ACTA ARITHMETICA
165.3 (2014)

On the ordinarity of the maximal real subfield of cyclotomic function fields

by

Daisuke Shiomi (Yamagata)

1. Introduction. Let p be a prime. Let $\mathbb{F}_q$ be the field with $q = p^r$ elements. For a global function field K over $\mathbb{F}_q$, let J_K be the Jacobian of $K\bar{\mathbb{F}}_q$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. Let g_K be the genus of K. The p-primary subgroup $J_K(p)$ of J_K satisfies

$$J_K(p) \simeq \bigoplus_{i=1}^{\lambda_K} \mathbb{Q}_p/\mathbb{Z}_p.$$

The above integer λ_K is called the *Hasse–Witt invariant* of K, and satisfies $0 \le \lambda_K \le g_K$. In particular, we call K *ordinary* if $\lambda_K = g_K$.

Our aim of this paper is to clarify the ordinarity of cyclotomic function fields. We put $k = \mathbb{F}_q(T)$ and $A = \mathbb{F}_q[T]$. For a monic polynomial $m \in A$, let K_m and K_m^+ be the mth cyclotomic function field and its maximal real subfield, respectively. Let g_m, g_m^+ be the genuses of K_m, K_m^+, respectively. Let λ_m, λ_m^+ be the Hasse–Witt invariants of K_m, K_m^+, respectively. For definitions and properties of cyclotomic function fields, see [Go], [Ha], [Ro].

First, we state our previous results. In the irreducible case, the author showed the following.

Theorem 1.1 (cf. [Sh2]). *Assume that $q \neq p$ and $m \in A$ is monic irreducible. Then:*

(1) *K_m is ordinary if and only if* $\deg m \le 1$.
(2) *K_m^+ is ordinary if and only if* $\deg m \le 2$.

Next we consider the general case. In [Sh3], by using explicit formulas for λ_m in the case of degree two, we showed the following result.

Theorem 1.2 (cf. [Sh3]). *Assume that $q \neq p$ and $m \in A$ is monic. Then K_m is ordinary if and only if* $\deg m = 1$.

2010 *Mathematics Subject Classification*: Primary 11R60; Secondary 14H40.
Key words and phrases: cyclotomic function field, Jacobian.

DOI: 10.4064/aa165-3-2

In this paper, we consider the plus part. Our main theorem is the following.

THEOREM 1.3. *Assume that $q \neq p$ and $m \in A$ is monic. Then K_m^+ is ordinary if and only if* $\deg m \leq 2$.

REMARK 1.4. Theorem 1.3 is not true in the case $q = p$. For example, if we consider $q = 3$ and $m = T^4 + T^2 + 2 \in \mathbb{F}_3[T]$, then K_m^+ is ordinary. Many monic irreducible polynomials m such that K_m^+ is ordinary and $\deg m \geq 3$ have been found in the case $q = p$. However, it is not known whether there are infinitely many such polynomials.

This paper is organized as follows. In Section 2, we review some results on zeta functions and Hasse–Witt invariants. In Section 3, we derive explicit formulas for λ_m^+ in the case of degree three, and show that K_m^+ is not ordinary if $r \geq 2$ and $\deg m = 3$. In Section 4, we prove Theorem 1.3.

2. Preparations

2.1. Zeta functions. In this subsection, we review some results on zeta functions. For the details, see [G-R] and [Ro].

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

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

where $\mathfrak{p}$ runs through all primes of K, and $N\mathfrak{p}$ is the number of elements of the residue class field of $\mathfrak{p}$.

THEOREM 2.1 (cf. [Ro, Theorem 5.9]). *There exist $Z_K(u) \in \mathbb{Z}[u]$ of degree $2g_K$ with $Z_K(0) = 1$ such that*

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

It is well-known that λ_K can be expressed in terms of $Z_K(u)$ as follows.

PROPOSITION 2.2 (cf. [Ro, Proposition 11.20]). *Let $\bar{Z}_K(u) \in \mathbb{F}_p[u]$ be the reduction of $Z_K(u)$ modulo p. Then*

$$\lambda_K = \deg \bar{Z}_K(u).$$

We write

$$Z_K(u) = \prod_{i=1}^{2g_K} (1 - \pi_i u).$$

Let L be a number field containing $\mathbb{Q}(\pi_1, \ldots, \pi_{2g_K})$. Let $\mathcal{P}$ be a prime of L above p, and let $\mathrm{ord}_{\mathcal{P}}$ be the valuation of $\mathcal{P}$ satisfying $\mathrm{ord}_{\mathcal{P}}(L^\times) = \mathbb{Z}$.

Proposition 2.3. *In the above notation,*

$$K \text{ is ordinary} \Leftrightarrow \operatorname{ord}_{\mathcal{P}}(\pi_i) \in \operatorname{ord}_{\mathcal{P}}(q)\mathbb{Z} \ (i = 1, \ldots, 2g_K).$$

Proof. The polynomial $Z_K(u)$ can be written as follows:

$$Z_K(u) = \prod_{i=1}^{g_K} (1 - \pi_i u)(1 - \pi_{i+g_K} u),$$

where $\pi_i \pi_{i+g_K} = q$. Therefore

$$\deg((1 - \pi_i u)(1 - \pi_{i+g_K} u) \bmod \mathcal{P}) \le 1.$$

Hence, by Proposition 2.2,

$$\lambda_K = g_K \Leftrightarrow \operatorname{ord}_{\mathcal{P}}(\pi_i) = 0 \text{ or } \operatorname{ord}_{\mathcal{P}}(\pi_{i+g_K}) = 0 \ (i = 1, \ldots, g_K).$$

This yields Proposition 2.3. ∎

Next 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 the zeta functions of K_m, K_m^+, respectively. By Theorem 2.1, there exist polynomials $Z_m(u)$ and $Z_m^{(+)}(u)$ such that

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

Let X_m be the group of Dirichlet characters modulo m. For $\chi \in X_m$, let f_χ be the conductor of χ. We call χ *real* if $\chi(\mathbb{F}_q^\times) = 1$, and *imaginary* otherwise. Let X_m^+ be the set of all real characters of X_m. Then

$$\zeta(s, K_m) = \Big\{ \prod_{\chi \in X_m} L(s, \chi) \Big\} (1 - q^{-s})^{-[K_m^+ : k]}, \tag{2.1}$$

$$\zeta(s, K_m^+) = \Big\{ \prod_{\chi \in X_m^+} L(s, \chi) \Big\} (1 - q^{-s})^{-[K_m^+ : k]}. \tag{2.2}$$

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

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

where a runs through all monic polynomials of A, and $N(a) = q^{\deg a}$. Here, we view χ as a primitive character when we write $L(s, \chi)$. Let χ_0 be the trivial character. Then $L(s, \chi)$ can be described as follows:

$$L(s, \chi) = \begin{cases} 1/(1 - q^{1-s}) & \text{if } \chi = \chi_0, \\ \sum_{i=0}^{d-1} s_i(\chi) q^{-si} & \text{otherwise,} \end{cases} \tag{2.3}$$

where $s_i(\chi) = \sum_{a:\,\mathrm{monic},\,\deg(a)=i} \chi(a)$. We set

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

where $X_m^- = X_m \backslash X_m^+$. Assume that χ is a non-trivial real character. Then

$$\sum_{i=0}^{d-1} s_i(\chi) = 0.$$

Therefore

$$\varPhi_\chi(u) = \sum_{i=0}^{d-2} s_i^+(\chi)u^i, \quad \text{where} \quad s_i^+(\chi) = \sum_{j=0}^{i} s_j(\chi).$$

Proposition 2.4.

$$Z_m(u) = \prod_{\substack{\chi\in X_m \\ \chi\neq\chi_0}} \varPhi_\chi(u), \qquad Z_m^{(+)}(u) = \prod_{\substack{\chi\in X_m^+ \\ \chi\neq\chi_0}} \varPhi_\chi(u).$$

Proof. This follows from Theorem 2.1 and equalities (2.1)–(2.3). ∎

Remark 2.5. For later use, we consider some special cases. If χ is a non-trivial real character with $\deg f_\chi \le 2$, then $\varPhi_\chi(u) = 1$. Hence we have the following results.

If $\deg m = 3$, then

$$Z_m^{(+)}(u) = \prod_{\substack{\chi\in X_m^+ \\ f_\chi = m}} (1 + s_1^+(\chi)u). \tag{2.4}$$

If $m = Q_1Q_2$ where Q_1, Q_2 are distinct monic irreducible polynomials of degree two, then

$$Z_m^{(+)}(u) = \prod_{\substack{\chi\in X_m^+ \\ f_\chi = m}} (1 + s_1^+(\chi)u + s_2^+(\chi)u^2). \tag{2.5}$$

Proposition 2.6. *Let $m_1, m_2 \in A$ be monic polynomials with $m_1 \mid m_2$.*

(1) *If K_{m_2} is ordinary, then K_{m_1} is ordinary.*
(2) *If $K_{m_2}^+$ is ordinary, then $K_{m_1}^+$ is ordinary.*

Proof. By Proposition 2.4, we see that $Z_{m_1}(u) \mid Z_{m_2}(u)$ and $Z_{m_1}^{(+)}(u) \mid Z_{m_2}^{(+)}(u)$. Hence Proposition 2.6 follows from Proposition 2.3. ∎

2.2. The Hasse–Witt invariant. Let $m \in A$ be a monic irreducible polynomial of degree d. For $0 \le i \le d-1$, we set

$$s_i(n) = \sum_{a \in A_i} a^n, \qquad s_i^+(n) = \sum_{j=0}^{i} s_j(n),$$

where A_i is the set of monic polynomials in A of degree i. For $1 \le n \le q^d - 2$, we define $B_n(u) \in A[u]$ by

$$B_n(u) = \begin{cases} \sum_{i=0}^{d-2} s_i^+(n)u^i & \text{if } n \equiv 0 \bmod q-1, \\ \sum_{i=0}^{d-1} s_i(n)u^i & \text{if } n \not\equiv 0 \bmod q-1. \end{cases} \tag{2.6}$$

In a previous work, the author showed that λ_m and λ_m^+ can be expressed via $B_n(u)$. In this subsection, we review these results. For more details, see [Sh2].

Let us 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 $\sigma : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$. Via this embedding, we regard $\bar{\mathbb{Q}} \subseteq \bar{\mathbb{Q}}_p$. Let ord_p be 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 $(q^d - 1)$th roots of unity. 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 q^d elements.

Let $\mathcal{R}_m = A/mA$. Then the cardinality of $\mathcal{R}_m$ is q^d. Hence $\mathcal{R}_m$ is isomorphic to $\mathcal{F}_M$. Fix an isomorphism $\phi : \mathcal{R}_m \to \mathcal{F}_M$. This map induces a group isomorphism $\phi_\# : \mathcal{R}_m^\times \to \mathcal{F}_M^\times$, and a ring isomorphism $\phi_* : \mathcal{R}_m[u] \to \mathcal{F}_M[u]$. Since the cardinality of W is prime to p, we have the isomorphism

$$\tau : W \to \mathcal{F}_M^\times \ (\zeta \mapsto \zeta \bmod p\mathcal{O}_M).$$

Put $\omega = \tau^{-1} \circ \phi_\#$. Then ω is a generator of X_m. We see that $\omega^n \in X_m^+$ if and only if $n \equiv 0 \bmod q-1$. Notice that

$$\phi(a^n \bmod mA) \equiv \omega^n(a \bmod mA) \bmod p\mathcal{O}_M \tag{2.7}$$

for $a \in A$. Hence

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

where $\bar{\Phi}_{\omega^n}(u) = \Phi_{\omega^n}(u) \bmod p\mathcal{O}_M$ and $\bar{B}_n(u) = B_n(u) \bmod m$. From Proposition 2.4, we obtain the following results.

Proposition 2.7.

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

Therefore, by Proposition 2.2, we have the following relations between the Hasse–Witt invariant and $B_n(u)$.

COROLLARY 2.8.

$$\lambda_m = \sum_{n=1}^{q^d-2} \deg \bar{B}_n(u), \qquad \lambda_m^+ = \sum_{\substack{n=1 \\ n\equiv 0 \bmod q-1}}^{q^d-2} \deg \bar{B}_n(u).$$

3. Explicit formulas for λ_m^+ in the case of degree three. In this section, we derive explicit formulas for λ_m^+ in the case of degree three. As an application, we show that K_m^+ is not ordinary if $q \neq p$ and $\deg m = 3$.

THEOREM 3.1. *Assume that $m \in A$ is monic and $q = p^r$. Let $m = Q_1^{n_1} \cdots Q_t^{n_t}$ be the irreducible decomposition of m. Let $d_i = \deg Q_i$.*

(1) *If $\deg m \le 2$, then $\lambda_m^+ = 0$.*

(2) *If $\deg m = 3$, then*

$$\lambda_m^+ = \begin{cases} 0 & \text{if } m = Q_1^3 \text{ and } d_1 = 1, & \text{(I)} \\ 0 & \text{if } m = Q_1^2 Q_2 \text{ and } d_1 = d_2 = 1, & \text{(II)} \\ (p(p+1)/2)^r - 3q + 3 & \\ & \text{if } m = Q_1Q_2Q_3 \text{ and } d_1 = d_2 = d_3 = 1, & \text{(III)} \\ (p(p+1)/2)^r - q - 1 & \text{if } m = Q_1Q_2,\ d_1 = 2, \text{ and } d_2 = 1, & \text{(IV)} \\ (p(p+1)/2)^r & \text{if } m = Q_1 \text{ and } d_1 = 3. & \text{(V)} \end{cases}$$

REMARK 3.2. Assume that $\deg m \le 2$. By the Kida–Murabayashi formula, we have $g_m^+ = 0$ (cf. [K-M, Corollary 1]). Hence $\lambda_m^+ = 0$. This proves Theorem 3.1(1).

REMARK 3.3. Cases (I) and (II) follow from more general results (cf. [Sh1, Theorem 1.1]):

(I) $\lambda_{Q_1^n}^+ = 0$ if $d_1 = 1$ and $n \ge 0$,

(II) $\lambda_{Q_1^n Q_2}^+ = 0$ if $d_1 = d_2 = 1$ and $n \ge 0$.

We give a sketch of the proof of (I) for the reader's convenience. By the Kida–Murabayashi formula, we have $g_{Q_1}^+ = 0$. Hence $\lambda_{Q_1}^+ = 0$. We notice that $K_{Q_1^n}^+/K_{Q_1}^+$ is a Galois p-extension. Therefore, by applying the Deuring–Shafarevich formula in $K_{Q_1^n}^+/K_{Q_1}^+$, we obtain $\lambda_{Q_1^n}^+ = q^n \lambda_{Q_1}^+$. Hence $\lambda_{Q_1^n}^+ = 0$.

By the same argument, we deduce (II).

REMARK 3.4. If $\deg m \ge 4$, then λ_m^+ is not determined only from the irreducible decomposition of m. For example, consider $q = 3$, $m_1 = T^4 + T + 2$, and $m_2 = T^4 + T^2 + 2$. Then $m_1, m_2 \in \mathbb{F}_3[T]$ are both irreducible monic polynomials of degree four. However, $\lambda_{m_1}^+ = 38$ and $\lambda_{m_2}^+ = 39$.

By the Kida–Murabayashi formula, we can calculate g_m^+ as follows:

$$g_m^+ = \begin{cases} q(q-1)/2 & \text{if } m = Q_1^3 \text{ and } d_1 = 1, & \text{(I)} \\ (q-2)(q-1)/2 & \text{if } m = Q_1^2 Q_2 \text{ and } d_1 = d_2 = 1, & \text{(II)} \\ q(q+1)/2 - 3q + 3 & \text{if } m = Q_1 Q_2 Q_3 \text{ and } d_1 = d_2 = d_3 = 1, & \text{(III)} \\ q(q+1)/2 - q - 1 & \text{if } m = Q_1 Q_2,\ d_1 = 2, \text{ and } d_2 = 1, & \text{(IV)} \\ q(q+1)/2 & \text{if } m = Q_1 \text{ and } d_1 = 3. & \text{(V)} \end{cases}$$

By comparing g_m^+ and λ_m^+, we obtain the following result.

COROLLARY 3.5. *Assume that $q \neq p$ and $\deg m = 3$. Then K_m^+ is not ordinary.*

REMARK 3.6. The above corollary does not hold for $q = p$. For example, by comparing g_m^+ and λ_m^+, we see that K_m^+ is ordinary in cases (III)–(V) if $q = p$.

3.1. Case (III). Let $m = (T-\alpha)(T-\beta)(T-\gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_q$ are distinct. Then we have the isomorphism

$$(A/mA)^\times \to (\mathbb{F}_q^\times)^3 \ (a(T) \bmod m \mapsto (a(\alpha), a(\beta), a(\gamma))).$$

Hence any character $\chi : (A/mA)^\times \to \mathbb{C}^\times$ can be given by

$$a(T) \bmod m \mapsto \chi_1(a(\alpha))\chi_2(a(\beta))\chi_3(a(\gamma)),$$

where $\chi_1,\ \chi_2,\ \chi_3$ are characters of $\mathbb{F}_q^\times$. We see that $\chi_3^{-1} = \chi_1\chi_2$ if χ is real. Hence we have the following one-to-one correspondence:

$$\{\chi \in X_m^+ : f_\chi = m\} \overset{1:1}{\longleftrightarrow} \left\{ (\chi_1, \chi_2) \in (\widehat{\mathbb{F}_q^\times})^2 : \begin{matrix} \chi_1,\ \chi_2,\ \chi_1\chi_2 \\ \text{are non-trivial} \end{matrix} \right\}. \tag{3.1}$$

Take $\chi \in X_m^+$ corresponding to (χ_1, χ_2). Then

$$\begin{aligned} s_1^+(\chi) &= 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha, \beta, \gamma}} \chi(T-a) \\ &= 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha, \beta, \gamma}} \chi_1\left(\frac{a-\alpha}{a-\gamma}\right)\chi_2\left(\frac{a-\beta}{a-\gamma}\right) \\ &= \chi_1(1-\tau)\chi_2(1-1/\tau)J(\chi_1, \chi_2), \end{aligned} \tag{3.2}$$

where $\tau = (\alpha-\gamma)/(\beta-\gamma)$ and $J(\chi_1, \chi_2)$ is the Jacobi sum defined by

$$J(\chi_1, \chi_2) = \sum_{\substack{a \in \mathbb{F}_q \\ a \neq 0,1}} \chi_1(a)\chi_2(1-a).$$

Let $K = \mathbb{Q}(e^{2\pi i/(q-1)})$ and $\mathcal{O}_K$ the ring of integers of K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p. Since r is the relative degree of p in $K/\mathbb{Q}$ (recall that $q = p^r$), we see that $\mathbb{F}_q$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}$. Fix an isomorphism $\theta : \mathbb{F}_q \to \mathcal{O}_K/\mathfrak{p}$. We define an isomorphism ϕ by

$$\phi : W \to (\mathcal{O}_K/\mathfrak{p})^\times \ (\zeta \mapsto \zeta \bmod \mathfrak{p}),$$

where W is the group of $(q-1)$th roots of unity. We define $\chi_\mathfrak{p}$ by

$$\chi_\mathfrak{p} : \mathbb{F}_q^\times \to W \ (x \mapsto \phi^{-1}(\theta(x))).$$

Then $\chi_\mathfrak{p}$ is a generator of $\widehat{\mathbb{F}_q^\times}$. Therefore, by (3.1), we have the following one-to-one correspondence:

$$\{\chi \in X_m^+ : f_\chi = m\} \overset{1:1}{\longleftrightarrow} \left\{ (\chi_\mathfrak{p}^{n_1}, \chi_\mathfrak{p}^{n_2}) : \begin{array}{l} 1 \le n_1, n_2 \le q-2, \\ n_1 + n_2 \not\equiv 0 \bmod q-1 \end{array} \right\}.$$

Take $\chi \in X_m^+$ corresponding to $(\chi_\mathfrak{p}^{n_1}, \chi_\mathfrak{p}^{n_2})$. By (3.2), we have

$$s_1^+(\chi) \notin \mathfrak{p} \ \Leftrightarrow \ \mathrm{ord}_\mathfrak{p}(J(\chi_\mathfrak{p}^{n_1}, \chi_\mathfrak{p}^{n_2})) = 0.$$

By (2.4) and Proposition 2.2,

$$\lambda_m^+ = \# \left\{ (n_1, n_2) \in [1, q-2]^2 : \begin{array}{l} n_1 + n_2 \not\equiv 0 \bmod q-1, \\ \mathrm{ord}_\mathfrak{p}(J(\chi_\mathfrak{p}^{n_1}, \chi_\mathfrak{p}^{n_2})) = 0 \end{array} \right\},$$

where $[1, q-2] = \{1, \ldots, q-2\}$.

Next we investigate the value of $\mathrm{ord}_\mathfrak{p}(J(\chi_\mathfrak{p}^{n_1}, \chi_\mathfrak{p}^{n_2}))$. For $n \in \mathbb{Z}$, we define $L(n) \in \mathbb{Z}$ as follows:

$$0 \le L(n) < q-1, \qquad L(n) \equiv n \bmod q-1.$$

Consider the p-adic expansion

$$L(n) = a_0(n) + a_1(n)p + \cdots + a_{r-1}(n)p^{r-1} \qquad (0 \le a_i(n) < p),$$

and put

$$l(n) = a_0(n) + a_1(n) + \cdots + a_{r-1}(n).$$

By the Stickelberger theorem for Jacobi sums, we obtain

$$\begin{aligned} \mathrm{ord}_\mathfrak{p}(J(\chi_\mathfrak{p}^{n_1}, \chi_\mathfrak{p}^{n_2})) &= r - \frac{l(n_1) + l(n_2) - l(n_1+n_2)}{p-1} \\ &= r - \#\{0 \le i \le r-1 : L(n_1 p^i) + L(n_2 p^i) > q-1\} \end{aligned}$$

for $1 \le n_1, n_2 \le q-2$ and $n_1 + n_2 \ne q-1$ (cf. [B-E-W, Corollary 11.2.4 and Theorem 11.2.9]). 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 have

$$\begin{aligned}\lambda_m^+ &= \#\left\{(n_1,n_2)\in[1,q-2]^2 : \begin{matrix} n_1+n_2\not\equiv 0 \bmod q-1, \\ \mathrm{ord}_{\mathfrak{p}}(J(\chi_{\mathfrak{p}}^{n_1},\chi_{\mathfrak{p}}^{n_2}))=r \end{matrix}\right\} \\ &= \#\left\{(n_1,n_2)\in[1,q-2]^2 : \begin{matrix} n_1+n_2\not\equiv 0 \bmod q-1, \\ l(n_1)+l(n_2)=l(n_1+n_2) \end{matrix}\right\}.\end{aligned}$$

We see that

$$\begin{aligned}&l(n_1)+l(n_2)=l(n_1+n_2) \\ &\qquad\Leftrightarrow\ L(n_1p^{r-1-i})+L(n_2p^{r-1-i})\le q-1\ (0\le i\le r-1) \\ &\qquad\Leftrightarrow\ a_i(n_1)+a_i(n_2)\le p-1\ (0\le i\le r-1).\end{aligned}$$

Hence

$$\lambda_m^+ = \#\left\{(n_1,n_2)\in[1,q-2]^2 : \begin{matrix} n_1+n_2\not\equiv 0 \bmod q-1, \\ a_i(n_1)+a_i(n_2)\le p-1\ (0\le i\le r-1) \end{matrix}\right\}.$$

Now,

$$\begin{aligned}&(p(p+1)/2)^r \\ &\qquad = \#\{(n_1,n_2)\in[0,q-1]^2 : a_i(n_1)+a_i(n_2)\le p-1\ (0\le i\le r-1)\}, \\ &3q-3 = \#\{(n_1,n_2)\in[0,q-1]^2 : n_1=0 \text{ or } n_2=0 \text{ or } n_1+n_2=q-1\}.\end{aligned}$$

Therefore

$$\lambda_m^+ = (p(p+1)/2)^r - 3q+3.$$

3.2. Case (IV). Let $m=m_0(T-\alpha)$ where $\alpha\in\mathbb{F}_q$ and $m_0\in A$ is a monic irreducible polynomial of degree two. Then we have the isomorphism

$$(A/mA)^\times \to (A/m_0A)^\times\times\mathbb{F}_q^\times\ (a(T) \bmod m \mapsto (a(T) \bmod m_0, a(\alpha))).$$

Hence any character $\chi:(A/mA)^\times\to\mathbb{C}^\times$ can be given by

$$a(T) \bmod m \mapsto \chi_1(a(T) \bmod m_0)\chi_2(a(\alpha)),$$

where χ_1 is a character of $(A/m_0A)^\times$, and χ_2 is a character of $\mathbb{F}_q^\times$. If χ is real, then $\chi_2=(\chi_1|_{\mathbb{F}_q^\times})^{-1}$. Hence we have the following one-to-one correspondence:

$$\{\chi\in X_m^+ : f_\chi=m\} \xleftrightarrow{1:1} \{\chi_1\in X_{m_0}^- : f_{\chi_1}=m_0\}.$$

Take $\chi\in X_m^+$ corresponding to $\chi_1\in X_{m_0}^-$. Then

$$\begin{aligned} s_1^+(\chi) &= 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha}} \chi(T-a) = 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha}} \chi_1(T-a)\chi_2(\alpha - a) \\ &= 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha}} \chi_1\left(\frac{T-a}{\alpha - a}\right). \end{aligned}$$

Let ω be the generator of X_{m_0} defined in Subsection 2.2. Take $n \in [1, q^2-2]$ such that $\chi_1 = \omega^n$. Since χ_1 is imaginary, we have $n \not\equiv 0 \bmod q-1$. By (2.7), we have

$$s_1^+(\chi) \in p\mathcal{O}_M \iff 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha}} \left(\frac{T-a}{\alpha - a}\right)^n \in m_0 A. \tag{3.3}$$

Lemma 3.7. *For* $1 \leq n \leq q^2 - 2$ $(n \not\equiv 0 \bmod q-1)$, *set*

$$f_n(T) = 1 + \sum_{\substack{a \in \mathbb{F}_q \\ a \neq \alpha}} \left(\frac{T-a}{\alpha - a}\right)^n.$$

Consider the q-adic expansion $n = a(n) + b(n)q$ $(0 \leq a(n), b(n) \leq q-1)$. *Then*

$$f_n(T) \notin m_0 A \iff \binom{b(n)}{q-1-a(n)} \not\equiv 0 \bmod p,$$

where $\binom{*}{*}$ *is a binomial coefficient.*

Proof. We put $g_n(T) = T^n f_n(1/T + \alpha)$. Then

$$\text{(i) } g_n(T) = \sum_{a \in \mathbb{F}_q} (T+a)^n, \qquad \text{(ii) } f_n(T) = (T-\alpha)^n g_n\left(\frac{1}{T-\alpha}\right).$$

Gekeler [Ge, Corollary 3.14] established the following equality:

$$g_n(T) = \begin{cases} -\binom{b(n)}{q-1-a(n)} (T^q - T)^{i(n)} & \text{if } a(n) + b(n) > q-1, \\ 0 & \text{if } a(n) + b(n) < q-1, \end{cases}$$

where $i(n) = a(n) + b(n) - (q-1)$. Hence

$$g_n(T) \notin m_1 A \iff \binom{b(n)}{q-1-a(n)} \not\equiv 0 \bmod p$$

for any irreducible polynomial m_1 of degree two. Therefore, by (ii), we obtain Lemma 3.7 . ∎

By Proposition 2.2 and Lemma 3.7 and the equalities (2.4) and (3.3), we have

$$\lambda_m^+ = \#\left\{1 \le n \le q^2-2 : \begin{array}{c} n \not\equiv 0 \bmod q-1, \\ \binom{b(n)}{q-1-a(n)} \not\equiv 0 \bmod p \end{array}\right\}. \tag{3.4}$$

For $1 \le n \le q^2-2$ ($n \not\equiv 0 \bmod q-1$), we write

$$a(n) = a_0(n) + a_1(n)p + \cdots + a_{r-1}(n)p^{r-1},$$
$$b(n) = b_0(n) + b_1(n)p + \cdots + b_{r-1}(n)p^{r-1},$$

where $0 \le a_i(n), b_i(n) \le p-1$ ($i = 0, 1, \ldots, r-1$). Noting that

$$q-1-a(n) = \sum_{i=0}^{r-1}(p-1-a_i(n))p^i,$$

we have

$$\binom{b(n)}{q-1-a(n)} \equiv \prod_{i=0}^{r-1}\binom{b_i(n)}{p-1-a_i(n)} \bmod p.$$

Hence

$$\binom{b(n)}{q-1-a(n)} \not\equiv 0 \bmod p \Leftrightarrow a_i(n)+b_i(n) \ge p-1 \ (0 \le i \le r-1).$$

Therefore the equality (3.4) can be written as follows:

$$\lambda_m^+ = \#\left\{1 \le n \le q^2-2 : \begin{array}{l} n \not\equiv 0 \bmod q-1, \\ a_i(n)+b_i(n) \ge p-1 \ (0 \le i \le r-1) \end{array}\right\}.$$

We see that

$$(p(p+1)/2)^r = \#\{n \in [0, q^2-1] : a_i(n)+b_i(n) \ge p-1 \ (0 \le i \le r-1)\},$$
$$q = \#\{n \in [0, q^2-1] : a(n)+b(n) = q-1\},$$
$$1 = \#\{n \in [0, q^2-1] : a(n)+b(n) = 2(q-1)\}.$$

Hence we obtain

$$\lambda_m^+ = (p(p+1)/2)^r - q - 1.$$

3.3. Case (V). Let m be a monic irreducible polynomial of degree three. For $n \in [1, q^3-2]$ ($n \equiv 0 \bmod q-1$), we see that $1+s_1(n)+s_2(n) = 0$ (cf. [Ge, Lemma 6.1]). Therefore

$$B_n(u) = 1 + s_1^+(n)u = 1 - s_2(n)u.$$

By Corollary 2.8, we have

$$\lambda_m^+ = \#\left\{1 \le n \le q^3-2 : \begin{array}{c} n \equiv 0 \bmod q-1, \\ s_2(n) \not\equiv 0 \bmod m \end{array}\right\}.$$

For $n \in [1, q^3-2]$ ($n \equiv 0 \bmod q-1$), consider the q-adic expansion

$$n = a(n) + b(n)q + c(n)q^2 \quad (0 \le a(n), b(n), c(n) < q).$$

Put $l(n) = a(n) + b(n) + c(n)$. Then $l(n) = q-1$ or $2(q-1)$. If $l(n) = q-1$, then $s_2(n) = 0$ (cf. [Ge, Corollary 2.12]). If $l(n) = 2(q-1)$, then Gekeler [Ge, Theorem 3.13]) proved the equality

$$s_2(n) = (-1)^{a(n)} \binom{c(n)}{q-1-a(n)} (T^q - T)^{i(n)} (T^{q^2} - T)^{j(n)},$$

where the integers $i(n)$, $j(n)$ are defined by

$$\begin{aligned} i(n) &= a(n) + b(n) + q(b(n) + c(n)) - (q^2 - 1), \\ j(n) &= a(n) + c(n) - (q-1). \end{aligned}$$

Since m is irreducible of degree three, we have

$$s_2(n) \notin mA \ \Leftrightarrow \ \binom{c(n)}{q-1-a(n)} \not\equiv 0 \bmod p.$$

Therefore

$$\lambda_m^+ = \# \left\{ 1 \le n \le q^3 - 2 : \begin{array}{l} l(n) = 2(q-1), \\ \binom{c(n)}{q-1-a(n)} \not\equiv 0 \bmod p \end{array} \right\}.$$

By the same argument of case (IV), we can calculate the right side of the above equality to obtain

$$\lambda_m^+ = (p(p+1)/2)^r.$$

4. Proof of Theorem 1.3. In this section, we prove Theorem 1.3. The difficult point is to show that K_m^+ is not ordinary when m is a product of two distinct irreducible polynomials of degree two (see Subsection 4.2).

Assume that $q \neq p$. By Theorem 1.1 and Proposition 2.6, K_m^+ is not ordinary if m has a prime factor Q with $\deg Q \ge 3$. Hence we can assume that the irreducible decomposition of m is

$$m = Q_1^{n_1} \cdots Q_t^{n_t},$$

where each Q_i is monic with $d_i = \deg Q_i \le 2$. If we can show that K_m^+ is not ordinary in the following two cases: (VI) $m = Q_1^2$ ($d_1 = 2$), (VII) $m = Q_1 Q_2$ ($d_1 = d_2 = 2$), then we obtain Theorem 1.3 by Proposition 2.6 and Corollary 3.5.

4.1. Case (VI). If $m = Q_1^2$ ($d_1 = 2$), by applying the Deuring–Shafarevich formula in $K_{Q_1^2}^+/K_{Q_1}^+$, we have

$$\lambda_{Q_1^2}^+ = \lambda_{Q_1}^+ q^2 + q^2 - 1$$

(cf. [Sh1, Subsection 3.2]). Since $d_1 = 2$, we have $\lambda_{Q_1}^+ = 0$. Hence $\lambda_{Q_1^2}^+ = q^2 - 1$. On the other hand, the genus $g_{Q_1^2}^+$ can be calculated as follows:

$$g_{Q_1^2}^+ = (q^2 - 1)(q + 1)$$

(cf. [K-M]). Hence $K_{Q_1^2}^+$ is not ordinary.

4.2. Case (VII). If $m = Q_1Q_2$ $(d_1 = d_2 = 2)$, we see that

$$(A/mA)^\times \simeq (A/Q_1A)^\times \times (A/Q_2A)^\times.$$

This leads to the following isomorphism of character groups:

$$\widehat{(A/mA)^\times} \simeq \widehat{(A/Q_1A)^\times} \times \widehat{(A/Q_2A)^\times}.$$

Hence we have the following one-to-one correspondence:

$$\{\chi \in X_m^+ : f_\chi = m\} \overset{1:1}{\longleftrightarrow} \left\{ (\chi_1, \chi_2) \in X_{Q_1} \times X_{Q_2} : \begin{array}{l} f_{\chi_1} = Q_1,\ f_{\chi_2} = Q_2, \\ \chi_1\chi_2 \text{ is real} \end{array} \right\}.$$

Define $Q_1 = T^2 + u_1T + u_2$ and $Q_2 = T^2 + v_1T + v_2$ $(u_1, u_2, v_1, v_2 \in \mathbb{F}_q)$. Let $\chi \in X_m^+$ correspond to $(\chi_1, \chi_2) \in X_{Q_1} \times X_{Q_2}$.

LEMMA 4.1. *Assume that $u_1 = v_1$. Then*

$$s_2^+(\chi) = \begin{cases} s_1(\chi_1)s_1(\chi_2) & \text{if } \chi_1 \text{ is imaginary,} \\ q & \text{if } \chi_1 \text{ is real.} \end{cases}$$

LEMMA 4.2. *Assume that $u_1 \neq v_1$. Set $\varepsilon = (u_2 - v_2)/(u_1 - v_1)$, $\alpha = u_1 - \varepsilon$, and $\beta = v_1 - \varepsilon$. Then*

$$\chi_1(T+\alpha)\chi_2(T+\beta)s_2^+(\chi) = \begin{cases} s_1(\chi_1)s_1(\chi_2) & \text{if } \chi_1 \text{ is imaginary,} \\ q & \text{if } \chi_1 \text{ is real.} \end{cases}$$

Let $M = \mathbb{Q}(e^{2\pi i/(q^2-1)})$, and let $\mathfrak{p}$ be a prime ideal of M above p. We set

$$L = \mathbb{Q}(\pi_1, \ldots, \pi_{2g_m^+}, e^{2\pi i/(q^2-1)}),$$

where $Z_m^{(+)}(u) = \prod_{i=1}^{2g_m^+}(1 - \pi_i u)$. Let $\mathcal{P}$ be a prime ideal of L over $\mathfrak{p}$.

PROPOSITION 4.3. *Assume that χ_1 is imaginary. Then*

$$\mathrm{ord}_{\mathcal{P}}(s_2^+(\chi)) = \mathrm{ord}_{\mathcal{P}}(s_1(\chi_1)) + \mathrm{ord}_{\mathcal{P}}(s_1(\chi_2)).$$

Proof. This follows from Lemmas 4.1 and 4.2. ∎

Proof of Lemma 4.1. We see that

$$\begin{aligned} s_2(\chi) &= \sum_{a,b\in\mathbb{F}_q} \chi(T^2 + aT + b) \\ &= \sum_{a,b\in\mathbb{F}_q} \chi_1((a-u_1)T + (b-u_2))\chi_2((a-u_1)T + (b-v_2)) = H + I, \end{aligned}$$

where

$$H = \sum_{\substack{a\in\mathbb{F}_q\\ a\neq 0}} \sum_{b\in\mathbb{F}_q} \chi_1(aT+b)\chi_2(aT+b+u_2-v_2),$$
$$I = \sum_{b\in\mathbb{F}_q} \chi_1(b)\chi_2(b+u_2-v_2).$$

Notice that $u_2 \neq v_2$. If χ_1 is real, then $s_1(\chi_1) = s_1(\chi_2) = -1$. Hence

$$H = \begin{cases} s_1(\chi_1)s_1(\chi_2) - s_1(\chi) & \text{if } \chi_1 \text{ is imaginary,}\\ 1 - s_1(\chi) & \text{if } \chi_1 \text{ is real,}\end{cases}$$
$$I = \begin{cases} -1 & \text{if } \chi_1 \text{ is imaginary,}\\ q-2 & \text{if } \chi_1 \text{ is real.}\end{cases}$$

This proves Lemma 4.1. ∎

Proof of Lemma 4.2. We see that

$$\begin{aligned}&(T+\alpha)(T^2+aT+b)\\ &\qquad \equiv (-\varepsilon(a-u_1)+b-u_2)T-(a-u_1)u_2+\alpha(b-u_2) \bmod Q_1,\\ &(T+\beta)(T^2+aT+b)\\ &\qquad \equiv (-\varepsilon(a-v_1)+b-v_2)T-(a-v_1)v_2+\beta(b-v_2) \bmod Q_2.\end{aligned}$$

Noting that

$$-\varepsilon(a-u_1)+b-u_2 = -\varepsilon(a-v_1)+b-v_2,$$

we have

$$\begin{aligned}&\chi_1(T+\alpha)\chi_2(T+\beta)s_2(\chi)\\ &\qquad = \sum_{a,b\in\mathbb{F}_q} \chi_1\big((-\varepsilon(a-u_1)+b-u_2)T-(a-u_1)u_2+\alpha(b-u_2)\big)\\ &\qquad\qquad \times \chi_2\big((-\varepsilon(a-u_1)+b-u_2)T-(a-v_1)v_2+\beta(b-v_2)\big)\\ &\qquad = \sum_{a,b\in\mathbb{F}_q} \chi_1(bT+a(-u_2+\alpha\varepsilon)+b\alpha)\\ &\qquad\qquad \times \chi_2\big(bT+a(-v_2+\beta\varepsilon)+b\beta-v_2(u_1-v_1)+\beta(u_2-v_2)\big)\\ &\qquad = H+I,\end{aligned}$$

where

$$H = \sum_{\substack{a,b\in\mathbb{F}_q\\ b\neq 0}} \chi_1(bT+a\gamma+b\alpha)\chi_2(bT+a\gamma+b\beta+\delta),$$
$$I = \sum_{a\in\mathbb{F}_q} \chi_1(a\gamma)\chi_2(a\gamma+\delta).$$

Here, $\gamma = -u_2 + \alpha\varepsilon = -v_2 + \beta\varepsilon$ and $\delta = -v_2(u_1 - v_1) + \beta(u_2 - v_2)$. Notice that $\gamma \neq 0$ and $\delta \neq 0$. Hence

$$H = \begin{cases} s_1(\chi_1)s_1(\chi_2) - J & \text{if } \chi_1 \text{ is imaginary,} \\ 1 - J & \text{if } \chi_1 \text{ is real,} \end{cases}$$

$$I = \begin{cases} -1 & \text{if } \chi_1 \text{ is imaginary,} \\ q - 2 & \text{if } \chi_1 \text{ is real,} \end{cases}$$

where

$$J = \sum_{a \in \mathbb{F}_q} \chi_1(T + a)\chi_2(T + a + v_1 - u_1).$$

On the other hand, we see that

$$\begin{aligned} (T + \alpha)(T + a) &\equiv (a - \varepsilon)T + a\alpha - u_2 \bmod Q_1, \\ (T + \beta)(T + a) &\equiv (a - \varepsilon)T + a\beta - v_2 \bmod Q_2. \end{aligned}$$

Hence we have

$$\begin{aligned} &\chi_1(T + \alpha)\chi_2(T + \beta)(1 + s_1(\chi)) \\ &\quad = \chi_1(T + \alpha)\chi_2(T + \beta) \\ &\qquad + \sum_{a \in \mathbb{F}_q} \chi_1((a - \varepsilon)T + a\alpha - u_2)\chi_2((a - \varepsilon)T + a\beta - v_2) \\ &\quad = \chi_1(T + \alpha)\chi_2(T + \beta) + \sum_{a \in \mathbb{F}_q} \chi_1(aT + a\alpha + \gamma)\chi_2(aT + a\beta + \gamma) \\ &\quad = 1 + \sum_{a \in \mathbb{F}_q} \chi_1(T + a)\chi_2(T + a + v_1 - u_1) = 1 + J. \end{aligned}$$

This yields Lemma 4.2. ∎

Now we prove Theorem 1.3. Assume that $r \geq 2$. We see that A/Q_1A, A/Q_2A, and $\mathcal{O}_M/\mathfrak{p}$ are finite fields of the same cardinality. Fix isomorphisms

$$\sigma_1 : A/Q_1A \to \mathcal{O}_M/\mathfrak{p}, \qquad \sigma_2 : A/Q_2A \to \mathcal{O}_M/\mathfrak{p}.$$

Define an isomorphism τ by

$$\tau : W_{q^2-1} \to (\mathcal{O}_M/\mathfrak{p})^\times \ (\zeta \mapsto \zeta \bmod \mathfrak{p}).$$

Set

$$\omega_1 = \tau^{-1} \circ \sigma_1|_{(A/Q_1A)^\times}, \qquad \omega_2 = \tau^{-1} \circ \sigma_2|_{(A/Q_2A)^\times}.$$

Then ω_1, ω_2 are generators of X_{Q_1}, X_{Q_2}, respectively.

Lemma 4.4.

$$s_1(n) \equiv 0 \bmod Q_1 \ \Leftrightarrow\ s_1(\omega_1^n) \in \mathcal{P},$$
$$s_1(n) \equiv 0 \bmod Q_2 \ \Leftrightarrow\ s_1(\omega_2^n) \in \mathcal{P}.$$

Proof. This follows from $s_1(\omega_1^n) \equiv \sigma_1(s_1(n) \bmod Q_1) \bmod \mathfrak{p}$, and $s_1(\omega_2^n) \equiv \sigma_2(s_1(n) \bmod Q_2) \bmod \mathfrak{p}$. ∎

Let γ_1 be a generator of $(A/Q_1A)^\times$. Write $\alpha = \gamma_1^{q+1}$ and $\zeta = \omega_1(\gamma_1)$. Then α is a generator of $\mathbb{F}_q^\times$, and ζ is a primitive (q^2-1)th root of unity.

Lemma 4.5. *There exists a generator $\gamma_2 \in (A/Q_2A)^\times$ such that $\gamma_2^{q+1} = \alpha$.*

Proof. Let γ be a generator of $(A/Q_2A)^\times$. Since γ^{q+1} is a generator of $\mathbb{F}_q^\times$, we can take $i_0 \in \mathbb{Z}$ such that $\gamma^{(q+1)i_0} = \alpha$. We notice that $\gcd(i_0, q-1) = 1$. The map

$$(\mathbb{Z}/(q^2-1))^\times \to (\mathbb{Z}/(q-1))^\times \ (x \bmod (q^2-1) \mapsto x \bmod (q-1))$$

is surjective. Hence we can take $i \in \mathbb{Z}$ such that

$$i \equiv i_0 \bmod q-1, \qquad \gcd(i, q^2-1) = 1.$$

Set $\gamma_2 = \gamma^i$. Then γ_2 is a generator of $(A/Q_2A)^\times$ such that $\gamma_2^{q+1} = \alpha$. ∎

Take $n \in \mathbb{Z}$ such that $\zeta^n = \omega_2(\gamma_2)$. Then ζ^n is a primitive (q^2-1)th root of unity. Therefore $\gcd(n, q^2-1) = 1$. Take $m_1 \in \mathbb{Z}$ such that

$$1 \le m_1 \le q^2-2, \qquad nm_1 \equiv (q-p^{r-1}) + p^{r-1}q \bmod q^2-1.$$

Since $l((p-1)+q) = p < q-1$ (definition of $l(n)$, see Subsection 3.3), we have

$$s_1((q-p^{r-1}) + p^{r-1}q) = s_1((p-1)+q)^{p^{r-1}} = 0$$

(cf. [Ge, Corollary 2.12]). By Lemma 4.4, we have

$$s_1(\omega_1^{nm_1}) = s_1(\omega_1^{(q-p^{r-1})+p^{r-1}q}) \in \mathcal{P}.$$

Next we consider the complex conjugate $\overline{\omega}_1^{nm_1}$. We see that

$$-nm_1 \equiv (p^{r-1}-1) + (q-p^{r-1}-1)q \bmod q^2-1.$$

Since $l((p^{r-1}-1) + (q-p^{r-1}-1)q) = q-2 < q-1$, we have

$$s_1((p^{r-1}-1) + (q-p^{r-1}-1)q) = 0.$$

Again by Lemma 4.4,

$$s_1(\overline{\omega}_1^{nm_1}) = s_1(\omega_1^{(p^{r-1}-1)+(q-p^{r-1}-1)q}) \in \mathcal{P}.$$

Since $nm_1 \equiv 1 \bmod q-1$, we see that $\omega_1^{nm_1}$ is imaginary. Therefore,

$$s_1(\omega_1^{nm_1})s_1(\overline{\omega}_1^{nm_1}) = q.$$

Hence

$$1 \le \mathrm{ord}_{\mathcal{P}}(s_1(\omega_1^{nm_1})) < \mathrm{ord}_{\mathcal{P}}(q).$$

Let $c \in \mathbb{Z}$ be such that

$$1 \le c \le q-2, \qquad c \equiv m_1 \bmod q-1.$$

Set $m_2 = c + (q-1)q$. Then

$$s_1(m_2) = -\binom{q-1}{c}(T^q - T)^c$$

(cf. [Ge, Corollary 3.14]). Notice that $\binom{q-1}{c} \not\equiv 0 \bmod p$. Therefore $s_1(m_2) \not\equiv 0 \bmod Q_2$. By Lemma 4.4, we see that $s_1(\omega_2^{m_2}) \notin \mathcal{P}$. Since $\omega_2^{m_2}$ is imaginary, we have

$$\mathrm{ord}_{\mathcal{P}}(s_1(\omega_2^{-m_2})) = \mathrm{ord}_{\mathcal{P}}(q).$$

Let $\chi = \omega_1^{nm_1}\omega_2^{-m_2}$. Then $\chi(\alpha) = 1$ since $m_1 \equiv m_2 \bmod q-1$. Hence χ is a real character of conductor $m = Q_1Q_2$. By Proposition 4.3, we have

$$\mathrm{ord}_{\mathcal{P}}(s_2^+(\chi)) = \mathrm{ord}_{\mathcal{P}}(s_1(\omega_1^{nm_1})) + \mathrm{ord}_{\mathcal{P}}(s_1(\omega_2^{-m_2})) \notin \mathrm{ord}_{\mathcal{P}}(q)\mathbb{Z}.$$

By (2.5), there exist π_i, π_j $(i \ne j)$ such that $s_2^+(\chi) = \pi_i\pi_j$. Therefore, by Proposition 2.3, we see that K_m^+ is not ordinary. This completes the proof of Theorem 1.3.

Acknowledgements. The author wishes to thank the referee for pointing out some minor errors and misprints in an earlier version of this paper.

References

[B-E-W] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Ser. Monogr. Adv. Texts, Wiley, New York, 1998.

[G-R] S. Galovich and M. Rosen, *The class number of cyclotomic function fields*, J. Number Theory 13 (1981), 363–375.

[Ge] E.-U. Gekeler, *On power sums of polynomials over finite fields*, J. Number Theory 30 (1988), 11–26.

[Go] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, 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), 45–56.

[Ro] M. Rosen, *Number Theory in Function Fields*, Springer, Berlin, 2002.

[Sh1] D. Shiomi, *The Hasse–Witt invariant of cyclotomic function fields*, Acta Arith. 150 (2011) 227–240.

[Sh2] D. Shiomi, *Ordinary cyclotomic function fields*, J. Number Theory 133 (2013), 523–533.

[Sh3] D. Shiomi, *Explicit formulas for Hasse–Witt invariants of cyclotomic function fields with conductor of degree two*, RIMS Kôkyûroku Bessatsu B34 (2013), 213–222.

Daisuke Shiomi
Department of Mathematical Sciences
Faculty of Science
Yamagata University
Kojirakawa-machi 1-4-12
Yamagata 990-8560, Japan
E-mail: shiomi@sci.kj.yamagata-u.ac.jp

Received on 19.8.2013
and in revised form on 10.3.2014 (7556)