ACTA ARITHMETICA
150.3 (2011)

The Hasse–Witt invariant of cyclotomic function fields

by

Daisuke Shiomi (Nagoya)

1. Introduction. Let p be a prime, and let $\mathbb{F}_q$ be a field with $q = p^e$ elements. Fix an algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. For a global function field K over $\mathbb{F}_q$, we denote by J_K the Jacobian of $K\bar{\mathbb{F}}_q$ over $\bar{\mathbb{F}}_q$. For a prime l, it is well-known that the l-primary subgroup $J_K(l)$ of J_K satisfies

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

where g_K is the genus of K, and λ_K is an integer where $0 \leq \lambda_K \leq g_K$. The integer λ_K is called the *Hasse–Witt invariant* of K. For basic references about the Jacobian, see [Ro2], [Mi].

In this paper, we will investigate the structure of the Jacobian for a cyclotomic function field. For a monic polynomial $m \in \mathbb{F}_q[T]$, we denote by K_m the mth cyclotomic function field (see Subsection 2.1). Let g_m and λ_m be the genus of K_m and the Hasse–Witt invariant of K_m, respectively. By using the Riemann–Hurwitz formula, Kida–Murabayashi gave an explicit formula for g_m for all monic polynomials m (cf. [K-M]). Hence we know the l-rank of the Jacobian J_{K_m} for all prime l ($\neq p$).

On the other hand, it is more difficult to determine the p-rank of the Jacobian J_{K_m}. In the previous paper, the author showed that $\lambda_{Q^n} = 0$ for a monic polynomials Q of degree one, and $n \geq 0$ (cf. [Sh]). The aim of this paper is to determine all monic polynomials m such that $\lambda_m = 0$, which means that the Jacobian J_{K_m} has no p-torsion points. We will see that the Hasse–Witt invariant λ_m decomposes as $\lambda_m = \lambda_m^+ + \lambda_m^-$, where λ_m^+ is the Hasse–Witt invariant of the maximal real subfield of K_m (see Subsection 2.3). Our goal in this paper is the following result.

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

DOI: 10.4064/aa150-3-2

Theorem 1.1. *Assume that* $p \neq 2, 3$. *Then:*

1. $\lambda_m^+ = 0$ *if and only if* m *satisfies one of the following three conditions:*
   (a) m *is a monic irreducible polynomial of degree two,*
   (b) $m = Q^n$ *where* Q *is a monic polynomial of degree one, and* $n \geq 0$,
   (c) $m = RQ^n$ *where* R *and* Q *are distinct polynomials of degree one and* $n \geq 1$.
2. $\lambda_m^- = 0$ *if and only if* $m = Q^n$ *where* Q *is a monic polynomial of degree one, and* $n \geq 0$.

By combining both parts of the above theorem, we see that $\lambda_m = 0$ if and only if $m = Q^n$ where Q is a monic polynomial of degree one and $n \geq 0$.

As an application of Theorem 1.1, we have congruence relations for the class number of K_m. Let h_m, h_m^+ be the class numbers of K_m and of its maximal real subfield, respectively. It is well-known that h_m is divisible by h_m^+. Put $h_m^- = h_m/h_m^+$. By Theorem 1.1 and Proposition 2.1 (see Subsection 2.3), we obtain the following result.

Corollary 1.1. *In the notation of Theorem* 1.1, *we have the following results.*

- *If* m *satisfies* (a), (b) *or* (c) *then* $h_m^+ \equiv 1 \bmod p$.
- *If* $m = Q^n$ *for a monic polynomial of degree one and* $n \geq 0$, *then* $h_m^- \equiv 1 \bmod p$.

Remark 1.1. Corollary 1.1 was first showed by Guo and Shu in the case $m = Q^n$ for a monic polynomial Q of degree one and $n \geq 0$ (cf. [G-S]).

2. Preparations. In this section, we recall some basic facts for cyclotomic function fields, zeta functions, and L-functions. For the details, see [Ha], [G-R], [Ro2], and [Wa].

2.1. Cyclotomic function fields. Let k be the field of rational functions over $\mathbb{F}_q$. Fix a generator T of k, and let $A = \mathbb{F}_q[T]$ be the polynomial subring of k. 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 the $\mathbb{F}_q$-linear maps defined by

$$\varphi : \bar{k} \to \bar{k} \quad (x \mapsto x^q),$$
$$\mu : \bar{k} \to \bar{k} \quad (x \mapsto Tx).$$

With the above actions, $\bar{k}$ becomes an A-module, called the *Carlitz module*. Let Λ_m be the set of all x satisfying $m * x = 0$, which is a cyclic A-submodule of $\bar{k}$. Fix a generator λ_m of Λ_m. Then we have the following isomorphism of A-modules:

$$A/mA \to \Lambda_m \quad (a \bmod m \mapsto a * \lambda_m),$$

where mA is the principal ideal generated by m. Let $(A/mA)^\times$ be the unit group of A/mA, and denote its order by $\Phi(m)$. Let K_m be the field obtained by adding all elements of Λ_m to k. We shall call K_m the mth *cyclotomic function field*. We see that K_m/k is a Galois extension, and we have the following isomorphism:

$$(2.1) \qquad (A/mA)^\times \to \mathrm{Gal}(K_m/k) \quad (a \bmod m \mapsto \sigma_{a \bmod m}),$$

where $\mathrm{Gal}(K_m/k)$ is the Galois group of K_m/k, and $\sigma_{a \bmod m}$ is the isomorphism given by $\sigma_{a \bmod m}(\lambda_m) = a * \lambda_m$. From the above isomorphism, we have $[K_m : k] = \Phi(m)$.

We regard $\mathbb{F}_q^\times \subseteq (A/mA)^\times$. Let K_m^+ be the intermediate field of K_m/k corresponding to $\mathbb{F}_q^\times$. Again, by the isomorphism (2.1), we have $[K_m^+ : k] = \Phi(m)/(q-1)$. Let P_∞ be the unique prime of k which corresponds to the valuation ord_∞ with $\mathrm{ord}_\infty(T) < 0$. The prime P_∞ splits completely in K_m^+/k, and each prime of K_m^+ over P_∞ is totally ramified in K_m/K_m^+. Hence $K_m^+ = K_m \cap k_\infty$, where k_∞ is the completion of k by P_∞. We shall call K_m^+ the *maximal real subfield* of K_m.

Next, we provide basic facts about Dirichlet characters. For a monic polynomial $m \in A$, let X_m be the group of all primitive Dirichlet characters modulo m. For a character $\chi \in X_m$, we call χ *real* if $\chi(a) = 1$ for all $a \in \mathbb{F}_q^\times$. Otherwise, we call χ *imaginary*. Let X_m^+ be the subgroup of all real characters of X_m. We denote by $\mathbb{D}$ the group of all primitive Dirichlet characters. Put

$$\widetilde{K} = \bigcup_{m \text{ monic}} K_m,$$

where m runs through all monic polynomials of A. Then, by the same argument as in the case of number fields (cf. [Wa, Chapter 3]), we have a one-to-one correspondence between finite subgroups of $\mathbb{D}$ and finite subextension fields of $\widetilde{K}/k$. In particular, we see that X_m and X_m^+ correspond to K_m and K_m^+, respectively.

2.2. Zeta functions. In this subsection, we will give definitions and basic properties of zeta functions of global function fields. Let K be a global function field over $\mathbb{F}_q$. The zeta function of K is defined 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 residue class field of $\mathcal{P}$. We see that $\zeta(s, K)$ converges absolutely for $\mathrm{Re}(s) > 1$.

Theorem 2.1 (cf. [Ro2, Theorem 5.9]). *Let g_K be the genus of K, and let h_K be the order of the divisor class group of degree zero of K, which is called the class number of K. Then there is a polynomial $Z_K(X) \in \mathbb{Z}[X]$ of degree $2g_K$ such that*

$$\zeta(s, K) = \frac{Z_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})}, \tag{2.2}$$

and $Z_K(0) = 1$, $Z_K(1) = h_K$.

We see that the equation (2.2) provides the analytic continuation of $\zeta(s, K)$ to the whole of $\mathbb{C}$.

The next theorem is important to calculate the Hasse–Witt invariant.

Theorem 2.2 (cf. [Ro2, Proposition 11.20]). *With the above notation, we have*

$$\lambda_K = \deg \bar{Z}_K(X), \tag{2.3}$$

where $\bar{Z}_K(X) \in \mathbb{F}_p[X]$ is the reduction of $Z_K(X)$ modulo p.

By the above formula, we see that $\bar{Z}_K(X) = 1$ if and only if $\lambda_K = 0$.

2.3. L-functions. In this subsection, we provide some basic facts about L-functions. Let $m \in A$ be a monic polynomial of degree d. For a character $\chi \in X_m$, define the L-function by

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

where a runs through all monic polynomials of A, and $N(a) = q^{\deg a}$. We denote by χ_0 the trivial character. By a short calculation, we have

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

where $s_i(\chi) = \sum_{a \text{ monic}, \deg(a)=i} \chi(a)$ for $i = 0, 1, \ldots, d-1$. Put

$$\Phi_\chi(X) = \begin{cases} \Big(\displaystyle\sum_{i=0}^{d-1} s_i(\chi) X^i\Big)/(1-X) & \text{if } \chi \text{ is non-trivial real}, \\ \displaystyle\sum_{i=0}^{d-1} s_i(\chi) X^i & \text{if } \chi \text{ is imaginary}. \end{cases}$$

Then

$$\Phi_\chi(q^{-s}) = \begin{cases} L(s, \chi)/(1-q^{-s}) & \text{if } \chi \text{ is non-trivial real}, \\ L(s, \chi) & \text{if } \chi \text{ is imaginary}. \end{cases}$$

Let χ be a non-trivial real character. Noting that $\sum_{i=0}^{d-1} s_i(\chi) = 0$, we can easily check that

$$\Phi_\chi(X) = \sum_{i=0}^{d-2}\Big(\sum_{j=0}^{i} s_j(\chi)\Big)X^i.$$

Hence $\Phi_\chi(X)$ is a polynomial for all $\chi \in X_m\backslash\{\chi_0\}$.

Let L be an intermediate field in $\widetilde{K}/k$ of finite degree corresponding to the character group X_L. Let $\mathcal{O}_L$ be the integral closure of A in the field L. We define the zeta function $\zeta(s, \mathcal{O}_L)$ of the ring $\mathcal{O}_L$ by

$$\zeta(s, \mathcal{O}_L) = \prod_{\mathcal{P}}\Big(1 - \frac{1}{\mathcal{N}\mathcal{P}^s}\Big)^{-1},$$

where the product runs over all primes of $\mathcal{O}_L$. By the same argument as in the case of number fields (cf. [Wa]), we have the following decomposition into L-functions:

$$\zeta(s, \mathcal{O}_L) = \prod_{\chi\in X_L} L(s, \chi).$$

Let f_∞, g_∞ be the relative degree of P_∞ in L/k and the number of primes of L over P_∞, respectively. Then

$$\zeta(s, L) = \zeta(s, \mathcal{O}_L)(1 - q^{-sf_\infty})^{-g_\infty}.$$

We put $L^+ = L \cap k_\infty$. Notice that the prime P_∞ splits completely in L^+/k, and each prime of L^+ over P_∞ is totally ramified in L/L^+. Hence we have the following lemma.

Lemma 2.1. *Let L be an intermediate field in $\widetilde{K}/k$ of finite degree corresponding to the character group X_L. Then*

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

Put $X_L^+ = X_{L^+}$ and $X_L^- = X_L\backslash X_{L^+}$, where X_{L^+} is the character group corresponding to L^+. We also put $Z_L^{(+)}(X) = Z_{L^+}(X)$ and $Z_L^{(-)}(X) = Z_L(X)/Z_{L^+}(X)$. By the definition, $Z_L^{(-)}(X)$ is a rational function over $\mathbb{Q}$. However, by the next lemma, we see that $Z_L^{(-)}(X)$ is a polynomial with integral coefficients.

Lemma 2.2. *Let L be an intermediate field in $\widetilde{K}/k$ of finite degree. Then $Z_L^{(+)}(X) \mid Z_L(X)$ in $\mathbb{Z}[X]$.*

Proof. By Lemma 2.1, we have

$$\frac{Z_L(q^{-s})}{Z_L^{(+)}(q^{-s})} = \frac{\zeta(s, L)}{\zeta(s, L^+)} = \prod_{\chi\in X_L^-} L(s, \chi).$$

Since $L(s,\chi)$ is a polynomial of q^{-s} for $\chi \in X_L^-$, we have $Z_L^{(+)}(X) \mid Z_L(X)$ in $\mathbb{C}[X]$. Noting that $Z_L^{(+)}(X)$ and $Z_L(X)$ are polynomials with integral coefficients such that $Z_L^{(+)}(0) = Z_L(0) = 1$, we have $Z_L^{(+)}(X) \mid Z_L(X)$ in $\mathbb{Z}[X]$. ■

Put $g_L^+ = g_{L^+}$, $g_L^- = g_L - g_{L^+}$, $\lambda_L^+ = \lambda_{L^+}$, $\lambda_L^- = \lambda_L - \lambda_{L^+}$. By Lemma 2.2, $Z_L^{(-)}(X)$ is a polynomial with integral coefficients of degree $2g_L^-$. By Theorem 2.2, we have $\lambda_L^- = \deg \bar{Z}_L^{(-)}(X)$. Let h_L, h_L^+ be the class numbers of L and L^+, respectively. By Theorem 2.1, we have $Z_L(1) = h_L$ and $Z_L^{(+)}(1) = h_L^+$. It follows that $Z_L^{(-)}(1) = h_L^-$. Hence we have the following result.

Proposition 2.1. *In the above notation, we have the following results.*

- *If $\lambda_L^+ = 0$, then $h_L^+ \equiv 1 \bmod p$.*
- *If $\lambda_L^- = 0$, then $h_L^- \equiv 1 \bmod p$.*

From Theorem 2.1 and Lemma 2.1, we have the following result.

Proposition 2.2. *Let L be an intermediate field in $\widetilde{K}/k$ of finite degree corresponding to the character group X_L. Then*

$$Z_L^{(+)}(X) = \prod_{\chi \in X_L^{+,*}} \Phi_\chi(X), \qquad Z_L^{(-)}(X) = \prod_{\chi \in X_L^-} \Phi_\chi(X),$$

where $X_L^{+,*} = X_L^+ \setminus \{\chi_0\}$.

Proposition 2.3. *Let L_1, L_2 be intermediate fields in $\widetilde{K}/k$ of finite degree such that $L_1 \subseteq L_2$. Then $Z_{L_1}^{(+)}(X) \mid Z_{L_2}^{(+)}(X)$ and $Z_{L_1}^{(-)}(X) \mid Z_{L_2}^{(-)}(X)$ in $\mathbb{Z}[X]$.*

Proof. By Proposition 2.2, we have

$$Z_{L_2}^{(+)}(q^{-s})/Z_{L_1}^{(+)}(q^{-s}) = \prod_{\chi \in X_{L_2}^+ \setminus X_{L_1}^+} \Phi_\chi(q^{-s}).$$

Hence $Z_{L_1}^{(+)}(X) \mid Z_{L_2}^{(+)}(X)$ in $\mathbb{Z}[X]$. On the other hand, we notice that $X_{L_1}^- \subseteq X_{L_2}^-$. By Proposition 2.2,

$$Z_{L_2}^{(-)}(q^{-s})/Z_{L_1}^{(-)}(q^{-s}) = \prod_{\chi \in X_{L_2}^- \setminus X_{L_1}^-} \Phi_\chi(q^{-s}).$$

It follows that $Z_{L_1}^{(-)}(X) \mid Z_{L_2}^{(-)}(X)$ in $\mathbb{Z}[X]$. ■

From Theorem 2.2 and Proposition 2.3, we have the following result.

Corollary 2.1. *Let L_1, L_2 be intermediate fields in $\widetilde{K}/k$ of finite degree such that $L_1 \subseteq L_2$. Then $\lambda_{L_2}^+ \geq \lambda_{L_1}^+$ and $\lambda_{L_2}^- \geq \lambda_{L_1}^-$.*

Let $m_1, m_2 \in A$ be monic polynomials such that $m_1 \mid m_2$. Then $K_{m_1} \subseteq K_{m_2}$. Put $\lambda_{m_2}^+ = \lambda_{K_{m_2}}^+$, $\lambda_{m_2}^- = \lambda_{K_{m_2}}^-$, $\lambda_{m_1}^+ = \lambda_{K_{m_1}}^+$, $\lambda_{m_1}^- = \lambda_{K_{m_1}}^-$. The next result is important in the proof of Theorem 1.1.

COROLLARY 2.2. *If* $\lambda_{m_2}^+ = 0$ (*resp.* $\lambda_{m_2}^- = 0$), *then* $\lambda_{m_1}^+ = 0$ (*resp.* $\lambda_{m_1}^- = 0$).

Proof. This follows from Corollary 2.1. ∎

3. Proof of the main theorem. Our goal in this section is to prove Theorem 1.1. We shall do this in three steps.

3.1. The irreducible case. The aim of this subsection is to determine all monic irreducible polynomials m with $\lambda_m^+ = 0$ (resp. $\lambda_m^- = 0$). To do this, we will use Goss's idea on the Kummer and Herbrand theorem for cyclotomic function fields (cf. [Go1]).

We assume that $m \in A$ is a monic irreducible polynomial of degree d. Put $Z_m(X) = Z_{K_m}(X)$, $Z_m^{(+)}(X) = Z_{K_m}^{(+)}(X)$, $Z_m^{(-)}(X) = Z_{K_m}^{(-)}(X)$. Then

$$Z_m(X) = Z_m^{(+)}(X) Z_m^{(-)}(X).$$

By Proposition 2.2, we have

$$Z_m^{(+)}(X) = \prod_{\chi \in X_m^{+,*}} \Phi_\chi(X), \qquad Z_m^{(-)}(X) = \prod_{\chi \in X_m^-} \Phi_\chi(X),$$

where $X_m^{+,*} = X_m^+ \setminus \{\chi_0\}$.

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 be the p-adic valuation of $\bar{\mathbb{Q}}_p$ with $\mathrm{ord}_p(p) = 1$. Let M be the field obtained by adding a primitive $(p^{de} - 1)$th root of unity to $\mathbb{Q}_p$ (note that $q = p^e$). Denote by $\mathcal{O}_M$ the valuation ring of M. Since $M/\mathbb{Q}_p$ is unramified, the residue class field $\mathcal{R}_M = \mathcal{O}_M / p\mathcal{O}_M$ consists of p^{de} elements. For $\chi \in X_m$, we see that the image of χ is contained in $\mathcal{O}_M$. Hence $\Phi_\chi(X) \in \mathcal{O}_M[X]$ for all $\chi \neq \chi_0$. By Theorem 2.2,

$$\begin{aligned} \lambda_m^+ &= \deg \bar{Z}_m^{(+)}(X) = \sum_{\chi \in X_m^{+,*}} \deg \bar{\Phi}_\chi(X), \\ \lambda_m^- &= \deg \bar{Z}_m^{(-)}(X) = \sum_{\chi \in X_m^-} \deg \bar{\Phi}_\chi(X), \end{aligned} \tag{3.1}$$

where $\bar{\Phi}_\chi(X)$ is the reduction of $\Phi_\chi(X)$ modulo $p\mathcal{O}_M$.

Our next task is to investigate $\deg \bar{\Phi}_\chi(X)$. Notice that A/mA and $\mathcal{R}_M$ are finite fields with the same cardinality. Hence A/mA is isomorphic to $\mathcal{R}_M$. Fix an isomorphism $\phi : A/mA \to \mathcal{R}_M$. This map induces a group isomorphism $\phi_0 : (A/mA)^\times \to \mathcal{R}_M^\times$. Let $W \subseteq \mathcal{O}_M$ be the group of $(p^{de}-1)$th roots of unity. Then we have the isomorphism

$$\psi : W \to \mathcal{R}_M^\times \quad (\zeta \to \zeta \bmod p\mathcal{O}_M).$$

Put $\omega = \psi^{-1} * \phi_0$. Then ω is a generator of X_m (recall that X_m is the group of primitive Dirichlet characters modulo m). Hence we have

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

Notice that ω^t is real if $t \equiv 0 \bmod q-1$, and ω^t is imaginary if $t \not\equiv 0 \bmod q-1$. We recall that

$$s_i(\omega^t) = \sum_{\substack{a \text{ monic} \\ \deg(a)=i}} \omega^t(a)$$

for $i = 0, 1, \ldots, d-1$ and $t = 1, \ldots, q^d - 2$ (see Subsection 2.3). Since $\omega(a) \equiv \phi(a) \bmod p\mathcal{O}_M$, we have

$$\phi\Big(\sum_{\substack{a \text{ monic} \\ \deg(a)=i}} a^t \bmod mA\Big) \equiv s_i(\omega^t) \bmod p\mathcal{O}_M.$$

We see that ϕ naturally induces an isomorphism $\phi^* : (A/mA)[X] \to \mathcal{R}_M[X]$. For this isomorphism, we have

$$\phi^*(B_t(X) \bmod mA) = \bar{\Phi}_{\omega^t}(X),$$

where $B_t(X) \in A[X]$ is defined by

$$B_t(X) = \begin{cases} \displaystyle\sum_{i=0}^{d-2}\Big(\sum_{\substack{a \text{ monic} \\ 0 \le \deg(a) \le i}} a^t\Big)X^i & \text{if } t \equiv 0 \bmod q-1, \\ \displaystyle\sum_{i=0}^{d-1}\Big(\sum_{\substack{a \text{ monic} \\ \deg(a)=i}} a^t\Big)X^i & \text{if } t \not\equiv 0 \bmod q-1 \end{cases}$$

for $t = 1, \ldots, q^d - 2$. In particular,

$$\deg(B_t(X) \bmod mA) = \deg(\bar{\Phi}_{\omega^t}(X)). \tag{3.2}$$

Remark 3.1. Goss considered the above polynomial $B_t(X)$, and showed that $B_t(X)$ is closely related to the values of characteristic p zeta functions. For the properties of $B_t(X)$, see [Ge] and [Go2].

By equations (3.1) and (3.2), we have the following result.

Lemma 3.1. *Let $m \in A$ be a monic irreducible polynomial of degree d. Then*

- $\lambda_m^+ = 0$ *if and only if*
$$\sum_{\substack{a \text{ monic} \\ 0\le\deg(a)\le i}} a^t \equiv 0 \bmod mA$$
for $i = 1,\dots,d-2$ *and* $t = 1,\dots,q^d-2$ *with* $t \equiv 0 \bmod q-1$.
- $\lambda_m^- = 0$ *if and only if*
$$\sum_{\substack{a \text{ monic} \\ \deg(a)=i}} a^t \equiv 0 \bmod mA$$
for $i = 1,\dots,d-1$ *and* $t = 1,\dots,q^d-2$ *with* $t \not\equiv 0 \bmod q-1$.

By the above result, we will determine monic irreducible polynomials m with $\lambda_m^+ = 0$ (resp. $\lambda_m^- = 0$). To do this, we need the following lemma.

LEMMA 3.2.
$$\sum_{\substack{a \text{ monic} \\ 0\le\deg(a)\le 1}} a^{q^2-1} = -(T^q-T)^{q-1}, \qquad \sum_{\substack{a \text{ monic} \\ \deg(a)=1}} a^{(q-1)+q} = -(T^q-T).$$

Proof. This follows from Corollary 3.14 and Theorem 4.1 in [Ge]. ∎

Now we conclude the irreducible case.

PROPOSITION 3.1. *Let $m \in A$ be a monic irreducible polynomial. Then*

- $\lambda_m^+ = 0$ *if and only if* $\deg m \le 2$.
- $\lambda_m^- = 0$ *if and only if* $q = 2$ *or* $\deg m = 1$.

Proof. First, we assume that $\lambda_m^+ = 0$. Notice that $T^q - T = \prod_{\alpha\in\mathbb{F}_q}(T-\alpha)$. By Lemmas 3.1 and 3.2, we have $\deg m \le 2$. By the same argument, $\lambda_m^- = 0$ implies that $q = 2$ or $\deg m = 1$.

Conversely, by the Riemann–Hurwitz formula, we can easily check that $g_m^+ = 0$ if $\deg m \le 2$, and $g_m^- = 0$ if $q = 2$ or $\deg m = 1$. Notice that $\lambda_m^+ \le g_m^+$ and $\lambda_m^- \le g_m^-$. Hence we obtain the conclusion. ∎

3.2. The irreducible power case. In this subsection, we suppose that Q is a monic irreducible polynomial of degree d, and n is a non-negative integer. First we state a classical result on the Hasse–Witt invariant.

THEOREM 3.1 (cf. [Su], [Ro1]). *Let K be a global function field over $\mathbb{F}_q$, and let L/K be a geometric cyclic extension of degree p. Let λ_L and λ_K be the Hasse–Witt invariants of L and K, respectively. Let S_K be the set of all primes of K. Then*
$$\lambda_L - 1 = p(\lambda_K - 1) + \sum_{P\in S_K} (e_P - 1)\deg_K P$$

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

By using the above formula, we will calculate $\lambda^+_{Q^n}$ (resp. $\lambda^-_{Q^n}$) from λ^+_Q (resp. λ^-_Q). To do this, we need the following lemma.

LEMMA 3.3 (cf. [Ro2]). *Let Q be a monic irreducible polynomial, and let n be a non-negative integer. Then:*

1. *The prime Q is totally ramified in K_{Q^n}/k.*
2. *The prime P_∞ splits completely in $K^+_{Q^n}/k$, and each prime of $K^+_{Q^n}$ over P_∞ is totally ramified in $K_{Q^n}/K^+_{Q^n}$.*
3. *Any prime except Q and P_∞ is unramified in K_{Q^n}/k.*

By the Galois isomorphism (2.1), we see that K_{Q^n}/K_Q is a Galois extension of degree $q^{d(n-1)} = p^{ed(n-1)}$. We use Theorem 3.1 and Lemma 3.3, repeatedly, and obtain the following relations:

$$\lambda_{Q^n} = \lambda_Q q^{d(n-1)} + (\deg Q - 1)(q^{d(n-1)} - 1),$$
$$\lambda^+_{Q^n} = \lambda^+_Q q^{d(n-1)} + (\deg Q - 1)(q^{d(n-1)} - 1),$$
$$\lambda^-_{Q^n} = \lambda^-_Q q^{d(n-1)}.$$

By the above relations and Proposition 3.1, we obtain the next result.

PROPOSITION 3.2. *Let $Q \in A$ be a monic irreducible polynomial of degree d, and let n be a non-negative integer. Then:*

- $\lambda^+_{Q^n} = 0$ *if and only if either* $\deg Q = 1$ *or* $n = 1$ *and* $\deg Q = 2$.
- $\lambda^-_{Q^n} = 0$ *if and only if* $q = 2$ *or* $\deg Q = 1$.

3.3. The general case. Our goal in this subsection is to prove Theorem 1.1. To do this, we need some preparations. For a monic polynomial $m \in A$, put

$$Z_m(X) = 1 + c_{1,m}X + c_{2,m}X^2 + \cdots + c_{2g_m,m}X^{2g_m},$$
$$Z^{(+)}_m(X) = 1 + c^{(+)}_{1,m}X + c^{(+)}_{2,m}X^2 + \cdots + c^{(+)}_{2g^+_m,m}X^{2g^+_m},$$
$$Z^{(-)}_m(X) = 1 + c^{(-)}_{1,m}X + c^{(-)}_{2,m}X^2 + \cdots + c^{(-)}_{2g^-_m,m}X^{2g^-_m}.$$

Then $c_{1,m} = c^{(+)}_{1,m} + c^{(-)}_{1,m}$. First, we will calculate $c^{(+)}_{1,m}$ and $c^{(-)}_{1,m}$.

LEMMA 3.4 (cf. [Ro2, Theorem 5.9]). *For a global function field K over $\mathbb{F}_q$, we put*

$$Z_K(X) = 1 + c_1(K)X + c_2(K)X^2 + \cdots + c_{2g_K}(K)X^{2g_K}.$$

Then $1 + q + c_1(K) = a_1(K)$, where $a_1(K)$ is the number of primes of K of degree one.

By assertion 2 of Lemma 3.3, and Lemma 3.4, we obtain

$$1+q+c_{1,m}=\Phi(m)/(q-1)+\sum_R W_{m,R}, \tag{3.3}$$

$$1+q+c_{1,m}^{(+)}=\Phi(m)/(q-1)+\sum_R W_{m,R}^{+}, \tag{3.4}$$

where R runs through all monic irreducible polynomials of A. Here $W_{m,R}$ (resp. $W_{m,R}^{+}$) is the number of primes of K_m (resp. K_m^{+}) of degree one over R. We notice that $W_{m,R}=0$, and $W_{m,R}^{+}=0$ if $\deg R\geq 2$. By equations (3.3), (3.4), we have

$$c_{1,m}^{(-)}=\sum_R (W_{m,R}-W_{m,R}^{+}).$$

PROPOSITION 3.3. *Suppose that $m=\prod_Q Q^{n_Q}$, where Q is a monic irreducible polynomial, and $n_Q\geq 0$. Let R be a monic polynomial of degree one. Then*

$$\text{(1)}\qquad W_{m,R}=\begin{cases} 0 & \text{if } \deg(m/R^{n_R})\geq 2,\\ 0 & \text{if } \deg(m/R^{n_R})=1 \text{ and } R\not\equiv 1 \bmod m/R^{n_R},\\ q-1 & \text{if } \deg(m/R^{n_R})=1 \text{ and } R\equiv 1 \bmod m/R^{n_R},\\ 1 & \text{if } \deg(m/R^{n_R})=0,\end{cases}$$

$$\text{(2)}\qquad W_{m,R}^{+}=\begin{cases} 0 & \text{if } \deg(m/R^{n_R})\geq 2,\\ 1 & \text{if } \deg(m/R^{n_R})=1,\\ 1 & \text{if } \deg(m/R^{n_R})=0.\end{cases}$$

To prove this, we need the following lemma.

LEMMA 3.5. *Let $m\in A$ be a monic polynomial, and let $R\in A$ be a monic irreducible polynomial which is prime to m. Let $\mathcal{R}$ (resp. $\mathcal{R}^{+}$) be a prime of K_m (resp. K_m^{+}) over R. Then R is unramified in K_m/k, $\deg_{K_m}\mathcal{R}\geq\deg m$ and $\deg_{K_m^{+}}\mathcal{R}^{+}\geq\deg m$.*

Proof. By Theorem 12.10 in [Ro2], the prime R is unramified in K_m/k, and $\sigma_{R \bmod m}=(R,K_m/k)$ (see the Galois isomorphism (2.1)), where $(R,K_m/k)$ is the Artin symbol of R in K_m/k. It follows that $R^{f_R}-1\in mA$, where f_R is the relative degree of R in K_m/k. Hence $\deg_{K_m}\mathcal{R}=f_R\deg R\geq\deg m$.

On the other hand, we recall that the subgroup $\mathbb{F}_q^{\times}$ ($\subseteq (A/mA)^{\times}$) corresponds to K_m^{+}. Hence there is an $\alpha\in\mathbb{F}_q^{\times}$ such that $R^{f_R^{+}}-\alpha\in mA$, where f_R^{+} is the relative degree of R in K_m^{+}/k. Hence $\deg_{K_m^{+}}\mathcal{R}^{+}=f_R^{+}\deg R\geq\deg m$. ∎

Proof of Proposition 3.3. First we prove assertion (2). Put $m'=m/R^{n_R}$. Then we see that $K_{m'}^{+}\subseteq K_m^{+}$. We consider the following three cases:

(I) We assume $\deg m'\geq 2$. By Lemma 3.5, the degree of a prime of $K_{m'}^{+}$ over R is at least 2. It follows that $W_{m,R}^{+}=0$.

(II) We assume $\deg m' = 1$. Then $K^+_{m'} = k$. By Lemma 3.3, we see that R is unramified in $K_{m'}/K^+_{m'}$. It follows that each prime of K^+_m over R is unramified in K_m/K^+_m. On the other hand, the ramification index of R in $K_{R^{n_R}}/k$ is equal to $\Phi(m)/(q-1)$. It follows that R is totally ramified in K^+_m/k. Hence $W^+_{m,R} = 1$.

(III) We assume $\deg m' = 0$. Then $m = R^{n_R}$. The prime R is totally ramified in K^+_m/k. Hence $W^+_{m,R} = 1$.

Next we prove assertion (1). By the same argument as in (I), (III), we can prove (1) if $\deg m' \geq 2$ or $\deg m' = 0$. Hence we only consider the following two cases:

(IV) We assume $\deg m' = 1$ and $R \not\equiv 1 \bmod m'$. Then the relative degree of R in $K_{m'}/k$ is at least 2. It follows that $W_{m,R} = 0$.

(V) We assume $\deg m' = 1$ and $R \equiv 1 \bmod m'$. Then R splits completely in $K_{m'}/k$. On the other hand, each prime of $K_{m'}$ over R is totally ramified in $K_m/K_{m'}$. Hence $W_{m,R} = q-1$. ■

Proof of Theorem 1.1. First, we prove assertion 2. If $m = Q^n$ where Q is a monic polynomial of degree one and $n \geq 0$, then $\lambda^-_m = 0$ by Proposition 3.1.

Conversely, we assume that $\lambda^-_m = 0$. By Corollary 2.2 and Proposition 3.2, we can suppose that $m = \prod_{i=1}^s R_i^{n_i}$ where R_i $(i = 1, \ldots, s)$ are distinct polynomials of degree one. We assume $s \geq 2$. Put $m' = R_1R_2$. By using (2) of Proposition 3.3, we have $W^+_{m',R_1} = W^+_{m',R_2} = 1$. Hence $c^{(-)}_{1,m'} = W_{m',R_1} + W_{m',R_2} - 2$. By using (1) of Proposition 3.3, we see that $W_{m',R_1} + W_{m',R_2}$ is 0, $q-1$ or $2(q-1)$. Noting that $p \neq 2, 3$, we have $c^{(-)}_{1,m'} \not\equiv 0 \bmod p$. This leads to $\lambda^-_{m'} \geq 1$. By Corollary 2.2, we have $\lambda^-_m \geq 1$. This contradicts $\lambda^-_m = 0$. Hence $s = 1$. This completes the proof of assertion 2.

Next we prove assertion 1. By Proposition 3.2, we have $\lambda^+_m = 0$ if m satisfies (a) or (b). We assume that $m = RQ^n$ where R and Q are distinct polynomials of degree one, and $n \geq 1$. By the Riemann–Hurwitz formula, we have $g^+_{RQ} = 0$. Hence $\lambda^+_{RQ} = 0$. Notice that Q is totally ramified in $K^+_{RQ^n}/k$, and any prime of K^+_{RQ} except over Q is unramified in $K^+_{RQ^n}/K^+_{RQ}$. By Theorem 3.1, we obtain $\lambda^+_{RQ^n} = 0$.

Conversely, we assume that $\lambda^+_m = 0$. We will show that m satisfies one of conditions (a), (b), (c). By Proposition 3.2 and Corollary 2.2, this will follow if $\lambda^+_m \geq 1$ in the following four cases:

(A) $m = QR$ where Q is a monic irreducible polynomial of degree two, and R is a monic polynomial of degree one.

(B) $m = QR$ where Q, R are distinct monic irreducible polynomials of degree two.
(C) $m = Q^2R^2$ where Q, R are distinct monic polynomials of degree one.
(D) $m = QRS$ where Q, S, R are distinct monic polynomials of degree one.

By Proposition 3.3, we can easily check that $c_{1,m}^{(+)} \not\equiv 0 \bmod p$ in cases (A), (B), (C). Hence $\lambda_m^+ \geq 1$ in these cases.

Finally, we investigate case (D). Let L be an intermediate field in K_{QRS}^+/K_{QR}^+ with $[L : K_{QR}^+]=2$. Put $Z_L(X) = 1+c_1(L)X+\cdots+c_{2g_L}(L)X^{2g_L}$, where g_L is the genus of L. Then $a_1(L) = 1 + q + c_1(L)$, where $a_1(L)$ is the number of primes of L of degree one. For each prime $\mathcal{P}$ of L not over Q, R, P_∞, we have $\deg_L \mathcal{P} \geq 2$ by applying Lemma 3.5 to K_{QR}^+. Hence

$$a_1(L) = 2(q-1) + W_Q(L) + W_R(L)$$

where $W_Q(L)$ (resp. $W_R(L)$) is the number of primes of L of degree one over Q (resp. R). Since Q and R are totally ramified in K_{QR}^+/k, we can see that $W_Q(L)+W_R(L)$ is 0, 2 or 4. Noting that $p \neq 2, 3$, we have $a_1(L) \not\equiv 1 \bmod p$. It follows that $c_1(L) \not\equiv 0 \bmod p$. Hence $\lambda_L \geq 1$. By Corollary 2.1, we have $\lambda_{QRS}^+ \geq 1$. ∎

Remark 3.2. Theorem 1.1 does not work in the case $p = 2, 3$. We give counterexamples:

- Assume that $q = p = 2$. Then $\lambda^+_{(T^2+T+1)T} = \lambda^-_{(T^2+T+1)T} = 0$.
- Assume that $q = p = 3$. Then $\lambda^+_{T(T-1)(T-2)} = \lambda^-_{T(T-1)(T-2)} = 0$.

Acknowledgements. The author wishes to thank the referee for many helpful suggestions.

References

[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*, ibid. 30 (1988), 11–26.

[Go1] D. Goss, *Kummer and Herbrand criterion in the theory of function fields*, Duke Math. J. 49 (1982), 377–384.

[Go2] —, *The Γ-function in the arithmetic of function fields*, ibid. 56 (1988), 163–191.

[G-S] L. Guo and L. Shu, *Class numbers of cyclotomic function fields*, Trans. Amer. Math. Soc. 351 (1999), 4445–4467.

[Ha] D. R. Hayes, *Explicit class field theory for rational function fields*, ibid. 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.

[Mi] J. S. Milne, *Jacobian varieties*, in: Arithmetic Geometry, Springer, New York, 1986.
[Ro1] M. Rosen, *Some remarks on the p-rank of an algebraic curve*, Arch. Math. (Basel) 41 (1983), 143–146.
[Ro2] —, *Number Theory in Function Fields*, Springer, Berlin, 2002.
[Sh] D. Shiomi, *On the Deuring–Shafarevich formula*, preprint.
[Su] D. Subrao, *The p-rank of Artin–Schreier curves*, Manuscripta Math. 16 (1975), 169–193.
[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer. New York, 1982.

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

Received on 21.10.2010
and in revised form on 7.4.2011 (6520)