}(u). \tag{13}$$

Proposition 2.2 leads the following relation between λ_m(or λ_m^+) and $B_n(u)$.

Corollary 2.1.

$$(1)\ \lambda_m = \sum_{n=1}^{q^d-2} \deg \bar{B}_n(u), \tag{14}$$

$$(2)\ \lambda_m^+ = \sum_{\substack{n=1 \\ t\equiv 0 \mod q-1}}^{q^d-2} \deg \bar{B}_n(u). \tag{15}$$

Proof. By Proposition 11.20 in [Ro1], we have

$$\lambda_m = \deg \bar{Z}_m(u), \quad \lambda_m^+ = \deg \bar{Z}_m^{(+)}(u).$$

Hence we obtain Corollary 2.1 from Proposition 2.2. □

2.4 Degrees of $B_n(u)$

In this subsection, we shall study the degree of $B_n(u)$. To see this, we review some results of Gekeler [Ge].

Fix an integer $d \geq 0$. For $n = a_0 + a_1 q + \cdots + a_{d-1} q^{d-1}$ $(0 \leq a_i \leq q-1)$, we define e_i $(1 \leq i \leq l(n))$ as follows:

$$n = \sum_{i=1}^{l(n)} q^{e_i} \quad (0 \leq e_i \leq e_{i+1},\ e_i < e_{i+q-1}).$$

(Recall that $l(n) = a_0 + a_1 + \cdots + a_d$). We set

$$\rho(n) = \begin{cases} -\infty & \text{if } l(n) < q-1, \\ n - \sum_{i=1}^{q-1} q^{e_i} & \text{Otherwise.} \end{cases}$$

Moreover $\rho(-\infty) = -\infty$, $\rho^{(0)}(n) = n$, and $\rho^{(i)} = \rho^{(i-1)} \circ \rho$. We also put $\deg 0 = -\infty$. Then Gekeler showed the following result.

Proposition 2.3. *(cf. Proposition 2.11 in [Ge])*

$$\deg(s_i(n)) \leq \rho^{(1)}(n) + \rho^{(2)}(n) \cdots + \rho^{(i)}(n).$$

Moreover, the equality holds if q=p(:prime).

In particular, we have the following results.

Corollary 2.2. *If $l(n)/(q-1) < i$, then $s_i(n) = 0$. Assume that $q = p$. Then $l(n)/(p-1) < i$ if and only if $s_i(n) = 0$.*

Next we set

$$C_n(u) = \sum_{i=0}^{\infty} s_i(n) u^i.$$

From Corollary 2.2, we see that $C_n(u) \in A[u]$. Moreover, we have the following result.

Lemma 2.1. $\deg C_n(u) \leq \left[\frac{l(n)}{q-1}\right]$. *The equality holds if $q = p$.*

Proof. This follows from Corollary 2.2. □

Lemma 2.2. *If $1 \leq n \leq q^d - 2$ ($n \equiv 0 \mod q-1$), then $C_n(1) = 0$.*

Proof. This follows from Lemma 6.1 in [Ge] □

From Lemma 2.2, we obtain

$$B_n(u) = \begin{cases} C_n(u)/(1-u) & \text{if } n \equiv 0 \mod q-1, \\ \\ C_n(u) & \text{if } n \not\equiv 0 \mod q-1 \end{cases} \tag{16}$$

for $1 \leq n \leq q^d - 2$. From equation (16), we see that $B_n(u)$ is only depend on n (independent on the choice of d).

Proposition 2.4.

$$\begin{aligned} &(1) \quad \deg B_n(u) \leq \left[\tfrac{l(n)}{q-1}\right] - 1 \quad && \textit{if } n \equiv 0 \mod q-1, \\ &(2) \quad \deg B_n(u) \leq \left[\tfrac{l(n)}{q-1}\right] && \textit{if } n \not\equiv 0 \mod q-1. \end{aligned} \tag{17}$$

In particular, equalities hold if $q = p$.

Proof. This follows from Lemma 2.1 . □

3 A proof of Theorem 1.1

Our goal in this section is to prove Theorem 1.1. To do this, we first show the following lemma.

Lemma 3.1. *For a positive integer d, we have*

$$\text{(1)} \quad \sum_{\substack{n=1 \\ n\equiv 0 \mod q-1}}^{q^d-2} \left[\frac{l(n)}{q-1}\right] = \frac{d}{2}\Big(\frac{q^d-1}{q-1}-1\Big), \tag{18}$$

$$\text{(2)} \quad \sum_{\substack{n=1 \\ n\not\equiv 0 \mod q-1}}^{q^d-2} \left[\frac{l(n)}{q-1}\right] = \frac{(d-1)(q-2)(q^d-1)}{2(q-1)}. \tag{19}$$

Proof. We can check that

$$l(n) + l(q^d-1-n) = (q-1)d$$

for $1 \le n \le q^d-2$. Assume that $n \equiv 0 \mod q-1$. Since $l(n) \equiv l(q^d-1-n) \equiv 0 \mod q-1$, we have

$$\left[\frac{l(n)}{q-1}\right] + \left[\frac{l(q^d-1-n)}{q-1}\right] = d.$$

Therefore,

$$\sum_{\substack{n=1 \\ n\equiv 0 \mod q-1}}^{q^d-2} \left\{\left[\frac{l(n)}{q-1}\right] + \left[\frac{l(q^d-1-n)}{q-1}\right]\right\} = d\Big(\frac{q^d-1}{q-1}-1\Big).$$

This leads equation (18). Next we assume that $n \not\equiv 0 \mod q-1$. Then

$$\left[\frac{l(n)}{q-1}\right] + \left[\frac{l(q^d-1-n)}{q-1}\right] = d-1.$$

Therefore,

$$\sum_{\substack{n=1 \\ n\not\equiv 0 \mod q-1}}^{q^d-2} \left\{\left[\frac{l(n)}{q-1}\right] + \left[\frac{l(q^d-1-n)}{q-1}\right]\right\} = \frac{(d-1)(q-2)(q^d-1)}{(q-1)}.$$

Hence we obtain equation (19). □

Now we give the proof of Theorem 1.1.

Proof. One shows that g_m, g_m^+ can be calculated as follows

$$2g_m = (dq-d-q)\Big(\frac{q^d-1}{q-1}\Big)-(d-2), \tag{20}$$

$$2g_m^+ = (d-2)\Big(\frac{q^d-1}{q-1}-1\Big) \tag{21}$$

(cf. [K-M]). By comparing with Lemma 3.1, we obtain

$$g_m = \sum_{\substack{n=1 \\ n\equiv 0 \mod q-1}}^{q^d-2} \Big(\Big[\frac{l(n)}{q-1}\Big]-1\Big)+\sum_{\substack{n=1 \\ n\not\equiv 0 \mod q-1}}^{q^d-2} \Big[\frac{l(n)}{q-1}\Big], \tag{22}$$

$$g_m^+ = \sum_{\substack{n=1 \\ n\equiv 0 \mod q-1}}^{q^2-2} \Big(\Big[\frac{l(n)}{q-1}\Big]-1\Big). \tag{23}$$

First we assume that $\lambda_m = g_m$. Then, by Corollary 2.1 and Proposition 2.4, and equation (22), we see that equation (2) holds. Conversely, we assume that equation (2) holds. Then, by Corollary 2.1 and equation (22), we obtain $\lambda_m = g_m$. This complete the proof of the part 1 of Theorem 1.1.

By the same arguments, we can prove the part 2 of Theorem 1.1. □

Remark 3.1. From the proof of Theorem 1.1, we have the following results.

1. If K_m is ordinary, then

$$\deg \bar{B}_n(u) = \deg B_n(u) = \begin{cases} \Big[\frac{l(n)}{q-1}\Big]-1 & \text{if } n\equiv 0 \mod q-1, \\ \Big[\frac{l(n)}{q-1}\Big] & \text{if } n\not\equiv 0 \mod q-1 \end{cases}$$

   for all $1 \le n \le q^d-2$.

2. If K_m^+ is ordinary, then

$$\deg \bar{B}_n(u) = \deg B_n(u) = \Big[\frac{l(n)}{q-1}\Big]-1$$

   for all $1 \le n \le q^d-2$ $(n \equiv 0 \mod q-1)$.

By using Theorem 1.1, we determine all ordinary cyclotomic function field in the case of $q \neq p$.

Corollary 3.1. *We assume that $q \neq p$. Let m be a monic irreducible polynomial. Then we have the following results.*

1. *K_m is ordinary if and only if $\deg m = 1$.*
2. *K_m^+ is ordinary if and only if $\deg m \leq 2$.*

Proof. First we show the assertion 1. Assume that $\deg m = 1$. Then we obtain $g_m = 0$ by equation (20). Hence K_m is ordinary. Next, we put $n = (q-p) + pq$. Then $l(n) = q \not\equiv 0 \mod q-1$. By Corollary 3.14 in [Ge], we have

$$s_1(n) = -\begin{pmatrix} p \\ p-1 \end{pmatrix} (T^p - T) = 0.$$

Hence $B_n(u) = 1$. Notice that $\deg B_n(u) < [\frac{l(n)}{q-1}]$. It follows that K_m is not ordinary if $\deg m \geq 2$. This leads the assertion 1 of Corollary 3.1.

Secondly, we will show the assertion 2 of Corollary 3.1. By equation (21), we see that K_m^+ is ordinary if $\deg m \leq 2$. Next, we put $n = p + (q-p)q + (q-2)q^2$, and $n_0 = n/p = 1 + (q - q/p - 1)q + (q/p - 1)q^2$. Then we have $l(n) = 2(q-1)$, and $l(n_0) = q-1$. By Proposition 2.4, we have $1 + s_1(n_0) = 0$. Noting that

$$1 + s_1(n) = (1 + s_1(n_0))^p = 0,$$

we have $B_n(u) = 1$. Hence $\deg B_n(u) < [\frac{l(n)}{q-1}] - 1$. It follows that K_m^+ is not ordinary if $\deg m \geq 3$. This leads the assertion 2 of Corollary 3.1. □

The above corollary is not true in the case $q = p$. We will see this in the next section.

4 Some examples of ordinary cyclotomic function field

In this section, we assume $q = p$. As an application of Theorem 1.1, we shall construct some examples of ordinary cyclotomic function fields.

Proposition 4.1. *Assume $m \in A$ is a monic irreducible polynomial of degree two. Then K_m^+, and K_m are ordinary.*

Proof. From equation (20), we have $g_m^+ = 0$. Hence K_m^+ is ordinary.

Next we will show that K_m is ordinary. To see this, we shall see that equation (2) holds. We first consider the case $l(n) \leq p-1$. By Proposition 2.4, we have $B_n(u) = 1$. Hence equation (2) holds in this case.

Secondly, we consider the case $p \leq l(n) < 2(p-1)$. Noting that $n \not\equiv 0 \mod p-1$, we obtain

$$B_n(u) = 1 + s_1(n)u.$$

Here we put $n = a + bp$ $(0 \leq a,\ b \leq p-1)$. Then Gekeler showed

$$s_1(n) = -\begin{pmatrix} b \\ p-1-a \end{pmatrix} (T^p - T)^{a+b-(p-1)}$$

(cf. Corollary 3.14 in [Ge]). Hence $s_1(n) \not\equiv 0 \mod m$. Therfore equation (2) holds in this case. This complete the proof of Proposition 4.1. □

Proposition 4.2. *Assume that $m \in A$ is a monic irreducible polynomial of degree three. Then K_m^+ is ordinary.*

Proof. Fix an integer n such that $1 \leq n \leq p^3 - 2$ $(n \equiv 0 \mod p-1)$. Then we have

$$B_n(u) = 1 + f_n(T)u,$$

where $f_n(T)$ is defined by

$$f_n(T) = 1 + s_1(n) = 1 + \sum_{\alpha \in \mathbb{F}_q} (T+\alpha)^n.$$

We notice that $l(n) = p-1$ or $2(p-1)$. First, we assume that $l(n) = p-1$. Then, by Proposition 2.4, we have $B_n(u) = 1$. Hence equation (3) holds in this case.

Secondly, we consider the case $l(n) = 2(p-1)$. From Proposition 2.4, we see that $f_n(T) \neq 0$. Assume that $f_n(T) \equiv 0 \mod m$. Let ω be a root of m. Then ω is also a root of $f_n(T)$. We put

$$\begin{aligned} W_1 &= \Big\{ a + \frac{b}{\omega + c} : a, c \in \mathbb{F}_q,\ b \in \mathbb{F}_q^\times \Big\}, \\ W_2 &= \Big\{ a + b\omega : a, b \in \mathbb{F}_q \Big\}. \end{aligned}$$

We can easily check that (i) $f_n(T+\alpha) = f_n(T) \quad (\alpha \in \mathbb{F}_q)$, (ii) $f_n(\alpha T) = f_n(T) \quad (\alpha \in \mathbb{F}_q^\times)$, (iii) $T^n f_n(1/T) = f_n(T)$. Hence each element of $W_1 \cup W_2$ is also a root of $f_n(T)$. Notice that ω is a root of irreducible polynomial of degree 3. Hence

$$W_1 \cap W_2 = \phi, \ \ {}^{\#}W_1 = p^3 - p^2, \ \ {}^{\#}W_2 = p^2.$$

Therefore $f_n(T)$ has distinct p^3 roots. However $\deg f_n(T) \leq n \leq p^3 - 2$. This is a contradiction. Therefore $f_n(T) \not\equiv 0 \mod m$. Hence equation (3) holds in this case. □

Remark 4.1. The above result is not true for K_m. In fact, we consider the case $p = 3$ and $m = T^3 + 2T + 1$. Then $g_m = 19$, and $\lambda_m = 18$.

References

[Ge] E.-U. Gekeler: On power sums of polynomials over finite fields, J. Number Theory **30** (1988), no. 1, 11–26.

[G-R] S. Galovich and M. Rosen: The class number of cyclotomic function fields, J. Number Theory **13** (1981), no. 3, 363–375.

[Go1] D. Goss: Basic Structures of Function field Arithmetic, Springer-Verlag, Berlin, 1998.

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

[K-M] M. Kida and N. Murabayashi: Cyclotomic function fields with divisor class number one, Tokyo J. Math. **14** (1991), no. 1, 45–56.

[Mi] J.S. Milne: Jacobian varieties, in Arithmetic Geometry, Springler-Verlag, New York, 1986

[Ro1] M. Rosen: Number Theory in Function Fields, Springer-Verlag, Berlin, 2002.

[Sh1] Daisuke Shiomi: A determinant formula for relative congruence zeta functions for cyclotomic function fields, J. Aust. Math. Soc. **89** (2010), 133–144.

[Sh2] Daisuke Shiomi: The Hasse-Witt invariant of cyclotomic function fields, Acta Arith. **150** (2011), 227-240.

Daisuke Shiomi
Graduate School of Mathematics, Nagoya University
Furou-cho, Chikusa-ku, Nagoya 464-8602, Japan
Mail: m05019e@math.nagoya-u.ac.jp