Commun. Korean Math. Soc. **22** (2007), No. 2, pp. 163–171

DETERMINATION OF ALL SUBFIELDS OF CYCLOTOMIC FUNCTION FIELDS WITH DIVISOR CLASS NUMBER TWO

JAEHYUN AHN AND HWANYUP JUNG

ABSTRACT. In this paper, we determine all subfields of cyclotomic function fields with divisor class number two. We also give the generators of such fields explicitly.

1. Introduction

Let $k = \mathbb{F}_q(T)$ be the rational function field over the finite field $\mathbb{F}_q$ with q elements and $\mathbb{A} = \mathbb{F}_q[T]$ the ring of polynomials. Let ∞ be the prime divisor of k associated to $(1/T)$. For each polynomial $N \in \mathbb{A}$, one uses the Carlitz module to construct the N-th cyclotomic function field K_N and its maximal real subfield K_N^+. For the theory of cyclotomic function fields, we refer to the Rosen's Book ([12, Chap.12]).

Let K be a finite abelian extension of k which is contained in some cyclotomic function field. By the conductor of K, we mean the monic polynomial $N \in \mathbb{A}$ such that K_N is the smallest cyclotomic function field containing K and we denote it by $cond(K)$. Let $K^+ = K \cap K_N^+$ be the maximal real subfield of K, i.e., the maximal subfield of K on which ∞ splits completely. We say that K is a *real* extension of k if $K = K^+$ and *imaginary* otherwise. Let us denote by g_K and h_K the genus and the divisor class number of K, respectively. The aim of this paper is the determination of all subfields K of cyclotomic function fields with $h_K = 2$. In section 2, based on the work of Leitzel, Madan and Queen [10], we show that it is enough to consider the fields K with $g_K = 1$ when $q = 2, 3, 4$ and 5 (Proposition 2.1). Finally we determine all fields K with $h_K = 2$ among these explicitly (Theorem 3.1 and 3.2).

2. Divisor class number two and genus

Let K be a finite abelian extension of k with $h_K = 2$. Since $g_K = 0$ implies $h_K = 1$, we must have $g_K \geq 1$. By Theorem 3 in [10], it is sufficient to consider the following cases;

Received January 23, 2006.
2000 *Mathematics Subject Classification.* 11R58.
Key words and phrases. cyclotomic function field, divisor class number, genus.
This work was supported by Korea Research Foundation Grant (KRF-2004-002-C0004).

(i) $q = 2$ and $g_K \leq 5$
(ii) $q = 3$ and $g_K \leq 2$
(iii) $q = 4$ or 5 and $g_K = 1$.

From now on, by a finite abelian extension K of k we always assume that K is contained in some cyclotomic function fields over k. Let $S_\infty(K)$ be the set of all prime divisors of K lying above ∞. The primes in $S_\infty(K)$ are called the infinite primes of K. In our case, the following proposition shows that it is sufficient to consider the fields K with $g_K = 1$ when $q \leq 5$.

Proposition 2.1. *Let K be a finite abelian extension of k.*

(i) *If $g_K = 1$, then h_K is equal to the number of primes of K of degree one.*
(ii) *If $h_K = 2$, then $g_K = 1$ and $q \leq 5$.*

Proof. (i) follows immediately from the equation (13) in [10].

(ii) Let N_d be the number of primes of K of degree d. Then

$$N_1 \geq |S_\infty(K)| = [K^+ : k].$$

At first, we assume that $q = 2, g_K \geq 2$ and $h_K = 2$. Since K is a real extension of k, $N_1 \geq 2$. Then by Theorem 4 in [10], $(g_K, N_1, N_2) = (2, 2, 1)$. Thus

$$|S_\infty(K)| = [K : k] = 2.$$

Since $N_1 = 2$ and ∞ splits completely in K, the inertia degree of (T) and $(T + 1)$ in the extension K/k is 2. Thus $N_2 \geq 2$, which is a contradiction. Hence if $q = 2$ and $h_K = 2$, then $g_K = 1$. Now we consider the case that $q = 3, g_K = 2$ and $h_K = 2$. Then by Theorem 4 in [10], $N_1 = 0$. But

$$N_1 \geq |S_\infty(K)| = [K^+ : k] \geq 1,$$

and so this case is impossible. Hence if $q = 3$ and $h_K = 2$, then $g_K = 1$. □

From Proposition 2.1, we need the result of the subfields of cyclotomic function fields with $g_K = 1$. In [8], we have determined all such subfields K when $q \geq 3$.

Lemma 2.2. *Let $q = 2$. Let K be a real finite abelian extension of k. Then $h_K = 1$ if and only if $g_K = 0$. In this case $K(\neq k)$ is $K_{P_1^2}$ or K_{P_2}, where $\deg P_1 = 1$ and $\deg P_2 = 2$.*

Proof. If $g_K = 0$, then $h_K = 1$ obviously. Conversely, if $h_K = 1$, then $g_K \leq 4$ by Theorem 1 in [11]. When $g_K = 1$, h_K is equal to the number of prime divisors of K of degree one. Since K is a real extension of k,

$$1 = h_K \geq |S_\infty(K)| = [K : k].$$

Thus $K = k$, which is impossible (because $g_K = 1$). If $g_K = 2$, then, as in the proof of Theorem 2 in [11],

$$h_K = (N_1^2 + N_1 + 2N_2 - 4)/2 = 1.$$

Thus $N_1^2 + N_1 + 2N_2 = 6$. Since $N_1 \geq n = [K : k] \geq 2$, we have $(N_1, N_2, n) = (2, 0, 2)$. Since $N_1 = 2$ and ∞ splits completely in K, two prime divisors (T) and $(T+1)$ must inert in K. Then $N_2 \geq 2$, which is impossible. Assume that $g_K = 3$ or 4. Since $N_1 \geq |S_\infty(K)| \geq 1$, there is no K with $h_K = 1$ by Theorem 2 in [11].

When $g_K = 0$, we can see that the same argument of section 4 in [7] holds for the case $q = 2$. Thus the last statement follows from Proposition 4.1, 4.2 and Theorem 4.3 in [7]. □

Almost the same argument as in [8, Thoerems 3.4-3.5] gives

Proposition 2.3. *Let $q = 2$ and K be a real extension of k with $g_K = 1$. Then K is one of the followings;*

(1) *K is a quadratic extension of k with $cond(K) = P_1^4, P_2^2$ or $P_1^2 P_1'^2$, where $\deg P_1 = \deg P_1' = 1$ and $\deg P_2 = 2$,*
(2) *K is a quartic extension of k with $cond(K) = P_1^3$, where $\deg P_1 = 1$,*
(3) *K is a biquadratic extension of k with $cond(K) = P_1^2 P_1'^2$, where $\deg P_1 = \deg P_1' = 1$,*

By Proposition 2.3, it is easy to check that Theorem 3.4 and 3.5 in [8] holds without assuming that $q \geq 3$. In this paper we use results in [8] without assuming that $q \geq 3$.

3. Divisor class number two problem

In this section, we determine all subfields K of cyclotomic function fields with $h_K = 2$. By proposition 2.1, it is equivalent to determine all subfields K with $g_K = 1$ and $N_1 = 2$ when $q = 2, 3, 4, 5$. Since any infinite prime divisor of K has degree one,

$$[K^+ : k] = |S_\infty(K)| \leq 2.$$

If $[K^+ : k] = 2$, then $N_1 = |S_\infty(K)| = 2$. Thus any monic polynomials $P \in \mathbb{A}$ of degree one must have inertia degree $f_P \geq 2$ in the extension K/k. If $[K^+ : k] = 1$, then exactly one monic polynomial $P \in \mathbb{A}$ must be totally ramified in K and the others must have inertia degree ≥ 2.

Let us denote by X_K the character group of $\mathrm{Gal}(K/k)$. For a fixed monic irreducible polynomial Q, let $Y_K = \{\chi \in X_K : \chi(Q) \neq 0\}$ and $Z_K = \{\chi \in X_K : \chi(Q) = 1\}$. From [14, Chap. 3], we know that $[Y_K : Z_K] = f_Q, |Z_K| = g_Q$, the number of primes lying above Q.

3.1. K/k is a real extension with $h_K = 2$

Theorem 3.1. *Let K/k be a real extension with $h_K = 2$. Then $[K : k] = 2$ and, up to isomorphisms $(x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*)$, K is one of the following cases;*

(1) *$q = 2$, $K = k(\alpha)$, α is a root of $y^2 + y = 1/(T^2 + T + 1)$,*
(2) *$q = 4$, $K = k(\alpha)$, α is a root of $y^2 + y = 1/(T^2 + T + \omega)$ or $y^2 + y = \omega^2/(T^2 + wT + 1)$, where ω is a generator of $\mathbb{F}_4^*$,*

(3) $q = 3$, $K = k(\sqrt{T^4 + 2T^2 + 2})$,
(4) $q = 5$, $K = k(\sqrt{T^4 + 2})$.

Proof. Let $p = char(k)$. First suppose that $[K : k]$ is p-power. By Theorem 3.4 in [8], it suffices to consider the following cases;

(i) $p = 2$, K is a quadratic extension of k with conductor P_1^4, $\deg P_1 = 1$,
(ii) $p = 2$, K is a quadratic extension of k with conductor P_2^2, $\deg P_2 = 2$,
(iii) $p = 2$, K is a quadratic extension of k with conductor $P_1^2 P_1'^2$, $\deg P_1 = \deg P_1' = 1$.

If K is an extension of cases (i) or (iii), then $f_{P_1} = 1$ or $f_{P_1} = f_{P_1'} = 1$. Thus $h_K > 2$. If K is an extension of case (ii), then $q = 2$ or 4.

First suppose $q = 2$. Then we have

$$\mathrm{Gal}(K_{P_2^2}/k) \cong (\mathbb{Z}/3) \oplus (\mathbb{Z}/2) \oplus (\mathbb{Z}/2)$$

and $P_2 = T^2 + T + 1$. By [5, Section 3], we see that

$$\mathrm{Gal}(K_{P_2^2}/k) \cong (\mathbb{F}_q[T]/P_2^2)^* \cong \langle \overline{T^2+1} \rangle \times \langle \overline{T^2+T} \rangle \times \langle \overline{T^3+T^2+T+1} \rangle,$$

where $\overline{M}$ denotes $M \pmod{P_2}$ for $M \in \mathbb{A}$. It is easily checked that $T \pmod{P_2^2}$ corresponds to $(1,1,1)$ and $T+1 \pmod{P_2^2}$ corresponds to $(2,0,1)$. Since

$$X_{K_{P_2^2}} \cong (\mathbb{Z}/3) \oplus (\mathbb{Z}/2) \oplus (\mathbb{Z}/2),$$

the nontrivial element of X_K corresponds to $(0,0,1)$, $(0,1,0)$ or $(0,1,1)$. Clearly the character which corresponds to $(0,0,1)$ takes -1 at both prime ideals (T) and $(T+1)$. Now we want to find a generator for K/k. By [4, Proposition 3.1], K must be isomorphic to $\mathbb{F}_q(x,y)$ with

$$y^2 + xy = x^3 + x^2 + 1.$$

Let $y_1 = (y+1)/x$. Then

$$y_1^2 + y_1 = x + 1 + 1/x.$$

Let $x_1 = x + 1/(y_1^2 + y_1 + 1)$. Then

$$x_1^2 + x_1 = \frac{1}{y_1^2 + y_1 + 1}.$$

Let $T = y_1, y_2 = x_1$. Then

$$y_2^2 + y_2 = \frac{1}{T^2 + T + 1}.$$

By [13, Proposition III.7.8], it is immediately checked that this equation defines the required quadratic extension K. Therefore we have $K = k(\alpha)$, where α is any root of $y^2 + y = 1/(T^2 + T + 1)$. Next suppose that $q = 4$. By the similar argument in the case $q = 2$, we find that $K = k(\alpha)$, where α is a root of $y^2 + y = 1/(T^2 + T + \omega)$ or $y^2 + y = \omega^2/(T^2 + \omega T + 1)$. Here ω is a generator of $\mathbb{F}_4^*$.

Now suppose $([K : k], p) = 1$. Since $[K : k] = 2$, we have $q = 3$ or 5. By [8, Theorem 3.5], it suffices to consider the following cases;

(i) $K = k(\sqrt{P_4}), \deg P_4 = 4$,
(ii) $K = k(\sqrt{P_1P_3}), \deg P_1 = 1, \deg P_3 = 3$,
(iii) $K = k(\sqrt{P_2P_2'}), \deg P_2 = \deg P_2' = 2$,
(iv) $K = k(\sqrt{P_1P_1'P_2}), \deg P_1 = \deg P_1' = 1, \deg P_2 = 2$,
(v) $K = k(\sqrt{P_1P_1'P_1''P_1'''}), \deg P_1 = \deg P_1' = \deg P_1'' = \deg P_1''' = 1$.

If a monic irreducible polynomial P divides $cond(K)$, then P must totally ramify in K/k because $[K : k] = 2$. Thus we do not need to check the cases (ii), (iv) and (v).

Case (i) : Let $X_{K_{P_4}} = \langle\chi\rangle$. Then $X_K = \langle\chi^{(q^4-1)/2}\rangle$. Since $[K^+ : k] = 2$, all monic irreducible polynomials of degree one must inert in K/k. Thus we must find all monic irreducible polynomials P_4 of degree 4 such that $\{P_4(\alpha)|\alpha \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^*\backslash(\mathbb{F}_q^*)^2$. An elementary calculation shows that only $P_4 = T^4 + 2T^2 + 2$ (resp. $P_4 = T^4 + 2$) for $q = 3$ (resp. $q = 5$) satisfies the above condition. Thus, up to isomorphisms $(x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*)$, we have

$$K = \begin{cases} k(\sqrt{T^4 + 2T^2 + 2}) & \text{if } q = 3 \\ k(\sqrt{T^4 + 2}) & \text{if } q = 5. \end{cases}$$

Case (iii) : By the similar argument in Case (i), we must find all pairs of monic irreducible polynomials P_2, P_2' of degree 2 such that $\{P_2(\alpha)P_2'(\alpha)|\alpha \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^*\backslash(\mathbb{F}_q^*)^2$. A simple calculation shows that no such pairs of polynomials exist. It completes the proof. □

3.2. K/k is an imaginary extension with $h_K = 2$

Theorem 3.2. *Let K/k be an imaginary extension with $h_K = 2$. If K/k is totally imaginary, then up to isomorphisms $(x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*)$, K is one of the following cases;*

(1) $q = 5$, $K = k(\sqrt{-(T+3)}\sqrt[4]{-T})$,
(2) $q = 3$, $K = k(\sqrt{-T(T^2+T+2)})$,
(3) $q = 5$, $K = k(\sqrt{-T(T^2+2)})$.

If K/k is not totally imaginary, then up to isomorphisms $(x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*)$, K is one of the following cases;

(1) $q = 5$, $K = k(\sqrt[4]{T^2+3})$,
(2) $q = 5$, $K = k(\sqrt{-(T+3)}, \sqrt[4]{-T})$,
(3) $q = 3$, $K = k(\sqrt{T^2+1}, \sqrt{-(T+1)})$,
(4) $q = 5$, $K = k(\sqrt{T^2+2}, \sqrt{-T})$.

Proof. First assume that K/k is totally imaginary. By [8, Theorem 4.2], it suffices to consider the following cases;

(i) $K = k(\sqrt[3]{-P_2^2}), \deg P_2 = 2, q \equiv 1 \pmod 3$,
(ii) $K = k(\sqrt[3]{P_1P_1'}), \deg P_1 = \deg P_1' = 1, q \equiv 1 \pmod 3$,
(iii) $K = k(\sqrt{-P_1}\sqrt[4]{-P_1'}), \deg P_1 = \deg P_1' = 1, q \equiv 1 \pmod 4$,

(iv) $K = k(\sqrt{-P_1}, \sqrt[3]{-P_1'}), \deg P_1 = \deg P_1' = 1, q \equiv 1 \pmod 6$,
(v) $K = k(\sqrt{-P_3}), \deg P_3 = 3, q$ odd,
(vi) $K = k(\sqrt{-P_1P_2}), \deg P_1 = 1, \deg P_2 = 2, q$ odd,
(vii) $K = k(\sqrt{-P_1P_1'P_1''}), \deg P_1 = \deg P_1' = \deg P_1'' = 1, q$ odd.

In any cases, K/k must have exactly one finite prime of degree one. For cases (ii) and (vii), each monic irreducible divisor P_i of the conductor is of degree one and totally ramifies in K/k. Thus we discard these cases. Since $q = 2, 3, 4$ or 5, we also discard the case (iv). In the case (i), an elementary calculation shows that h_K is 1 or 3.

Case (iii) : Clearly, $q = 5$. Write

$$X_{K_{P_1P_1'}} \cong X_{K_{P_1}} \times X_{K_{P_1'}} = \langle \chi_1 \rangle \times \langle \chi_2 \rangle.$$

Then $X_K = \langle \chi_1^2\chi_2 \rangle$. We may assume that $P_1' = T$. Write $P_1 = T + \alpha$ with $\alpha \in \mathbb{F}_5^*$. Since P_1' totally ramifies in K/k, the other monic polynomials Q of degree one must have $f_Q \geq 2$. Since $\chi_2(P_1) = \chi_2(\alpha)$, we must have $\alpha \in \{2, 3\}$. For $\alpha = 2$, we have

$$(\chi_2^2\chi_2)(T+1) = \chi_2^2(4)\chi_2(1) = 1.$$

Thus $T + 1$ splits completely in K/k and so $h_K \geq 6$. For $\alpha = 3$, we have

$$\begin{aligned}(\chi_1^2\chi_2)(T+1) &= \chi_1^2(3)\chi_2(1) = -1,\\ (\chi_1^2\chi_2)(T+2) &= \chi_1^2(4)\chi_2(2) = \exp(2\pi i/4) \neq 1,\\ (\chi_1^2\chi_2)(T+4) &= \chi_1^2(1)\chi_2(4) = -1.\end{aligned}$$

Thus $h_K = 2$ and we have $K = k(\sqrt{-(T+3)}\sqrt[4]{-T})$ with $q = 5$.

Case (v) : By [3, Corollary 4.7], we see that h_K is odd.

Case (vi) : Suppose that $q = 3$. Under isomorphisms $T \mapsto T + \alpha, \alpha \in \mathbb{F}_q^*$, we may assume that $P_1 = T$ and $P_2 \in \{T^2+1, T^2+T+2, T^2+2T+2\}$. Since ∞ and P_1 totally ramify in K/k, $T+1, T+2$ must be inert. We write

$$X_K = \{1, \chi_1\chi_2^4\},$$

where each χ_i can be viewed as a primitive character of $(\mathbb{F}_q[T]/P_i)^*$. Let $P_2 = T^2 + T + 2$. Then T is a primitive root modulo $T^2 + T + 2$. And $T + 1 \equiv T^7$ and $T + 2 \equiv T^6 \pmod{T^2 + T + 2}$. Thus

$$(\chi_1\chi_2^4)(T+1) = 1 \cdot (-1) = -1, \quad (\chi_1\chi_2^4)(T+2) = (-1) \cdot 1 = -1.$$

An elementary calculation shows that other choices of P_2 do not satisfy this condition. Thus we have

$$K = k(\sqrt{-T(T^2+T+2)}).$$

Suppose that $q = 5$. We may assume that $P_1 = T$. Again an elementary calculation shows that only $P_2 = T^2 + 2$ satisfies the condition for $h_K = 2$. Thus we have

$$K = k(\sqrt{-T(T^2+2)})$$

up to isomorphisms $T \mapsto T + \alpha, \alpha \in \mathbb{F}_q^*$. It is easy to see that this K is isomorphic to $\mathbb{F}_q(x, y)$ with $y^2 = x^3 + 2x$ in [4, Proposition 3.1] $(x \mapsto -x.)$

Next assume that K/k is not totally imaginary and $cond(K) = cond(K^+)$. By [8, Theorem 4.4], it suffices to consider the following cases;

(i) $K = k(\sqrt[4]{P_2}), \deg P_2 = 2, q \equiv 1 \pmod 4$,
(ii) $K = k(\sqrt{-P_1}, \sqrt[4]{-P_1'}), \deg P_1 = \deg P_1' = 1, q \equiv 1 \pmod 4$,
(iii) $K = k(\sqrt[3]{-P_1}, \alpha), \deg P_1 = 1$, $\alpha \in K^+_{P_1^2}$ such that $k(\alpha)$ is a quadratic subfield of $K^+_{P_1^2}$, $q = 4$.

Case (i) : Clearly, $q = 5$. We must find all monic irreducible polynomials P_2 of degree 2 such that

$$\{P_2(\alpha) | \alpha \in \mathbb{F}_5\} \subseteq \mathbb{F}_5^* \backslash (\mathbb{F}_5^*)^4 = \{2, 3, 4\}.$$

Up to isomorphisms $(x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*)$, it suffices to consider two polynomials $P_2 = T^2 + 2$ or $T^2 + 3$. If $P_2 = T^2 + 2$, $P_2 \equiv 1 \pmod{T + 3}$. Thus $h_K \geq 6$. (In fact, $h_K = 10$). If $P_2 = T^2 + 3$, $P_2 \equiv 2, 4 \pmod{T + \alpha}, \alpha \in \mathbb{F}_q$. Thus $h_K = 2$ and we have

$$K = k(\sqrt[4]{T^2 + 3}), q = 5.$$

Case (ii) : We have $q = 5$. Write

$$X_{K_{P_1 P_1'}} \cong X_{K_{P_1}} \times X_{K_{P_1'}} = \langle \chi_1 \rangle \times \langle \chi_2 \rangle.$$

Then $X_K = \langle \chi_1^2, \chi_2 \rangle$. We may assume that $P_1' = T, P_1 = T + \alpha, \alpha \in \mathbb{F}_q^*$. Since the ramification index of P_1 in K/k is 2, we must have

$$\chi_2(P_1) = \chi_2(\alpha) \neq 1, \quad \chi_1^2(T) = \chi_1^2(-\alpha) \neq 1.$$

Thus $\alpha \in \{2, 3\}$. For $\alpha = 2$, we have

$$\chi_1^2(T + 1) = \chi_1^2(4) = 1, \quad \chi_2^2(T + 1) = \chi_2^2(1) = 1.$$

Thus $(T + 1)$ splits completely in K. Thus $h_K \geq 10$. For $\alpha = 3$, we have

$$\begin{aligned} &\chi_1^2(T + 1) = \chi_1^2(3) = -1, \\ &\chi_1^2(T + 2) = \chi_1^2(2) = \exp(2\pi i/4) \neq 1, \\ &\chi_1^2(T + 4) = \chi_1^2(4) = -1. \end{aligned}$$

Thus $h_K = 2$ and we have

$$K = k(\sqrt{-(T + 3)}, \sqrt[4]{-T}) \text{ with } q = 5.$$

Case (iii) : Since $cond(K) = cond(K^+) = P_1^2$, P_1 is totally ramified in K/k. Thus $h_K > 2$.

Finally, assume that K/k is not totally imaginary and $cond(K) \neq cond(K^+)$. By [8, Theorem 4.6], we need to consider the following cases;

(i) $K = k(\sqrt{P_2}, \sqrt{-P_1}), \deg P_2 = 2, \deg P_1 = 1, q$ odd,
(ii) $K = k(\sqrt{-P_1}, \sqrt{P_1' P_1''}), \deg P_1 = \deg P_1' = \deg P_1'' = 1, q$ odd.

Case (i) : We have $q = 3$ or 5. We write $\chi_1 = \chi_{P_1}, \chi_2 = \chi_{P_2}$. Suppose that $q = 3$. We may assume that $P_2 = T^2 + 1$ under isomorphisms ($x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*$). Since T is a square modulo P_2, we have $P_1 = T + 1$ or $T + 2$. For $P_1 = T + 2$, we have

$$\chi_1(T) = \chi_1(1) = 1, \quad \chi_2^{(q^2-1)/2}(T) = \chi_2^4(T) = 1.$$

Thus $h_K > 2$. For $P_1 = T + 1$, we have

$$\chi_1(T) = \chi_1(2) = -1, \quad \chi_2^4(T + 2) = -1.$$

Thus $h_K = 2$ and we have

$$K = k(\sqrt{T^2 + 1}, \sqrt{-(T + 1)}) \text{ with } q = 3.$$

Suppose that $q = 5$. Under isomorphisms ($x \mapsto x + \alpha, \alpha \in \mathbb{F}_q^*$), we may assume that $P_2 = T^2 + 2$ or $T^2 + 3$. Suppose that $P_2 = T^2 + 2$. Since $T + 2$ is a square modulo P_2, we have $P_1 = T, T + 1$ or $T + 4$. For $P_1 = T + 1$, we have

$$\chi_1^2(T + 2) = \chi_1^2(1) = 1, \quad \chi_2^2(T + 2) = 1.$$

Thus $h_K > 2$. For $P_1 = T + 4$, we have

$$\chi_2^{12}(T + 3) = 1, \quad \chi_1^2(T + 3) = \chi_1^2(4) = 1.$$

Thus $h_K > 2$. For $P = T$, we have

$$\chi_2^{12}(T + 1) = -1, \quad \chi_1^2(T + 2) = \chi_1^2(2) = -1,$$
$$\chi_1^2(T + 3) = \chi_1^2(3) = -1, \quad \chi_2^{12}(T + 4) = -1.$$

Thus $h_K = 2$ and we have

$$K = k(\sqrt{T^2 + 2}, \sqrt{-T}) \text{ with } q = 5.$$

Suppose that $P_2 = T^2 + 3$. Then $P_1 \in \{T, T + 2, T + 3\}$. It is easily checked that $h_K > 2$ in any cases.

Case (ii) : We have $q = 3$ or 5. We write $\chi_1 = \chi_{P_1}, \chi_2 = \chi_{P_1'}, \chi_3 = \chi_{P_1''}$ Suppose that $q = 3$. We may assume that $P_1 = T$, $P_1' = T + 1$ and $P_1'' = T + 2$. Since

$$\chi_1^{(q-1)/2}(P_1') = \chi_1(1) = 1,$$

thus $f_{P_1'} = 1$ and so $h_K \geq 4$. Suppose that $q = 5$. We may assume that $P_1 = T$ and so $P_1', P_1'' \in \{T + 1, T + 2, T + 3, T + 4\}$. Both $\chi_1^2(P_1')$ and $\chi_1^2(P_1'')$ must not be 1. Thus $\{P_1', P_1''\} = \{T + 2, T + 3\}$, say $P_1' = T + 2, P_1'' = T + 3$. Then

$$\chi_2^{(q-1)/2}\chi_3^{(q-1)/2}(P_1) = \chi_2^2(3)\chi_3^2(2) = (-1) \cdot (-1) = 1.$$

Thus $f_{P_1} = 1$ and so $h_K \geq 4$. □

References

[1] B. Angles, *On Hilbert class field towers of global function fields*: in "Drinfeld modules, modular schemes and applications," 261–271, World Sci. Publishing, River Edge, NJ 1997.

[2] R. Auer, *Ray class fields of global function fields with many rational places*, Dissertation at the University of Oldenburg, `www.bis.uni-oldenburg.de/dissertation/ediss.html`, 1999.

[3] S. Bae, H. Jung, and J. Ahn, *Class numbers of some abelian extensions of rational function fields*, Math. Comp. **73** (2004), no. 245, 377–386.

[4] D. Le Brigand, *Classification of algebraic function fields with divisor class number two*, Finite Fields Appl. **2** (1996), no. 2, 153–172.

[5] H. L. Claasen, *The group of units in* $\mathrm{GF}(q)[x]/(a(x))$, Nederl. Akad. Wetensch. Proc. Ser. A 80=Indag. Math. **39** (1977), no. 4, 245–255.

[6] R. Clement, *The genus field of an algebraic function field*, J. Number Theory **40** (1992), no. 3, 359–375.

[7] H. Jung and J. Ahn, *Divisor class number one problem for abelian extensions over rational function fields,* to appear in J. of Algebra.

[8] ———, *Determination of all subfields of cyclotomic function fields with genus one*, Commun. Korean math. Soc. **20** (2005), no. 2, 259–273.

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

[10] J. Leitzel, M. Madan, and C. Queen, *Algebraic function fields with small class number.* J. of Number Theory **7** (1975), 11–27.

[11] M. Madan and C. Queen, *Algebraic function fields of class number one,* Acta Arith. **20** (1972), 423–432.

[12] M. Rosen, *Number theory in function fields.* Graduate Texts in Mathematics **210**, Springer-Verlag, New York, 2002.

[13] H. Stichtenoth, *Algebraic function fields and codes,* Universitext, Springer-Verlag, (1993).

[14] L. Washington, *Introduction to cyclotomic fields,* Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

JAEHYUN AHN
DEPARTMENT OF MATHEMATICS
CHUNGNAM NATIONAL UNIVERSITY
DAEJON 305-764, KOREA
E-mail address: `jhahn@cnu.ac.kr`

HWANYUP JUNG
DEPARTMENT OF MATHEMATICS EDUCATION
CHUNGBUK NATIONAL UNIVERSITY
CHEONGJU 361-763, KOREA
E-mail address: `hyjung@chungbuk.ac.kr`