Explicit formulas for Hasse-Witt invariants of cyclotomic function fields with conductor of degree two

By

Daisuke SHIOMI *

§ 1. Introduction

Let $p$ be a prime. Let $\mathbb{F}_q$ be the field with $q = p^r$ elements. Let $k = \mathbb{F}_q(T)$ be the rational function field over $\mathbb{F}_q$, and let $A = \mathbb{F}_q[T]$ be the polynomial subring of $k$. For a monic polynomial $m \in A$, we denote the $m$-th cyclotomic function field by $K_m$. For definitions and basic properties of cyclotomic function field, see [Go], [Ha], and [Ro].

Let us denote by $J_m$ the Jacobian of $K_m \mathbb{F}_q$, where $\mathbb{F}_q$ is an algebraic closure of $\mathbb{F}_q$. For a prime $l$, it is well-known that the $l$-primary subgroup $J_m(l)$ of $J_m$ satisfies

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

where $g_m$ is the genus of $K_m$, and $\lambda_m$ is an integer where $0 \leq \lambda_m \leq g_m$. The integer $\lambda_m$ is called the Hasse-Witt invariant of $K_m$.

Kida and Murabayashi gave an explicit formula for $g_m$ for all monic polynomial $m \in A$ as Corollary 1 in the section 2 of [K-M]. Applying their genus formula to the cases of $\deg m = 1$ and $\deg m = 2$, we have gotten

**Theorem 1.1.** Let $m \in A$ be a monic polynomial.

(1) If $\deg m = 1$, then we have $g_m = 0$. 

2000 Mathematics Subject Classification(s): 11M38, 11R60.

Key Words: cyclotomic function field, Jacobian variety.

*Department of Mathematical Sciences, Faculty of Science, Yamagata University, 1-4-12 Kojirakawamachi, Yamagata, 990-8560, Japan. e-mail: shiomi@sci.kj.yamagata-u.ac.jp

© 2013 Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.
(2) If \( \deg m = 2 \), then we have

\[
g_m = \begin{cases} 
\frac{(q-2)(q+1)}{2} & \text{if } m \text{ is irreducible,} \\
\frac{(q-2)(q-1)}{2} & \text{if } m = P^2 \text{ where } P \text{ is a monic polynomial of degree one,} \\
\frac{(q-2)(q-3)}{2} & \text{if } m = PQ \text{ where } P, Q \text{ are distinct monic polynomials of degree one.}
\end{cases}
\]

Next we consider the Hasse-Witt invariant case. The main theorem of this paper is the following results.

**Theorem 1.2.** Let \( m \in A \) be a monic polynomial, and \( q = p^r \).

(1) If \( \deg m = 1 \), then we have \( \lambda_m = 0 \).

(2) If \( \deg m = 2 \), then we have

\[
\lambda_m = \begin{cases} 
\left( \frac{p(p+1)}{2} \right)^r q - 1 & \text{if } m \text{ is irreducible,} \\
0 & \text{if } m = P^2 \text{ where } P \text{ is a monic polynomial of degree one,} \\
\left( \frac{p(p+1)}{2} \right)^r - 3q + 3 & \text{if } m = PQ \text{ where } P, Q \text{ are distinct monic polynomials of degree one.}
\end{cases}
\]

**Remark.** Noting that \( \lambda_m \leq g_m \), we have \( \lambda_m = 0 \) if \( \deg m = 1 \). Hence we obtain the first assertion of Theorem 1.2.

We call \( K_m \) ordinary if \( \lambda_m = g_m \). By comparing Theorem 1.1 and 1.2, we obtain the following results.

**Corollary 1.3.** Let \( m \in A \) be a monic polynomial of degree two.

(1) Assume that \( q = p \). Then \( K_m \) is ordinary if and only if one of the following conditions holds: (a) \( q = 2 \), (b) \( m \) is irreducible, (c) \( m = PQ \) where \( P, Q \) are distinct polynomials of degree one.

(2) Assume that \( q = p^r (r \geq 2) \). Then \( K_m \) is not ordinary.
The second assertion of Corollary 1.3 is generalized as follows:

**Theorem 1.4.** Assume that $q = p^r (r \geq 2)$, and $m \in A$ is a monic polynomial. Then $K_m$ is ordinary if and only if $\deg m = 1$. In this case, $K_m$ is rational.

§ 2. Preparations

In this section, we review some basic facts for zeta functions, $L$-functions, and power residue symbols.

Let us define the zeta function of $K_m$ as follows

$$\zeta(s, K_m) = \prod_{\mathfrak{p} \text{prime}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1},$$

where $\mathfrak{p}$ runs through all primes of $K_m$, and $N\mathfrak{p}$ is the number of elements of the reduce class field of $\mathfrak{p}$. By the standard fact about the zeta function, there is a polynomial $Z_m(u) \in \mathbb{Z}[u]$ such that

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

Then we have the following relation between $\lambda_m$ and $Z_m(u)$.

**Theorem 2.1.** (cf. Proposition 11.20 in [Ro]).

$$\lambda_m = \deg \bar{Z}_m(u),$$

where $\bar{Z}_m(u) \in \mathbb{F}_p[u]$ is the reduction of $Z_m(u)$ modulo $p$.

Let $X_m$ be the group of all primitive Dirichlet characters modulo $m$. Then $\zeta(s, K_m)$ can be written as follows

$$\zeta(s, K_m) = \left\{ \prod_{\chi \in X_m} L(s, \chi) \right\} (1 - q^{-s})^{-\frac{[K_m:k]}{q-1}},$$

where $L(s, \chi) = \sum_{a \in A \text{monic}} \chi(a)q^{-s \deg a}$. (cf. Lemma 2.1 in [Sh1]).

For a character $\chi \in X_m$, we call $\chi$ real if $\chi(a) = 1$ for all $a \in \mathbb{F}_q^\times$. Otherwise, we call $\chi$ imaginary.

Let $m \in A$ be a monic polynomial of degree $d$. For $\chi \in X_m$, we put

$$s_i(\chi) = \sum_{a \text{monic} \atop \deg a = i} \chi(a).$$

Then it is known that
• $s_i(\chi) = 0$ if $\chi$ is non-trivial and $i \geq \deg f_\chi$,

• $\sum_{i=0}^{d-1} s_i(\chi) = 0$ if $\chi$ is non-trivial and real,

where $f_\chi$ is the conductor of $\chi$ (cf. section 3 in [G-R]). Assume that $d = 2$. Then $L(s, \chi)$ can be calculated as follows

$$L(s, \chi) = \begin{cases} (1 - q^{1-s})^{-1} & \text{if } f_\chi = 1, \\ 1 & \text{if } \deg f_\chi = 1, \\ 1 - q^{-s} & \text{if } f_\chi = m, \text{ and } \chi \text{ is real}, \\ 1 + s_1(\chi)q^{-s} & \text{if } f_\chi = m, \text{ and } \chi \text{ is imaginary.} \end{cases}$$

Hence we obtain

$$Z_m(u) = \prod_{\chi \text{ imaginary}} (1 + s_1(\chi)u).$$

In the end of this section, we review a power residue symbol. For an integer $n \geq 2$, let $W_n$ be the set of all $n$-th roots of unity. Let $K$ be a number field containing $W_n$, and let $\mathcal{O}_K$ be the ring of integers of $K$. Let $\mathfrak{p}$ be a prime ideal of $K$ not dividing $n$. For $\alpha \in \mathcal{O}_K$ which is prime to $\mathfrak{p}$, there exists uniquely $\left(\frac{\alpha}{\mathfrak{p}}\right)_n \in W_n$ satisfying

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{(N\mathfrak{p} - 1)/n} \mod \mathfrak{p}.$$  

We call $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ the power residue symbol mod $\mathfrak{p}$ of order $n$.

§ 3. A proof of Theorem 1.2

The purpose of this section is to prove the second assertion of Theorem 1.2.

§ 3.1. The case (I)

Assume that $m$ is a monic irreducible polynomial of degree two. Take $\gamma \in F_{q^2}$ so that $m(\gamma) = 0$. Then $f(T) \mapsto f(\gamma)$ gives rise to an isomorphism $A/mA \cong F_{q^2}$. Now let $\mathfrak{p}$ be a prime ideal of $K = \mathbb{Q}(e^{2\pi i/(q^2-1)})$ dividing $p$, and let $\chi_{\mathfrak{p}} = \left(\frac{\gamma}{\mathfrak{p}}\right)^{(q^2-1)/q-1}$ be the power residue symbol mod $\mathfrak{p}$ of order $q^2 - 1$. We see that $\chi_{\mathfrak{p}}^n$ is real if and only if $n$ is divisible by $q - 1$. Therefore, by the equality (2.1), we have

$$Z_m(u) = \prod_{0 \leq n \leq q^2 - 2 \atop n \equiv 0 \mod q - 1} (1 + s_1(\chi_{\mathfrak{p}}^n)u).$$
Under the identification $A/mA = \mathbb{F}_{q^2}$, we have an equality

$$s_1(\chi_p^n) = \sum_{\alpha \in \mathbb{F}_q} (\gamma + \alpha)^n$$

in $\mathbb{F}_{q^2} = \mathcal{O}_K/p$.

For $1 \leq n \leq q^2 - 2$ ($n \not\equiv 0 \pmod{q-1}$), we consider the $q$-adic expansion $n = a(n) + b(n)q$. By the Newton formula, we have gotten

$$\sum_{\alpha \in \mathbb{F}_q} (T + \alpha)^n = -\left(\begin{array}{lll}b(n) \\ q - 1 - a(n)\end{array}\right) (T^q - T)^{a(n)+b(n)-(q-1)},$$

as was verified by Gekeler (cf. Corollary 3.14 in [Ge]). Here $\left(\begin{array}{*}\end{array}\right)$ is a binomial coefficient. This implies an equality

$$s_1(\chi_p^n) = -\left(\begin{array}{lll}b(n) \\ q - 1 - a(n)\end{array}\right) (\gamma^q - \gamma)^{a(n)+b(n)-(q-1)}$$

in $\mathbb{F}_{q^2}$. Notice that $\left(\begin{array}{l}b(n) \\ q - 1 - a(n)\end{array}\right) \equiv 0 \pmod{p}$ for $a(n) + b(n) < q - 1$. Therefore, by Theorem 2.1 and the equality (3.1), we obtain

$$(3.2) \quad \lambda_m = \# \left\{ 1 \leq n \leq q^2 - 2 : a(n) + b(n) > q - 1, \left(\begin{array}{l}b(n) \\ q - 1 - a(n)\end{array}\right) \not\equiv 0 \pmod{p} \right\},$$

where $\#S$ is the number of elements of a set $S$. Next we will calculate the right side of the equality (3.2). For $1 \leq n \leq q^2 - 2$, we put

$$a(n) = a_0(n) + a_1(n)p + \cdots + a_{r-1}(n)p^{r-1},$$

$$b(n) = b_0(n) + b_1(n)p + \cdots + b_{r-1}(n)p^{r-1},$$

where $0 \leq a_i(n), b_i(n) \leq p - 1$ ($i = 0, 1, \ldots, r - 1$). Since

$$q - 1 - a(n) = (p - 1 - a_0(n)) + (p - 1 - a_1(n))p + \cdots + (p - 1 - a_{r-1}(n))p^{r-1},$$

we have

$$\left(\begin{array}{l}b(n) \\ q - 1 - a(n)\end{array}\right) \equiv \prod_{i=0}^{r-1} \left(\begin{array}{l}b_i(n) \\ p - 1 - a_i(n)\end{array}\right) \pmod{p}.$$ 

Hence we obtain the following equivalence

$$\left(\begin{array}{l}b(n) \\ q - 1 - a(n)\end{array}\right) \not\equiv 0 \pmod{p} \Leftrightarrow a_i(n) + b_i(n) \geq p - 1 \ (0 \leq i \leq r - 1).$$
We see that
\[
\left( \frac{p(p+1)}{2} \right)^r = \# \{ n \in [0, q^2 - 1] : a_i(n) + b_i(n) \geq p - 1 \ (0 \leq i \leq r - 1) \},
\]
\[
q = \# \{ n \in [0, q^2 - 1] : a(n) + b(n) = q - 1 \},
\]
\[
1 = \# \{ n \in [0, q^2 - 1] : a(n) + b(n) = 2(q - 1) \},
\]
where \([0, q^2 - 1] = \{0, 1, 2, \ldots, q^2 - 1\}\). Therefore we have
\[
\lambda_m = \left( \frac{p(p+1)}{2} \right)^r - q - 1.
\]

\section{The case (II)}

Let \(\alpha \in \mathbb{F}_q\) and \(m(T) = (T - \alpha)^2\). Let \(\varepsilon\) denote the image of \(T - \alpha\) in \(A/mA\). Then \(f(T) \mapsto f(\alpha) + f'(\alpha)\varepsilon\) gives rise to an isomorphism \(A/mA \cong \mathbb{F}_q[\varepsilon]\). It follows that any character \(\chi : (A/mA)\times \to \mathbb{C}\times\) is given by \(f(T) \mapsto \eta(f(\alpha))\psi(f'(\alpha)/f(\alpha))\), where \(\eta\) is a multiplicative character of \(\mathbb{F}_q\), and \(\psi\) is an additive character of \(\mathbb{F}_q\). Furthermore \(s_1(\chi)\) is nothing but the Gauss sum \(G(\eta^{-1}, \psi)\). It is readily seen that

- \(\chi\) is trivial \(\iff \eta\) is trivial and \(\psi\) is trivial,
- \(\deg f_\chi = 1 \iff \eta\) is non-trivial and \(\psi\) is trivial,
- \(f_\chi = m\) and \(\chi\) is real \(\iff \eta\) is trivial and \(\psi\) is non-trivial,
- \(f_\chi = m\) and \(\chi\) is imaginary \(\iff \eta\) is non-trivial and \(\psi\) is non-trivial.

By the equality (2.1), we have
\[
Z_m(u) = \prod (1 + G(\eta^{-1}, \psi)u),
\]
where \(\eta\) runs through all non-trivial multiplicative characters of \(\mathbb{F}_q\), and \(\psi\) runs through all non-trivial additive characters of \(\mathbb{F}_q\).

Let \(p\) be a prime ideal of \(\mathbb{Q}(e^{2\pi i/p}, e^{2\pi i/(q-1)})\) dividing \(p\). If \(\eta\) is non-trivial and \(\psi\) is non-trivial, then we have \(G(\eta^{-1}, \psi) \in p\) by the Stickelberger theorem for Gauss sums (cf. Theorem 11.2.1 in [B-E-W]). Hence we obtain \(\lambda_m = 0\) by Theorem 2.1. This completes the proof of the case (II).

\textbf{Remark.} I appreciate that the referee taught me the above proof. We can generalize the case (II) as follows: \(\lambda_{p^n} = 0 \ (n \geq 0)\) if \(P\) is a monic polynomial of degree one (cf. Proposition 3.2 in [Sh1]).
§ 3.3. The case (III)

Let $\alpha, \beta \in F_q$ (\(\alpha \neq \beta\)) and \(m(T) = (T - \alpha)(T - \beta)\). Then \(f(T) \mapsto (f(\alpha), f(\beta))\) gives rise to an isomorphism \((A/mA)^{\times} \cong F_q^{\times} \times F_q^{\times}\). It follows that any character \(\chi : (A/mA)^{\times} \to \mathbb{C}^{\times}\) is given by \(f(T) \mapsto \chi_1(f(\alpha))\chi_2(f(\beta))\), where \(\chi_1\) and \(\chi_2\) are the multiplicative characters of \(F_q\). Furthermore we have an equality

\[
(3.3) \quad s_1(\chi) = \chi_2(-1)(\chi_1\chi_2)(\alpha - \beta)J(\chi_1, \chi_2),
\]

where \(J(\chi_1, \chi_2)\) denotes the Jacobi sum associated to \(\chi_1\) and \(\chi_2\). It is readily seen that

- \(\chi\) is trivial \(\iff\) \(\chi_1\) and \(\chi_2\) are trivial,
- \(\deg f_\chi = 1\) \(\iff\) one of \(\chi_1\) and \(\chi_2\) is non-trivial and the other is trivial,
- \(f_\chi = m\) and \(\chi\) is real \(\iff\) \(\chi_1\) and \(\chi_2\) are non-trivial and \(\chi_1\chi_2\) is trivial,
- \(f_\chi = m\) and \(\chi\) is imaginary \(\iff\) \(\chi_1, \chi_2\), and \(\chi_1\chi_2\) are non-trivial.

Let \(p\) be a prime ideal of \(\mathbb{Q}(e^{2\pi i/(q-1)})\) above \(p\). Let \(\chi_p = \left(\frac{-}{p}\right)_{q-1}\) be the power residue symbol mod \(p\) of order \(q - 1\). Then we have the following one to one correspondence

\[
\left\{ \chi \in X_m : \chi\text{ is imaginary of conductor } m \right\} \xrightarrow{1:1} \left\{ (\chi_p^{n_1}, \chi_p^{n_2}) : 1 \leq n_1, n_2 \leq q - 2, n_1 + n_2 \not\equiv 0 \mod q - 1 \right\}.
\]

By the equalities (2.1) and (3.3), we have

\[
\lambda_m = \deg(Z_m(u) \mod p) = \sum_{\substack{1 \leq n_1 \leq q - 2 \\ 1 \leq n_2 \leq q - 2 \\ n_1 + n_2 \not\equiv 0 \mod q - 1}} \deg(1 + \chi_p^{n_2}(-1)\chi_p^{n_1+n_2}(\alpha - \beta)J(\chi_p^{n_1}, \chi_p^{n_2})u \mod p).
\]

Next we will calculate \(\text{ord}_p J(\chi_p^{n_1}, \chi_p^{n_2})\), where \(\text{ord}_p\) is the valuation of \(p\). For an integer \(n \in \mathbb{Z}\), we define \(L(n) \in \mathbb{Z}\) as follows

\[
0 \leq L(n) < q - 1, \quad L(n) \equiv n \mod q - 1.
\]

We consider the \(p\)-adic expansion

\[
L(n) = a_0(n) + a_1(n)p + \cdots + a_{r-1}(n)p^{r-1} \quad (0 \leq a_i(n) < p).
\]

Define \(l(n)\) as follows

\[
l(n) = a_0(n) + a_1(n) + \cdots + a_{r-1}(n).
\]
For $1 \leq n_1, n_2 \leq q - 2$ ($n_1 + n_2 \neq q - 1$), it is known as the Stickelberger theorem that
\[
\ord\mathfrak{p} J(\chi_{\mathfrak{p}}^{n_1}, \chi_{\mathfrak{p}}^{n_2}) = r - \frac{l(n_1) + l(n_2) - l(n_1 + n_2)}{p-1} = r - \# \left\{ 0 \leq i \leq r - 1 : L(n_1 p^i) + L(n_2 p^i) > q - 1 \right\}
\]
(cf. Corollary 11.2.4 and Theorem 11.2.9 in [B-E-W]). Noting that
\[
J(\chi_{\mathfrak{p}}^{n_1}, \chi_{\mathfrak{p}}^{n_2})J(\chi_{\mathfrak{p}}^{q-1-n_1}, \chi_{\mathfrak{p}}^{q-1-n_2}) = q,
\]
we obtain
\[
\lambda_m = \# \left\{ (n_1, n_2) \in [1, q-2]^2 : n_1 + n_2 \not\equiv 0 \mod q-1, \quad \ord\mathfrak{p} J(\chi_{\mathfrak{p}}^{n_1}, \chi_{\mathfrak{p}}^{n_2}) = 0 \right\}
= \# \left\{ (n_1, n_2) \in [1, q-2]^2 : n_1 + n_2 \not\equiv 0 \mod q-1, \quad \ord\mathfrak{p} J(\chi_{\mathfrak{p}}^{n_1}, \chi_{\mathfrak{p}}^{n_2}) = r \right\}
= \# \left\{ (n_1, n_2) \in [1, q-2]^2 : n_1 + n_2 \not\equiv 0 \mod q-1, \quad l(n_1) + l(n_2) = l(n_1 + n_2) \right\}
\]
by the Stickelberger theorem. We see that
\[
l(n_1) + l(n_2) = l(n_1 + n_2)
\iff L(n_1 p^{r-1-i}) + L(n_2 p^{r-1-i}) \leq q - 1 \ (i = 0, 1, 2, \ldots, r - 1)
\iff a_i(n_1) + a_i(n_2) \leq p - 1 \ (i = 0, 1, 2, \ldots, r - 1).
\]
Therefore we have
\[
\lambda_m = \# \left\{ (n_1, n_2) \in [1, q-2]^2 : n_1 + n_2 \not\equiv 0 \mod q-1, \quad a_i(n_1) + a_i(n_2) \leq p - 1 \ (0 \leq i \leq r - 1) \right\}.
\]
Notice that
\[
\left( \frac{p(p+1)}{2} \right)^r = \# \left\{ (n_1, n_2) \in [0, q-1]^2 : a_i(n_1) + a_i(n_2) \leq p - 1 \ (0 \leq i \leq r - 1) \right\},
3q - 3 = \# \left\{ (n_1, n_2) \in [0, q-1]^2 : n_1 = 0 \text{ or } n_2 = 0 \text{ or } n_1 + n_2 = q - 1 \right\}.
\]
Hence we have
\[
\lambda_m = \left( \frac{p(p+1)}{2} \right)^r - 3q + 3.
\]

§ 4. A proof of Theorem 1.4

The purpose of this section is to prove Theorem 1.4.
**Lemma 4.1.** Let $m_1, m_2$ be monic polynomials such that $m_1 | m_2$. If $K_{m_2}$ is ordinary, then $K_{m_1}$ is also ordinary.

This follows from the following general result.

**Lemma 4.2.** Let $k$ be a field of characteristic $p$, and let $\pi : Y \rightarrow X$ be a finite covering of projective non-singular curves over $k$. If $Y$ is ordinary, then $X$ is also ordinary.

**Proof.** We give a proof for the reader’s convenience. Let $A$, $B$ be the Jacobians of $X$, $Y$, respectively. Then $\pi$ induces the homomorphism of abelian varieties $\pi^* : A \rightarrow B$, and the embedding of $p$-divisible groups $\pi^* : T_pA \rightarrow T_pB$. Assume that $Y$ is ordinary. Then each slope of $T_pB$ is only 0 or 1. Hence each slope of $T_pA$ is only 0 or 1. Therefore $X$ is also ordinary. \qed

Now we prove Theorem 1.4.

**Proof.** Assume that $\deg m = 1$. Then we have $g_m = \lambda_m = 0$. Hence $K_m$ is ordinary. Conversely, we assume that $K_m$ is ordinary. Let $m = Q_1^{n_1}Q_2^{n_2} \cdots Q_t^{n_t}$ be the irreducible factorization, where $Q_1, Q_2, \ldots, Q_t$ are distinct monic polynomials. By Lemma 4.1, $K_{Q_i^{n_i}}$ is ordinary for each $i$. It follows from Corollary 1.3 and Corollary 3.1 in [Sh2] that $\deg Q_i = 1$ and $n_i = 1$. Now suppose that $t \geq 2$. Again by Lemma 4.1, $K_{Q_1Q_2}$ is ordinary, which contradicts to the second assertion of Corollary 1.3. \qed

**Acknowledgements**

The author wish to thank the referee for many helpful suggestions.

**References**


