J. Austral. Math. Soc. (*Series A*) **60** (1996), 301–310

GENUS THEORY FOR FUNCTION FIELDS

SUNGHAN BAE and JA KYUNG KOO

(Received 5 August 1992; revised 1 April 1993)

Communicated by J. H. Loxton

Abstract

We study the genus theory for function fields which is the analogue of the classical genus theory developed by Hasse and Fröhlich.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 11R58, 11R29.

0. Introduction

One of the important problems in number theory is to investigate ideal class groups. In 1951, Hasse introduced genus theory of quadratic number fields [3]. Later, Fröhlich generalized the theory to arbitrary number fields [2].

In the theory of funtion fields, Clement started the study of genus theory of function fields in the case of the cyclic extension of $\mathbb{F}_q(T)$ of prime degree ℓ dividing $q-1$ [1]. In this note we try to generalize the results in [1] following the methods of Fröhlich [2]. To do this we have defined the Hilbert class field and narrow Hilbert class field of a function field. Our definitions are somewhat different from those of [1]. Clement's definition allow a constant field extension inside the Hilbert class field, but ours does not. However they are essentially the same.

1. Notation and definitions

Let K be a global function field over a finite field $\mathbb{F}_q$ with a fixed place ∞ of degree d. Let $k(\infty)$ be the residue field at ∞. Fix a sign function (see [5] for definitions)

$$\operatorname{sgn} : K_\infty^* \to k(\infty)$$

Partially supported by the KOSEF Research Grant 91-08-00-07

where K_∞ is the completion of K at ∞ and a π uniformizer at ∞ with $\mathrm{sgn}(\pi) = 1$. In applications K_∞ replaces $\mathbb{R}$, so we need an analog of the field of complex numbers $\mathbb{C}$. Define $\widetilde{C} = K_\infty\left((-\pi)^{1/(q^d-1)}\right)$. In the following we mean by an *extension* of K, a separable extension of K for which any of its embeddings into K_∞^{ac} lies in $\widetilde{C}$ viewing as a subfield of K_∞^{ac}.

Let L be a finite Galois extension of K and S be the set of places of L lying above ∞. Denote by $\mathcal{O}_K$ (respectively $\mathcal{O}_L$) the set of elements of K (respectively L) which are regular outside ∞ (respectively S); these form the ring of integers in K (respectively L). For each $v \in S$, the completion L_v of L at v is a finite extension of K_∞ in $\widetilde{C}$. Let N_v be the norm map from L_v to K_∞.

Define a sign map

$$\mathrm{sgn}_v : L_v^* \longrightarrow k(v)$$

by $\mathrm{sgn}_v(x) = \mathrm{sgn}(N_v(x))$. We say that L is *totally real* if $L_v = K_\infty$ for every $v \in S$ and *totally complex* if $L_v = \widetilde{C}$ for every $v \in S$.

REMARK 1.1. The reason for taking $-\pi$ in the definition of $\widetilde{C}$ is to make the sign of $(-\pi)^{1/(q^d-1)}$ equal to 1.

Define the *Hilbert class field* of L relative to S to be the maximal unramified abelian extension of L where S splits completely. Similarly we define the *narrow Hilbert class field* H_L^+ to be the maximal abelian extension of L in $\widetilde{C}$, unramified outside S. We call a place in S the infinite place.

Let $J(L)$ be the idele group of L and

$$U(L) = \{(x_w) \in J(L) : x_w \text{ is a unit in } L_w,\ w \notin S\},$$
$$U_+(L) = \{(x_w) \in U(L) : \mathrm{sgn}_v(x_v) = 1 \quad \forall v \in S\}.$$

Then by class field theory, H_L corresponds to $L^* \cdot U(L)$ and H_L^+ to $L^* \cdot U_+(L)$.

An element $x \in L$ is called *totally positive* if $\mathrm{sgn}_v(x) = 1$ for every $v \in S$. The *ideal class group* $Cl(\mathcal{O}_L)$ is defined to be the group of fractional ideals modulo principal ideals in $\mathcal{O}_L$, and the *narrow ideal class group* $Cl^+(\mathcal{O}_L)$ is defined to be the group of fractional ideals modulo principal ideals generated by totally positive elements. Then one can readily see that

$$[H_L : L] = |Cl(\mathcal{O}_L)| := h(\mathcal{O}_L),$$
$$[H_L^+ : L] = |Cl^+(\mathcal{O}_L)| := h^+(\mathcal{O}_L).$$

We define the *genus field* $G(L/K)$ to be the maximal extension of L in H_L which is the composite of L and some abelian extension of K and, where necessary, abbreviate the notation by setting $G = G(L/K)$. Similarly, we can define the *narrow genus*

field $G_+(L/K)$ replacing H_L by H_L^+. The *genus group* $\mathfrak{G}(L/K)$ is defined to be $J(L)/N_{G/L}(J(G)) \cdot L^* \cong \mathrm{Gal}(G/L)$. The *principal genus* $\mathfrak{P}(L/K)$ is defined to be the kernel of the Artin map

$$Cl(\mathcal{O}_L) \to \mathfrak{G}(L/K).$$

The *narrow genus group* $\mathfrak{G}_+(L/K)$ and *narrow principal genus* $\mathfrak{P}_+(L/K)$ are defined similarly.

EXAMPLE 1.2. (Compare with [1]) Let $\ell | (q-1)$ be a prime number. Let $K = \mathbb{F}_q(T)$ and $L = K(\sqrt[\ell]{P(T)})$ where $P(T)$ is a polynomial in $\mathbb{F}_q[T]$. Write $P(T) = aP_1(T)\cdots P_s(T)$ for the factorization of $P(T)$ with $P_i(T)$ monic irreducible polynomial in $\mathbb{F}_q[T]$ and $a \in \mathbb{F}_q^*$. We fix $\mathrm{sgn}(1/T) = 1$. The condition for L to be contained in $\widetilde{C}$ is

$$\begin{aligned} &(-a) \in (\mathbb{F}_q^*)^\ell && \text{if } \ell \nmid \deg P(T) \text{ and } \ell \text{ is even,} \\ &a \in (\mathbb{F}_q^*)^\ell && \text{otherwise.} \end{aligned}$$

Then it can be easily seen that the class field $H^{(+)}$ of [1] is just the field $\mathbb{F}_{q^\ell} \cdot H_L^+$. Thus the narrow genus field $G_+(L/K)$ is $K(\sqrt[\ell]{a_1P_1(T)}, \ldots, \sqrt[\ell]{a_sP_s(T)})$ with some appropriate a_i's in $\mathbb{F}_q^*$ ([1, Theorem 2.1]).

2. Basic properties

Let C_L denote the idele class group of L and $\check{C}_L$ its Pontryagin dual. Then the norm map

$$N_{L/K} : L \longrightarrow K$$

induces conorm

$$\check{N}_{L/K} : \check{C}(K) \longrightarrow \check{C}(L).$$

Let $\Phi(L/K) = \mathrm{Ker}\,\check{N}_{L/K}$. As in the number field case, taking [1, Lemma 2.2] into account, it is easy to see that

$$\begin{aligned} &\mathfrak{G}(L/K) \cong J(L)/U(L) \cdot N_{L/K}^{-1}(K^*), \\ (*) \qquad &\mathfrak{G}_+(L/K) \cong J(L)/U_+(L) \cdot N_{L/K}^{-1}(K^*). \end{aligned}$$

Hence

$$\check{\mathfrak{G}}(L/K) = \{\phi \in \mathrm{Im}\,\check{N}_{L/K} : \phi \text{ is unramified and } \phi_v \text{ is trivial for } v \in S\},$$

and

$$\check{\mathfrak{G}}_+(L/K) = \{\phi \in \operatorname{Im} \check{N}_{L/K} : \phi \text{ is unramified outside } S \text{ and } \phi_v(x) = 1 \text{ for } v \in S, \operatorname{sgn}_v(x) = 1\}.$$

Consider the group

$$\Phi^*(L/K) = \{\phi \in \check{C}(K) : \check{N}_{L/K}\phi \text{ is unramified and trivial on } S\}.$$

Then we get an exact sequence

$$1 \to \Phi(L/K) \to \Phi^*(L/K) \to \check{\mathfrak{G}}(L/K) \to 1.$$

Similarly we define

$$\Phi_+^*(L/K) = \{\phi \in \check{C}(K) : \check{N}_{L/K}\phi \text{ is unramified on finite places and trivial on } U_+(L)\}$$

and get an exact sequence

$$1 \longrightarrow \Phi(L/K) \longrightarrow \Phi_+^*(L/K) \longrightarrow \check{\mathfrak{G}}_+(L/K) \longrightarrow 1.$$

PROPOSITION 2.1. (a) $\Phi^*(L/K) = \Phi(G(L/K)/K), \Phi_+^*(L/K) = \Phi(G_+(L/K)/K)$. (b) $\Phi^*(L/K)$ *(respectively* $\Phi_+^*(L/K)$*) is the subgroup of* $\check{C}(K)$ *of characters* ϕ *with the following property: For each finite place* v *of* K, $\phi_v = \phi_v^{(1)}\phi_v^{(2)}$ *where* $\phi_v^{(1)}$ *is unramified and* $\phi_v^{(2)} \in \Phi(L_w/K_v)$ *for* w *lying above* v*, and*

$$\phi_\infty \in \Phi(L_w/K_\infty) \quad (\textit{respectively } \phi_\infty(x) = 1 \textit{ when } \operatorname{sgn}(x) = 1)$$

for any $w \in S$.

PROOF. (a) follows from the definitions and (∗). Exactly the same method as in [2] would give (b). However the extra condition for ϕ_∞ comes from the fact that K_∞ is nonarchimedean in contrast with the number field case.

COROLLARY 2.2. *Suppose that* $Cl(\mathcal{O}_K) = 1$. *Let* m *be the exponent of* $\operatorname{Gal}(L/K)$. *Then* $\mathfrak{G}(L/K)^m = 1$.

PROPOSITION 2.3. $G(L/K)$ *is the maximal subfield of* $G_+(L/K)$ *whose ramification index at* ∞ *is the same as the ramification index of* L *at* ∞. *In particular, if* L *is totally complex, then* $G(L/K) = G_+(L/K)$. *The same is true if* $Cl(\mathcal{O}_K) = 1$ *and* $[L : K]$ *is prime to* $q - 1$.

PROOF. The first two statements follow immediately from the definitions. Since $Cl(\mathcal{O}_K) = 1$, degree of ∞ is 1 and so $Cl_+(\mathcal{O}_K) = 1$. Then $U(L)^{q-1} \subset U(L)_+ \subset U(L)$, so

$$\check{\mathfrak{G}}_+(L/K)^{q-1} \subset \check{\mathfrak{G}}(L/K) \subset \check{\mathfrak{G}}_+(L/K).$$

But by the above corollary, $\check{\mathfrak{G}}_+(L/K)^m \subset \check{\mathfrak{G}}(L/K)$ for some integer m prime to $q-1$. Hence $\check{\mathfrak{G}}_+(L/K) = \check{\mathfrak{G}}(L/K)$.

PROPOSITION 2.4. *Let L/K be cyclic with $\mathrm{Gal}(L/K)$ generated by an element σ. Then*

(a) $\mathfrak{P}(L/K) = Cl(\mathcal{O}_L)^{1-\sigma}$, *that is,* $\mathfrak{G}(L/K) = Cl(\mathcal{O}_L)/Cl(\mathcal{O}_L)^{1-\sigma}$. (*Compare with* [1, Proposition 3.4].)

If, moreover, $[L : K]$ *is a power of a prime* ℓ *and* A_ℓ *denotes the* ℓ*-Sylow subgroup of a group* A, *then*

(b) $\mathfrak{G}(L/K)_\ell = 1$ *if and only if* $Cl(\mathcal{O}_L)_\ell = 1$.

If, in addition, $[L : K] = \ell$ *and* $Cl(\mathcal{O}_K) = 1$, *then*

(c) $\dim_{\mathbb{F}_\ell}(\mathfrak{G}(L/K)_\ell) =$ *minimal number of generators of* $Cl(A_L)_\ell$ *over* $\mathbb{Z}[\zeta_\ell]$.

PROOF. Exactly the same as the number field case.

REMARK 2.5. The referee noted that one can generalize part (a) of the above proposition to abelian extension L/K as follows:

Let L/K be an abelian extension with Galois group Δ. Let I_Δ be the augmentation ideal of $\mathbb{Z}[\Delta]$. Then $\mathfrak{P}(L/K) = I_\Delta Cl(\mathcal{O}_L)$.

This follows by looking at the Galois group Σ over K of the Hilbert class field H of L and realizing that the genus field is the fixed field of the commutator subgroup of Σ. Then use the identification of $Cl(\mathcal{O}_L)$ with $\mathrm{Gal}(H/L)$.

3. Rational base field

In this section we assume that $K = \mathbb{F}_q(T)$ and ∞ is the place associated to $(1/T)$. Choose π to be $-1/T$ and a sign function sgn so that $\mathrm{sgn}(-1/T) = 1$. In this case, $\widetilde{C}$ will be $\mathbb{F}_q\left(\left((1/T)^{1/(q-1)}\right)\right)$. Let $K_\infty^+ = \{x \in K_\infty^* : \mathrm{sgn}(x) = 1\}$. Then it is easy to see that

$$J(K) = U_{\mathrm{fin}}(K) \times K^* \times K_\infty^+.$$

Let $\widetilde{K}^{\mathrm{ab}}$ be the maximal abelian extension of K inside $\widetilde{C}$. Then by class field theory (see [4]),

$$U_{\mathrm{fin}}(K) \cong \mathrm{Gal}(\widetilde{K}^{\mathrm{ab}}/K).$$

Let P be the projection of $J(K)$ onto $U_{\text{fin}}(K)$. If M is a finite extension of K inside $\widetilde{K}^{\text{ab}}$, write

$$V(M/K) = \text{Im}(\text{Gal}(\widetilde{K}^{\text{ab}}/M) \longrightarrow U_{\text{fin}}(K)).$$

Let α be a generator of $\mathbb{F}_q^*$. Then we get the following proposition.

PROPOSITION 3.1. *Let L/K be a Galois extension. Then*

(a) $P(N_{L/K}(J(L)) \cdot K^*) = V(L'/K)$ *where L' is the maximal abelian extension of K in L,*

(b) $P(N_{L/K}(U(L)_+) \cdot K^*) = N_{L/K}(U_{fin}(L))$ *and if the ramification index at ∞ is m,*

(c) $P(N_{L/K}(U(L)) \cdot K^*) = N_{L/K}(U_{fin}(L))\langle\alpha^m\rangle_{fin}$ *where $\langle\alpha^m\rangle$ denotes the subgroup of $\mathbb{F}_q^*$ generated by α^m.*

P gives rise to isomorphisms

$$\mathfrak{G}_+(L/K) \cong V(L'/K)/N_{L/K}(U_{fin}(L));$$
$$\mathfrak{G}(L/K) \cong V(L'K)/N_{L/K}(U_{fin}(L)) \cdot \langle\alpha^m\rangle_{fin}.$$

PROOF. The proofs of (a) and (b) are the same as those of number field case. We only prove (c). Since the ramification index at ∞ is m, the infinite component of $N_{L/K}(U(L))$ is $\langle\alpha^m\rangle_\infty U_\infty^{(1)}$, where $U_\infty^{(1)} = \{u \in U_\infty : \text{sgn}(u) = 1\}$ and $\langle\alpha^m\rangle$ is the subgroup of $\mathbb{F}_q^*$ generated by α^m. But

$$(\alpha^m)_\infty = \alpha^m \cdot (\alpha^{-m})_{\text{fin}} \in U_{\text{fin}}(K) \times K^*.$$

The rest is the same as in the classical case [2].

COROLLARY 3.2. *The followings are equivalent,*

(a) $\mathfrak{G}_+(L/K) = \mathfrak{G}(L/K)$.

(b) *The ramifications at ∞ of L and G_+ are equal.*

(c) $\alpha^m \in N_{L/K}(J(L))$ *where m is the ramification index of L at ∞.*

Now let S be a finite set of finite places of K including the ramified ones in L. Put

$$U_S = \prod_{v \in S} U(K_v), \qquad U^S = \prod_{\substack{v \notin S \\ v \neq \infty}} U(K_v).$$

Then $U_{\text{fin}}(K) = U_S \times U^S$ and $U^S \subset N_{L/K}(U(L)_+)$. Let P_S be the composition of P and the projection

$$U_{\text{fin}} \longrightarrow U_S.$$

Denote by $V(L'/K)_S$ the image of $V(L'/K)$ under this projection. Then we have

COROLLARY 3.3. *P_S gives rise to isomorphisms*

$$\mathfrak{G}_+(L/K) \cong V(L'/K)_S/\prod\nolimits_{v\in S} N_{L_w/K_v}(U(L_w))$$

and if m is the ramification index of L at ∞,

$$\mathfrak{G}(L/K) = V(L'/K)_S/\prod\nolimits_{v\in S} N_{L_w/K_v}(U(L_w))\langle\alpha^m\rangle_S.$$

REMARK 3.4. The element α plays the role of -1 of $\mathbb{Q}$, which is the generator of the unit group.

Let L/K be abelian. Let $\check{C}^0(K)$ be the subgroup of $\check{C}(K)$ consisting of the ϕ that are trivial on $K_\infty^+ \cdot K^*$. Let ϕ_v denote its v-component. We may identify $\check{C}^0(K)$ with $\check{U}_{\text{fin}}(K)$. Given $\phi \in \check{U}_{\text{fin}}(K)$, $\phi_{(v)}$ is the unique character of $U_{\text{fin}}(K)$ so that

$$\begin{aligned}\phi_{(v)}|_{U_v} &= \phi|_{U_v},\\ \phi_{(v)}|_{U_{v'}} &= 1 \quad \text{if } v' \neq v,\end{aligned}$$

where U_v is the group of units in K_v. For a finite subgroup Φ of $\check{C}^0(K)$, define $\Phi_{(v)} = \{\phi_{(v)} : \phi \in \Phi\}$.

THEOREM 3.5. *Let L be an abelian extension of K. Then*

$$\Phi_+^*(L/K) = \prod_{v\neq\infty} \Phi(L/K)_{(v)}.$$

If the ramification index of L at ∞ is m, then $\Phi^*(L/K)$ is the subgroup of $\Phi_+^*(L/K)$ of characters ϕ with $\phi(\alpha_{fin}^m) = 1$.

PROOF. The first part of the theorem follows from exactly the same arguments as in the number field case. Let m be the ramification index of L at ∞ and $\phi \in \Phi_+^*(L/K)$. Then by Proposition 2.1, $\phi \in \Phi^*(L/K)$ if and only if $\phi_\infty \in \Phi(L_\infty/K_\infty)$. This is so if and only if $\phi_\infty(x) = 1$ for every x with $\operatorname{sgn}(x) \in \langle\alpha^m\rangle$. Again this condition is equivalent to

$$1 = \phi_\infty(\alpha^m) = \phi((\alpha^m)_\infty).$$

Since ϕ is trivial on L^*, we get the result.

COROLLARY 3.6. *If L/K is abelian, then $\check{\mathfrak{G}}_+(L/K) \cong \prod_{v\neq\infty} \Phi(L/K)_{(v)}/\Phi(L/K)$.*

REMARK 3.7. It follows easily from the definition that $\#\Phi(L/K) = [L : K]$ and that $\#\Phi(L/K)_{(v)}$ is the ramification index of L/K at v.

EXAMPLE 3.8. Let $L = K(\Lambda_{m(T)})$ be the $m(T)$-th cyclotomic function field where m is a monic polynomial in $A = \mathbb{F}_q[T]$. Then by Corollary 3.6 the genus number g_K is given by

$$\prod_{\substack{p(T)|m(T) \\ \text{monic irreducible}}} e_{p(T)}(L/K)/[L : K],$$

where $e_{p(T)}(L/K)$ is the ramification index of L/K at the place $(p(T))$. However the product equals 1 by the elementary theory of Carlitz modules. So $L = G_+(L/K)$.

THEOREM 3.9. *Let L/K be abelian and S be the set of finite places which are ramified in L.*

(a) *Then the followings are equivalent*

(i) $L = G_+(L/K)$;
(ii) $\Phi(L/K) = \prod_{v\in S} \Phi(L/K)_{(v)}$;
(iii) $\mathrm{Gal}(L/K) = \bigoplus_{v\in S} \Gamma_{v,0}$, *where $\Gamma_{v,0}$ is the inertia group at v;*
(iv) *L is the composite of fields with prime power discriminant.*

(b) *$L = G(L/K)$ only in the following cases.*

(i) $L = G_+(L/K)$;
(ii) *L is the maximal subfield, with ramification index m at ∞, of an abelian extension M of K such that $M = G_+(M/K)$ and M/L is unramified at all finite places.*

PROOF. The equivalence of (iii) and (iv) can be derived easily from the theory of Carlitz modules. The rest is exactly the same as in the number field case.

THEOREM 3.10. *Let L/K be a cyclic extension of degree ℓ^n, ℓ a prime. Let v_i be the finite places, ramified in L, of ramification degree ℓ^{n_i}, $n_1 \geq n_2 \geq \cdots \geq n_t \geq 1$. Then $\mathfrak{G}_+(L/K)$ is abelian of type $(\ell^{n_2}, \ldots, \ell^{n_t})$.*

PROOF. Since $L \subset \widetilde{C}$, L must be totally ramified, and the rest of the argument is the same as in the number field case.

COROLLARY 3.11. *$Cl_+(A_L)_\ell = 1$ if and only if $t = 1$.*

COROLLARY 3.12. $\ell^{n_2+\cdots+n_t} | h_+(L)$.

Now let ℓ be a prime number dividing $q - 1$.

THEOREM 3.13. *Let L/K be a cyclic extension of degree ℓ^n. Let ℓ^r be the ramification index of L at ∞ and s be such that $\ell^{r+s} | q - 1$. If $h(L)$ is prime to ℓ, then either*

(a) *precisely one finite place is ramified in L, or*
(b) *$s \geq 1$ and precisely two finite places v_1 and v_2 are ramified in L of ramification degrees ℓ^n and ℓ^t where $1 \leq t \leq \min(s, n)$. Furthermore $\phi((\alpha^{\ell^r})_{v_2}) \neq 1$ where ϕ is a generator of $\Phi(L/K)$.*

PROOF. It follows from Proposition 2.4 that $h(\mathcal{O}_L)$ is prime to ℓ if and only if ℓ does not divide $[G(L/K) : L]$. But this is equivalent to $L = G(L/K)$ by Theorem 3.10.

Suppose that at least two finite places are ramified in L. Then $G_+(L/K) \neq L$, so $G(L/K) = L$ implies that $G_+(L/K)$ is cyclic of order ℓ^t over L and totally ramified at ∞ by Theorem 3.9. Hence t must satisfy the given condition and only two finite places can ramify in L. Because $G_+(L/K) \neq G(L/K)$, we must have $\alpha^{\ell^r} \notin N_{L/K}(J(L))$ by Corollary 3.2. If $\Phi((\alpha^{\ell^r})_{v_2}) \neq 1$, then the last condition holds. Assume that $\phi((\alpha^{\ell^r})_{v_2}) = 1$. Since ℓ^r is the ramification index of L at ∞, $\phi((\alpha^{\ell^r})_{\infty}) = 1$. Moreover $\phi((\alpha^{\ell^r})_v) = 1$ for $v \neq v_1, v_2$. Hence $\phi((\alpha^{\ell^r})_{v_1}) = 1$ by the product formula and so $\alpha^{\ell^r} \in N_{L/K}(J(L))$. Therefore we get the result.

COROLLARY 3.14. *Let L/K be a cyclic extension of degree ℓ. Then $h(\mathcal{O}_L)$ is prime to ℓ if and only if one of the following conditions holds.*

(a) *precisely one finite place is ramified in L*
(b) *L is totally real, precisely two finite places v_1 and v_2 are ramified in L and the degree of v_2 is prime to ℓ.*

PROOF. Suppose that $h(\mathcal{O}_L)$ is prime to ℓ and exactly two finite places v_1 and v_2 are ramified in L. Then $G_+(L/K) \neq G(L/K)$. Suppose that L is ramified at ∞. Then $\phi((\alpha^{\ell})_{v_2}) \neq 1$ by Theorem 3.13. However $[L : K] = \ell$ implies that $\alpha^{\ell} \in N_{L/K}(J(L))$, which is a contradiction. Therefore L must be totally real and $\phi((\alpha)_{v_2}) \neq 1$. This last condition is equivalent to the one that the degree of v_2 is prime to ℓ.

Conversely, assume (b). Suppose $h(\mathcal{O}_L)$ is not prime to ℓ. Then $G(L/K) \neq L$. Therefore $G(L/K) = G_+(L/K)$ because $[G_+(L/K) : L] = \ell$ a prime number. Since L is totally real, $\alpha \in N_{L/K}(J(L))$ by Corollary 3.2. This in turn implies that $\phi((\alpha)_{v_2}) = 1$, a contradiction.

REMARK 3.15. Unlike in the classical case, the converse of Theorem 3.13 does not hold, because the ramification type at ∞ is not unique. One can prove the above corollary using Example 1.2 in an explicit way, once we have Proposition 2.4.

COROLLARY 3.16. *Let L, not necessarily a subfield of $\widetilde{C}$, be a cyclic extension of degree ℓ of K with class number prime to ℓ. Then L is one of the following, with $a \in \mathbb{F}_q^*$,*

(i) $L = K(\sqrt[\ell]{ap(T)^m})$, *$p(T)$ any irreducible monic polynomial*;

(ii) $L = K(\sqrt[\ell]{ap_1(T)^{m_1}p_2(T)^{m_2}})$, *$p_1(T)$ and $p_2(T)$ are monic irreducible polynomials with* $\ell \mid m_1 \deg p_1 + m_2 \deg p_2$ *and* $\ell \nmid \deg p_2$;

(iii) $L = \mathbb{F}_{q^\ell}(T)$.

PROOF. The condition that L is totally real is equivalent to the condition $\ell \mid m_1 \deg p_1 + m_2 \deg p_2$ with some appropriate a' in the case that L is contained in $\widetilde{C}$. If we vary the sign function, then we can relax the condition on a so that L is either ramified or splits completely at ∞. Suppose that L is inert at ∞, and $L \neq \mathbb{F}_{q^\ell}(T)$. Then one can use [6, Lemma 4.1] to show that $\ell \mid h(\mathcal{O}_L)$. Hence we have the result.

References

[1] R. Clement, 'The genus field of an algebraic function field', *J. Number Theory* **40** (1992), 359–375.
[2] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math. 24 (Amer. Math. Soc., Providence, 1983).
[3] H. Hasse, 'Zur Geschlecht Theorie in quadratischen Zahlkörpern', *J. Math. Soc. Japan* **3** (1951), 45–51.
[4] D. Hayes, 'Explicit class field theory for rational function fields', *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
[5] ———, 'Stickelberger elements in function fields', *Compositio Math.* **55** (1985), 209–239.
[6] M. Rosen, 'The Hilbert class field in function fields', *Exposition. Math.* **5** (1987), 365–378.

Department of Mathematics
Korea Advanced Institute of Science and Technology
Taejon, 305-701
Korea