Commun. Korean Math. Soc. **20** (2005), No. 2, pp. 259–273

DETERMINATION OF ALL SUBFIELDS OF CYCLOTOMIC FUNCTION FIELDS WITH GENUS ONE

HWANYUP JUNG* AND JAEHYUN AHN

ABSTRACT. In this paper we determine all subfields with genus one of cyclotomic function fields over rational function 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 monic 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 more details on the theory of cyclotomic function fields we refer to the Rosen's book ([7, Chap. 12]).

In [6], Kida and Murabayashi have determined all cyclotomic function fields and their maximal real subfields with divisor class number one, based on previous work of Madan, Queen, Armitage and Macrae. Moreover they also have determined which of the above abelian extensions has genus one. In [5], the authors have determined all subfields of cyclotomic function fields with divisor class number one (when $q \geq 3$).

In this paper, we determine all subfields of cyclotomic function fields with genus one (when $q \geq 3$). From now on, by a finite abelian extension K of k we always assume that it 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. Let $K^+ = K \cap K_N^+$ be the maximal real subfield of K. We say that K is a *real* extension of k if $K = K^+$ and *imaginary* otherwise. An imaginary extension K of k is called *totally imaginary* if $K^+ = k$. The layout of this paper is as follow. In section two we give some basic tools needed

Received October 06, 2004.
2000 Mathematics Subject Classification: 11R58.
Key words and phrases: cyclotomic funtion fields, genus, divisor class number.
* This work was supported by Chungbuk National University Grant 2003.

in this paper. In section three we determine all real extensions K of k with genus one (Theorem 3.3 and 3.4). In section four we determine all imaginary extensions K of k with genus one (Theorem 4.2, 4.4 and 4.6).

The results obtained in this article will be used in a preparatory work where we determine all finite abelian extensions K of k with divisor class number two.

2. Preliminaries

For any algebraic function field K, denote by g_K the genus of K. The following Lemma is well-known (for example, [8, p.88]).

LEMMA 2.1 (Riemann-Hurwitz formula). *Let L/K be a finite abelian extension with the same constant field. Then we have*

$$2g_L - 2 = (2g_K - 2)[L : K] + \deg(\mathcal{D}(L/K)), \tag{2.1}$$

where $\mathcal{D}(L/K)$ is the different of L/K. Especially $g_L \geq g_K$.

When L/K is a finite abelian extension, the different $\mathcal{D}(L/K)$ of L/K can be calculated from the following formula (for example, [2, p.24]).

LEMMA 2.2 (Different formula). *Let L/K be a finite abelian extension with Galois group G. Let $\mathfrak{p}$ be a prime divisor of K and $\mathfrak{q}$ be any prime divisor of L lying above $\mathfrak{p}$. Let $d(\mathfrak{q}|\mathfrak{p})$ be the exponent of $\mathfrak{q}$ in the different $\mathcal{D}(L/K)$. Then we have*

$$d(\mathfrak{p}|\mathfrak{q}) = \sum_{n=0}^{\infty} \Big(|G^0(\mathfrak{p}, L/K)| - (G^0(\mathfrak{p}, L/K) : G^n(\mathfrak{p}, L/K)) \Big),$$

where $G^n(\mathfrak{p}, L/K)$ denotes the n-th upper ramification group of $\mathfrak{p}$ in L.

Since $\mathrm{Gal}(K_M/k) \cong (\mathbb{F}_q[T]/M)^*$, we need the following result on the structure of $(\mathbb{F}_q[T]/M)^*$ (see [3, Section 3]).

LEMMA 2.3. *For any monic polynomial $M \in \mathbb{F}_q[T]$, let $H(M)$ be the group of units in $\mathbb{F}_q[T]/M$. Let $M = \prod_{i=1}^{s} M_i^{n_i}$ be the canonical decomposition of M as monic irreducible polynomials M_i of degree d_i. We define for every $i = 1, 2, \ldots, s$ and j with $1 \leq j \leq n_i - 1$ the natural number $x_{i,j}$ by*

$$jp^{x_{i,j}-1} < n_i \leq jp^{x_{i,j}}.$$

For every r, i, t, j subjected to $0 \leq r \leq f-1, 1 \leq i \leq s$, and for every i : $0 \leq t \leq d_i - 1, 1 \leq j \leq n_i - 1$ and $p \nmid j$, define $A_i^{(r,t,j)}(M)$ be cyclic group of order $p^{x_{i,j}}$ and $A(M)$ be the direct product of all $A_i^{(r,t,j)}(M)$.

For $i = 1, \ldots, s$, define $B_i(M)$ be the cyclic group of order $q^{n_i} - 1$ and $B(M)$ be the direct product of $B_i(M), i = 1, \ldots, s$. Then $H(M)$ is isomorphic to the direct product of $A(M)$ and $B(M)$.

By similar arguments in the proof of [1, Lemma 3.2] and [4, Proposition 2.3], we have

LEMMA 2.4. *Let P be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Let ℓ be a natural number such that ℓ divides $q - 1, \ell > 1$. Let $d = \deg P$ and $d_0 = gcd(\ell, d)$. Let n, $1 \leq n \leq \ell/d_0$ be such that $nd \equiv d_0 \pmod{\ell}$. Then the unique cyclic subextension K of K_P/k with degree ℓ is given by $K = k(\sqrt[\ell]{(-1)^{d_0} P^n})$. Furthermore, ℓ divides d if and only if $K \subseteq K_P^+$.*

3. Real extension with genus one

Let K be a finite abelian extension of k. We can decompose it as $K = K_1 \cdot K_2$, where $[K_1 : k]$ is prime to $p = char(k)$ and $[K_2 : k]$ is a p-power.

LEMMA 3.1. *Let K be a real extension of k with $g_K = 1$. Let K_1 and K_2 be defined as above. If K_1 and K_2 are proper subfields of K, then $g_{K_1} = g_{K_2} = 0$.*

PROOF. Since $g_K = 1$, $g_{K_i} \leq 1$ for $i = 1, 2$. Assume that $g_{K_1} = 1$. Then Riemann-Hurwitz formula for K/K_1 implies that K/K_1 is an unramified extension. Thus K_2/k is also unramified extension, i.e., $K_2 = k$. Similarly, we show that if $g_{K_2} = 1$, then $K_1 = k$. □

PROPOSITION 3.2. *Let K be a real extension of k with $g_K = 1$. Then $[K : k]$ is a p-power or prime to p.*

PROOF. Let K_1 and K_2 be defined as above. If $K_1, K_2 \subsetneq K$, by Lemma 3.1, $g_{K_1} = g_{K_2} = 0$. Then K_1 is one of the followings ([5, Section 4]);

(i) K_1 is a subfield of K_P^+ with $\deg P = 2$,
(ii) K_1 is a subfield of $K_{P_1 P_2}^+$ with $\deg P_i = 1 (P_1 \neq P_2)$,
(iii) $K_1 = k(\sqrt{P_1 P_2}, \sqrt{P_1 P_3})$ with $\deg P_i = 1$ for all i and q odd

and K_2 is a subfield of $K_{Q^2}^+$ with $\deg Q = 1$.

In case (i) or (ii), as in the proof of [5, Theorem 4.3], $g_K = (\ell - 1)(p^a - 1)$ with $\ell = [K_1 : k]$ and $p^a = [K_2 : k]$. Thus $g_K = 1$ if and only if $\ell = 2, p^a = 2$. But then $(\ell, p) = 2$, which contradicts the definition of K_1 and K_2.

In case (iii), as in the proof of [5, Theorem 4.3], we have

$$g_K = \begin{cases} 3(p^a-1) & \text{if } Q \neq P_1, P_2, P_3, \\ 2(p^a-1) & \text{otherwise.} \end{cases}$$

Thus $g_K \neq 1$, which proves the Proposition. □

First we consider the case that $[K : k]$ is a p-power. Let $N = \prod_{i=1}^{s} P_i^{m_i}$ be the irreducible decomposition of the conductor of K. Since $[K : k]$ is a p-power, $m_i \geq 2$ for all i. We denote by e_i, g_i and f_i the ramification index, splitting number, and inertia degree of P_i, respectively. Let $\{\mathfrak{P}_{ij} | 1 \leq j \leq g_i\}$ be the set of primes of K lying above P_i. Then $\mathcal{D}(K/k) = \prod_{i=1}^{s} \prod_{j=1}^{g_i} \mathfrak{P}_{ij}^{d(\mathfrak{P}_{ij}|P_i)}$. From [8, Proposition III.8.6], we know that $d(\mathfrak{P}_{ij}|P_i) \geq 2(e_i - 1)$ and that the equality holds if and only if $m_i = 2$.

THEOREM 3.3. *Let K be a real extension of k with $[K : k]$ a p-power. Then $g_K = 1$ if and only if K is one of the followings;*

(1) *$p = 2$, K is a quadratic extension of k with conductor $P^4, \deg P = 1$,*
(2) *$p = 2$, K is a quartic extension of k with conductor $P^3, \deg P = 1$,*
(3) *$p = 2$, K is a quadratic extension of k with conductor $P^2, \deg P = 2$,*
(4) *$p = 3$, K is a cubic extension of k with conductor $P^3, \deg P = 1$,*
(5) *$p = 2$, K is a quadratic or biquadratic extension of K with conductor $P_1^2 P_2^2$ with $\deg P_1 = \deg P_2 = 1$.*

PROOF. Let $n = [K : k]$. From the Riemann-Hurwitz formula for K/k with $g_K = 1$, we have

$$0 \geq -2n + \sum_{i=1}^{s} 2(e_i - 1) f_i g_i d_i = -2n + \sum_{i} 2(e_i - 1)(n/e_i) d_i. \tag{3.1}$$

Note that the equality holds if and only if $m_1 = \cdots = m_s = 2$. From (3.1), we have $\sum_{i=1}^{s} (1 - \frac{1}{e_i}) d_i \leq 1$. Since $e_i \geq 2$ and $e_i | n$ ($= p$-power), we have $e_i \geq p$. Therefore

$$(1 - \frac{1}{p}) \sum_{i=1}^{s} d_i \leq \sum_{i=1}^{s} (1 - \frac{1}{e_i}) d_i \leq 1. \tag{3.2}$$

Since $p \geq 2$, we have $\sum_{i=1}^{s} d_i \leq 2$. Thus it suffices to consider the following cases; $(s, d) = (1, 1), (1, 2)$ or $(s, d_1, d_2) = (2, 1, 1)$. First we consider the case $(s, d) = (1, 1)$. If $m_1 = 2$, then $g_{K_{P2}^+} = 0$ ([6, Theorems 3, 4]) and so $g_K = 0$. Assume that $m_1 \geq 3$. By the Different formula,

$0 \geq -2n+2(n-1)+(n-a)$ with $a|n$ and $a<n$. Thus $a<n\leq a+2$. If $n=a+1$, then $a=(a,n)=1$. Thus $n=2$ and so $p=2$. Now we have $m_1=4$ from (3.1). If $n=a+2$, then $a=(a,n)=(a,2)$. If $a=2$, then $n=4, p=2$ and so $m_1=3$. If $a=1$, then $n=3, p=3$ and so $m_1=3$.

Next consider the case $(s,d)=(1,2)$. In this case we have $p=2, e=2$ from (3.2). Since P is totally ramified in K/k, we have $n=2$. Since the equality holds in (3.1), we have $m_1=2$.

Finally consider the case $(s,d_1,d_2)=(2,1,1)$. In this case we have $p=2, e_1=e_2=2$ from (3.2). In (3.1), the equality holds and so $m_1=m_2=2$. By Lemma 2.3, we see that $\mathrm{Gal}(K_{P_i^2}/k)\simeq \mathbb{F}_q^*\times A(P_i^2)$, where $A(P_i^2)$ is an elementary 2-group. Thus the character group of $K_{P_1^2P_2^2}/k$ can be expressed as

$$\{(\overrightarrow{a},\overrightarrow{b}) : \overrightarrow{a}=(a_0,a_1,\ldots,a_m),\ \overrightarrow{b}=(b_0,b_1,\ldots,b_m)\},$$

where $q=2^m, a_0,b_0\in\mathbb{Z}/(q-1)\mathbb{Z}, a_1,\ldots,a_m,b_1,\ldots,b_m\in\mathbb{Z}/2\mathbb{Z}$. Let X_K be the character group of K. If $(\overrightarrow{a},\overrightarrow{b})\in X_K$, $a_0=b_0=0$ because $e_1=e_2=2$ and $(q-1)$ is odd. In fact, it is easy to check that $(\overrightarrow{a},\overrightarrow{b})$ is real if and only if $a_0=b_0=0$. Therefore we have

$$X_K=\{(\overrightarrow{0},\overrightarrow{0}),(\overrightarrow{a},\overrightarrow{0}),(\overrightarrow{0},\overrightarrow{b}),(\overrightarrow{a},\overrightarrow{b})\} \text{ or } \{(\overrightarrow{0},\overrightarrow{0}),(\overrightarrow{a},\overrightarrow{b})\}.$$

Thus K is the compositum of any quadratic subfield of $K^+_{P_1^2}$ and any quadratic subfield of $K^+_{P_2^2}$ or K is its quadratic subfield with conductor $P_1^2P_2^2$. It completes the proof. □

We consider the case that $[K:k]$ is prime to p. Since $([K:k],p)=1$, the conductor N of K is square-free, say $N=\prod_{i=1}^s P_i$. Let n, d_i, e_i, g_i, f_i, and $\mathfrak{P}_{ij}$ be as above. Since all P_i are tamely ramified, we have $\mathcal{D}(K/k)=\prod_{i=1}^s\prod_{j=1}^{g_i}\mathfrak{P}_{ij}^{(e_i-1)}$.

THEOREM 3.4. *Let K be a real extension of k, whose degree over k is prime to p. Then $g_K=1$ if and only if K is one of the followings;*

(1) $K=k(\sqrt[3]{P})$ *with* $\deg P=3, q\equiv 1 \pmod 3$,
(2) $K=k(\sqrt{P})$ *with* $\deg P=4$, q *odd*,
(3) $K=k(\sqrt{-P_1\sqrt[4]{P_2}})$ *with* $\deg P_1=1, \deg P_2=2, q\equiv 1 \pmod 4$,
(4) $K=k(\sqrt[3]{-P_1^2P_2^2})$ *with* $\deg P_1=1, \deg P_2=2, q\equiv 1 \pmod 3$,
(5) $K=k(\sqrt[3]{-P_3^2P_1}, \sqrt[3]{-P_3^2P_2})$ *or* $k(\sqrt[3]{P_1P_2P_3})$ *with* $\deg P_i=1, q\equiv 1 \pmod 3$,
(6) $K=k(\sqrt{P_1P_3}, \sqrt[3]{-P_2P_3^2})$ *with* $\deg P_i=1, q\equiv 1 \pmod 6$,

(7) $K = k(\sqrt{P_1P_3}, \sqrt[4]{P_2P_3^3})$ or $k(\sqrt[4]{P_1^2P_2P_3})$ *with* $\deg P_i = 1$, $q \equiv 1 \pmod 4$,
(8) $K = k(\sqrt{P_1P_2})$ *with* $\deg P_1 = 1, \deg P_2 = 3$, q *odd*,
(9) $K = k(\sqrt{P_1P_2})$ or $k(\sqrt{P_1}, \sqrt{P_2})$ *with* $\deg P_i = 2$, q *odd*,
(10) $K = k(\sqrt{P_1P_2}, \sqrt{P_3})$ *or* $k(\sqrt{P_1P_2P_3})$ *with* $\deg P_1 = \deg P_2 = 1, \deg P_3 = 2$, q *odd*,
(11) $K = k(\sqrt{P_1P_2}, \sqrt{P_1P_3}, \sqrt{P_1P_4})$, $k(\sqrt{P_1P_2}, \sqrt{P_3P_4})$ or $k(\sqrt{P_1P_2P_3P_4})$ *with* $\deg P_i = 1$, q *odd*.

PROOF. From the Riemann-Hurwitz formula for K/k, we have

$$0 = -2n + \sum_{i=1}^{s}(e_i - 1)f_ig_id_i \geq -2n + n(\sum_{i=1}^{s} d_i) - \frac{n}{2}(\sum_{i=1}^{s} d_i).$$

Thus $\sum_{i=1}^{s} d_i \leq 4$. Note that $\sum_{i=1}^{s} d_i = 4$ if and only if $e_i = 2$ for all i. Since $([K : k], p) = 1$ it is possible only for odd q. If $\sum_{i=1}^{s} d_i \leq 2$, we have $g_K = 0$ ([5, Proposition 4.1]). Thus we must consider the following cases;

(i) $s = 1, d_1 = 3 : N = P, \deg P = 3$,
(ii) $s = 2, d_1 = 1, d_2 = 2 : N = P_1P_2, \deg P_1 = 1, \deg P_2 = 2$,
(iii) $s = 3, d_1 = d_2 = d_3 = 1 :$
$N = P_1P_2P_3, \deg P_i = 1, P_i \neq P_j$ if $i \neq j, q \geq 3$,
(iv) $s = 1, d_1 = 4 : N = P, \deg P = 4$,
(v) $s = 2, d_1 = 1, d_2 = 3 : N = P_1P_2, \deg P_1 = 1, \deg P_2 = 3$,
(vi) $s = 2, d_1 = 2, d_2 = 2 : N = P_1P_2, \deg P_i = 2, P_1 \neq P_2$,
(vii) $s = 3, d_1 = d_2 = 1, d_3 = 2 :$
$N = P_1P_2P_3, \deg P_1 = \deg P_2 = 1, P_1 \neq P_2, \deg P_3 = 2$,
(viii) $s = 4, d_1 = d_2 = d_3 = d_4 = 1 :$
$N = P_1P_2P_3P_4, \deg P_i = 1, P_i \neq P_j$ if $i \neq j, q \geq 4$.

Note that by the Riemann-Hurwitz formula for K/k, we have

$$g_K = 1 \text{ if and only if } \sum_{i=1}^{s}(1 - \frac{1}{e_i})d_i = 2. \tag{3.3}$$

Case (i) $N = P$ with $\deg P = 3$: By (3.3), we have $e_1 = 3$ and so $n = 3$. Note that $n(= 3)$ divides $[K_P^+ : k] = (q^3 - 1)/(q - 1) = q^2 + q + 1$. Thus $q \equiv 1 \pmod 3$. Since K_P^+/k is cyclic and $\deg P = 3$, we have $K = k(\sqrt[3]{P})$ by Lemma 2.4.

Case (iv) $N = P(\deg P = 4)$: By (3.3), $e_1 = 2$ and so $n = 2$. Since 2 divides $q^4 - 1$, q must be odd. Since K_P/k is cyclic, K is unique. Since 2 divides $q - 1$ and 2 divides $d(= 4)$, we have $K = k(\sqrt{P})$ by Lemma 2.4.

Case (ii) $N = P_1P_2(\deg P_1 = 1, \deg P_2 = 2)$: Note that $\mathrm{Gal}(K_{P_1}/k)$ is cyclic of order $q-1$, say $\langle\sigma_1\rangle$. $\mathrm{Gal}(K_{P_2}/k)$ is cyclic of order q^2-1, say $\langle\sigma_2\rangle$. Without loss of generality, we assume that the generator σ of $\mathrm{Gal}(K_{P_1P_2}/K^+_{P_1P_2})$ is mapped to $(\sigma_1, \sigma_2^{-(q+1)})$ under the canonical isomorphism $\mathrm{Gal}(K_{P_1P_2}/k) \simeq \mathrm{Gal}(K_{P_1}/k) \times \mathrm{Gal}(K_{P_2}/k)$. For any finite abelian extension K we denote by X_K the group of Dirichlet characters of K. Let $\chi_i \in X_{K_{P_i}}$ be the character associated to σ_i, that is, $\chi_1(\sigma_1) = \zeta_{q-1} = e^{2\pi i/(q-1)}, \chi_2(\sigma_2) = \zeta_{q^2-1} = e^{2\pi i/(q^2-1)}$. Then, for $0 \le a \le q-2, 0 \le b \le q^2-2$,

$$\chi_1^a\chi_2^b \in X_{K_{P_1P_2}} \text{ is real if and only if } a \equiv b \pmod{q-1}. \tag{3.4}$$

Thus if $\chi_1^a\chi_2^b \in X_K$, then a is uniquely determined by b. By (3.3), we have $1 = \frac{1}{e_1} + \frac{2}{e_2}$. Thus $(e_1, e_2) = (2,4)$ or $(3,3)$. First assume that $(e_1, e_2) = (2,4)$. If $\chi_1^a\chi_2^b \in X_K$, $a = 0, (q-1)/2$ and $b = 0, (q^2-1)/4$, $(q^2-1)/2$, $3(q^2-1)/4$. Note that it is only possible for odd q. Since $(e_1, e_2) = (2,4)$, there are only two possibilities for $\{(a,b)|\chi_1^a\chi_2^b \in X_K\}$, i.e., $\{(a,b)|a = 0, (q-1)/2$ and $b = 0, (q^2-1)/4, (q^2-1)/2, 3(q^2-1)/4\}$ and $\{(0,0), (q-1)/2, (q^2-1)/4), (0, (q^2-1)/2), ((q-1)/2, 3(q^2-1)/4)\}$. By (3.4), the first case is impossible and in the second case we must have $(q^2-1)/4 \equiv (q-1)/2 \pmod{q-1}$. It is easy to check that $(q^2-1)/4 \equiv (q-1)/2 \pmod{q-1}$ if and only if $q \equiv 1 \pmod 4$. Note that quartic subfield of $K^+_{P_1P_2}$ is unique because $K^+_{P_1P_2}/k$ is cyclic. By Lemma 2.4, we see that $k(\sqrt[4]{P_2})$ corresponds to $\{(0,b)|b = 0, (q^2-1)/4, (q^2-1)/2, 3(q^2-1)/4\}$. Thus we have $K = k(\sqrt{-P_1}\sqrt[4]{P_2})$. When $(e_1, e_2) = (3,3)$, similarly we have $K = k(\sqrt[3]{-P_1^2P_2^2})$ with $q \equiv 1 \pmod 3$. The other cases can be treated by similar method, so we leave it to the readers. □

4. Imaginary extensions with genus one

In this section, we determine all imaginary abelian extensions K of k with $g_K = 1$.

LEMMA 4.1. *Let K be an imaginary extension of k with $g_K = 1$. Then $g_{K^+} = 0$.*

PROOF. Since $g_K \ge g_{K^+}$, $g_{K^+} = 0$ or 1. Assume that $g_{K^+} = 1$. Then from the Riemann-Hurwitz formula for K/K^+, $\deg(\mathcal{D}(K/K^+)) = 0$ and so K/K^+ is unramified. But each infinite primes of K^+ are totally ramified in K. Thus $g_{K^+} = 0$. □

First we consider the case that K/k is a totally imaginary extension, i.e., $K^+ = k$. The degree $[K : k]$ of K/k is a divisor of $q-1$ and so the conductor N of K is a square-free.

THEOREM 4.2. *Let K be a totally imaginary extension of k. Then $g_K = 1$ if and only if K is one of the followings;*

(1) $K = k(\sqrt[3]{-P^2})$ *with* $\deg P = 2,\ q \equiv 1 \pmod 3$,
(2) $K = k(\sqrt[3]{P_1P_2})$ *with* $\deg P_1 = \deg P_2 = 1, q \equiv 1 \pmod 3$,
(3) $K = k(\sqrt{-P_1}\sqrt[4]{-P_2})$ *with* $\deg P_1 = \deg P_2 = 1,\ q \equiv 1 \pmod 4$,
(4) $K = k(\sqrt{-P_1}\sqrt[3]{-P_2})$ *with* $\deg P_1 = \deg P_2 = 1,\ q \equiv 1 \pmod 6$,
(5) $K = k(\sqrt{-P})$ *with* $\deg P = 3,\ q$ *odd*,
(6) $K = k(\sqrt{-P_1P_2})$ *with* $\deg P_1 = 1, \deg P_2 = 2,\ q$ *odd*,
(7) $K = k(\sqrt{-P_1P_2P_3})$ *with* $\deg P_i = 1,\ q \geq 3$ *odd*.

PROOF. Let $N = \prod_{i=1}^{s} P_i$ be the conductor of K. We denote by e_i, g_i and f_i the ramification index, splitting number, and inertia degree of P_i, respectively. Let $\{\mathfrak{P}_{ij} | 1 \leq j \leq g_i\}$ be the set of primes of K lying above P_i. Then $\mathcal{D}(K/k) = \infty^{(n-1)} \times \prod_{i=1}^{s} \prod_{j=1}^{g_i} \mathfrak{P}_{ij}^{(e_i-1)}$. Let $n = [K : k]$. From the Riemann-Hurwitz formula for K/k, we have

$$g_K = 1 \Longleftrightarrow \sum_{i=1}^{s} (1 - \frac{1}{e_i}) d_i = 1 + \frac{1}{n}. \tag{4.1}$$

Since $e_i \geq 2$, we have $1 < 1 + \frac{1}{n} < \sum_{i=1}^{s} d_i \leq 2 + \frac{2}{n} \leq 3$. Note that $\sum_{i=1}^{s} d_i = 3$ if and only if $n = 2$ and it is possible only for odd q. It suffices to consider the following cases;

(i) $s = 1, d_1 = 2 : N = P\,(\deg P = 2)$,
(ii) $s = 2, d_1 = d_2 = 1 : N = P_1P_2\,(\deg P_1 = \deg P_2 = 1, P_1 \neq P_2)$,
(iii) $s = 1, d_1 = 3 : N = P\,(\deg P = 3)$,
(iv) $s = 2, d_1 = 1, d_2 = 2 : N = P_1P_2\,(\deg P_1 = 1, \deg P_2 = 2)$,
(v) $s = 3, d_1 = d_2 = d_3 = 1 : N = P_1P_2P_3$
$(\deg P_i = 1, P_i \neq P_j$ if $i \neq j)(q \geq 3)$.

Case (i) $N = P(\deg P = 2)$: Since K/k is totally ramified, we have $e_1 = n$. From (4.1), we have $n = 3$. Note that q must satisfy $q \equiv 1 \pmod 3$. Since K_P/k is cyclic, we have the unique cubic subfield of K_P over k. From Lemma 2.4, we have $K = k(\sqrt[3]{-P^2})$.

Case (ii) $N = P_1P_2(\deg P_1 = \deg P_2 = 1, P_1 \neq P_2)$: From (4.1), we have

$$1 = \frac{1}{n} + \frac{1}{e_1} + \frac{1}{e_2}.$$

We may assume that $e_1 \leq e_2$. From the fact that e_i divides n, we have $(e_1, e_2, n) = (3,3,3), (2,3,6)$ or $(2,4,4)$. Note that $X_{K_{P_1P_2}} = X_{K_{P_1}} \times X_{K_{P_2}}$ and let χ_i be a generator of $X_{K_{P_i}}$. For $0 \leq a, b \leq q-2$, let $\chi_1^a \chi_2^b \in X_K$. By changing χ_i by χ_i^{-1}, if it is necessary, we may assume that $\chi_1^a \chi_2^b$ is real if and only if $a + b \equiv 0 \pmod{q-1}$. First consider the case $(e_1, e_2, n) = (3,3,3)$. Then we have $q \equiv 1 \pmod 3$ and $a, b \in \{0, (q-1)/3, 2(q-1)/3\}$. Since $n = 3$ and K/k is totally ramified, we have

$$\{(a,b)\} = \{(0,0), ((q-1)/3, (q-1)/3), (2(q-1)/3, 2(q-1)/3)\}$$

and so $K = k(\sqrt[3]{P_1P_2}) \subseteq k(\sqrt[3]{-P_1}, \sqrt[3]{-P_2})$. Similarly, we have $K = k(\sqrt{-P_1}\sqrt[4]{-P_2})$, $q \equiv 1 \pmod 4$ for $(e_1, e_2, n) = (2,4,4)$ and

$$K = k(\sqrt{-P_1}, \sqrt[3]{-P_2}), \quad q \equiv 1 \pmod 6 \text{ for } (e_1, e_2, n) = (2,3,6).$$

Case (iii) $N = P(\deg P = 3)$, q odd : Since $e_i = n = 2$, it suffices to find the (unique) quadratic subfield of K_P for K. From Lemma 2.4, we have $K = k(\sqrt{-P})$.

Case (iv) $N = P_1P_2(\deg P_1 = 1, \deg P_2 = 2)$, q odd : We must find a quadratic subfield K of $K_{P_1P_2}$ with $e_1 = e_2 = 2$. Note that $X_{K_{P_1P_2}} = X_{K_{P_1}} \times X_{K_{P_2}}$. Define $\langle \chi_i \rangle = X_{K_{P_i}}$. For $0 \leq a \leq q-2$ and $0 \leq b \leq q^2 - 2$, let $\chi_1^a \chi_2^b \in X_K$. As Case (ii), we have $a = 0, (q-1)/2$ and $b = 0, (q^2-1)/2$. Since $n = 2$, we have $\{(a,b)\} = \{(0,0), (q-1)/2, (q^2-1)/2)\}$. Since q is odd, $\chi_2^{(q^2-1)/2}$ is real. Thus such K is a required one. Note that $k(\sqrt{-P_1})$ corresponds to $\{1, \chi_1^{(q-1)/2}\}$ and $k(\sqrt{P_2})$ corresponds to $\{1, \chi_2^{(q^2-1)/2}\}$. Thus we have $K = k(\sqrt{-P_1P_2})$.

Case (v) $N = P_1P_2P_3(\deg P_i = 1, P_i \neq P_j \text{ if } i \neq j)$, $q \geq 3$ odd : We must find a quadratic subfield K of K_N with $e_1 = e_2 = e_3 = 2$. Let $X_{K_N} = \langle \chi_1 \rangle \times \langle \chi_2 \rangle \times \langle \chi_3 \rangle$. Since $e_1 = e_2 = e_3 = n = 2$, $X_K = \langle \chi_1^{(q-1)/2} \chi_2^{(q-1)/2} \chi_3^{(q-1)/2} \rangle$. Since $k(\sqrt{-P_i})$ is the subfield of K_{P_i} associated to $\langle \chi_i^{(q-1)/2} \rangle$, we have $K = k(\sqrt{-P_1P_2P_3})$. □

From now on, we assume that K is not totally imaginary, i.e., $K^+ \neq k$. Let $S(K)$ be the set of prime divisors of the conductor of K.

PROPOSITION 4.3. *Let K/k be an imaginary abelian extension with $g_K = 1$. Assume that K is not totally imaginary. Then we have*

$|S(K)| = |S(K^+)|$, *or* $|S(K)| = |S(K^+)| + 1$. *Moreover, if* $|S(K)| = |S(K^+)| + 1$, *then we have*

(i) $[K : K^+] = [K^+ : k] = 2$ *and* $\mathrm{Gal}(K/k) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$,

(ii) $K = F \cdot K^+$, *where* F/k *is totally imaginary abelian extension with* $[F : k] = 2$ *and* $P \in S(K) - S(K^+)$ *is totally ramified in* F/k, $\deg P = 1$, q *is odd.*

When $|S(K)| = |S(K^+)|$, K *and* K^+ *have the same conductor.*

PROOF. Assume that $S(K^+) \subsetneq S(K)$. Choose $P \in S(K) - S(K^+)$. Let $d = \deg P$, $\ell = [K : K^+]$ and $r = [K^+ : k]$. The infinite part of different $\mathcal{D}(K/K^+)$ of K/K^+ is $\prod_{i=1}^{r} \infty_i^{(\ell-1)}$. We write e_1, f_1, g_1 (resp. e_2, f_2, g_2) for the ramification index, inertia degree, splitting number of P in K^+/k (resp. K/K^+). The P-part of $\mathcal{D}(K/K^+)$ is $\prod_{i=1}^{g_1} \prod_{j=1}^{g_2} \mathfrak{P}_{ij}^{(e_2-1)}$. Thus we have

$$\begin{aligned} \deg\left(\mathcal{D}(K/K^+)\right) &\geq \deg\Big(\prod_{i=1}^{r} \infty_i^{(\ell-1)} \times \prod_{i=1}^{g_i} \prod_{j=1}^{g_2} \mathfrak{P}_{ij}^{(e_2-1)}\Big) \\ &= (\ell-1)r + \ell r d(1 - \frac{1}{e_2}) \geq (\ell-1)r + \frac{\ell r d}{2}. \end{aligned}$$

Note that if $\deg(\mathcal{D}(K/K^+)) = (\ell-1)r + \ell r d/2$, then primes lying above P are the only ramified finite primes between K/K^+ and $e_2 = 2$. By the Riemann-Hurwitz formula for K/K^+, we have

$$\begin{aligned} 0 &= -2\ell + \deg(\mathcal{D}(K/K^+)) \\ &\geq -2\ell + (\ell-1)r + \frac{\ell r d}{2} \geq -2\ell + (\ell-1)r + \ell. \end{aligned}$$

Thus $r \leq \frac{\ell}{\ell-1} = 1 + \frac{1}{\ell-1} \leq 2$, so $r = 2, \ell = 2$ and $d = 1$. If another prime is contained in $S(K) - S(K^+)$, $\deg(\mathcal{D}(K/K^+))$ must strictly larger than $(\ell-1)r + \ell r d/2$, which is a contradiction. Therefore we have shown that if $S(K) \neq S(K^+)$, then $S(K) = S(K^+) \cup \{P\}$ with $\deg P = 1$ and $[K : K^+] = [K^+ : k] = 2$. Thus $[K : k] = 4$ and $\mathrm{Gal}(K/k) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/4\mathbb{Z}$. We claim that $\mathrm{Gal}(K/k) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If $\mathrm{Gal}(K/k) \cong \mathbb{Z}/4\mathbb{Z}$, then K^+ is the unique nontrivial subfield of K. Let $Q \in S(K^+)$. Then $e(Q, K^+/k) = 2$ and $e(Q, K/k) = 2$ or 4. Since $e(Q, K/K^+) = 1$, we have $e(Q, K/k) = 2$. Let K_0 be the inertia field of Q in K. Then $[K : K_0] = e(Q, K/k) = 2$ and so $K_0 = K^+$. But Q is totally ramified in K/K_0 but unramified in K/K^+, which is a contradiction. This proves the claim. Note that $e(\infty, K/k) = e(\infty, K/K^+) = 2$. Let F/k be a quadratic subfield of K with $F \neq K^+$. Clearly, F/k is totally imaginary quadratic extension. For $P \in S(K) - S(K^+)$, since $e(P, K/k) = 2$ and

$e(P, K^+/k) = 1$, we have $e(P, F/k) = 2$, i.e., P is totally ramified in F/k.

Now suppose that $|S(K)| = |S(K^+)|$. Let $N = \prod_{i=1}^{s} P_i^{m_i}$ and $N^+ = \prod_{i=1}^{s} P_i^{m_i'}$ be the conductors of K and K^+, respectively. Then we have

$$[K_N : K_{N^+}] = \frac{\prod_{i=1}^{s} \Phi(P_i^{m_i})}{\prod_{i=1}^{s} \Phi(P_i^{m_i'})} = \prod_{i=1}^{s} q^{(m_i - m_i')d_i},$$

where $d_i = \deg P_i$. Thus $[K_N : K_{N^+}]$ is a q-power and so $[KK_{N^+} : K_{N^+}] = [K : K \cap K_{N^+}]$ is also a q-power. But $[K : K \cap K_{N^+}]$ is a divisor of $q - 1$ because $[K : K \cap K_{N^+}]$ divides $[K : K^+]$. Therefore $[K : K \cap K_{N^+}] = 1$, i.e., $K \subseteq K_{N^+}$. It shows that $N = N^+$, which completes the proof. □

First we consider the case that $|S(K)| = |S(K^+)|$.

THEOREM 4.4. *Let K/k be an imaginary abelian extension such that $K^+ \neq k$ and $|S(K)| = |S(K^+)|$. Then $g_K = 1$ if and only if K is one of the followings;*

(1) $K = k(\sqrt[4]{P})$ *with* $\deg P = 2$, $q \equiv 1 \pmod 4$,
(2) $K = k(\sqrt[3]{-P_1}, \sqrt[3]{-P_2})$ *with* $\deg P_i = 1$, $q \equiv 1 \pmod 3$,
(3) $K = k(\sqrt{-P_1}, \sqrt[4]{P_1 P_2^3})$ *with* $\deg P_i = 1$, $q \equiv 1 \pmod 4$,
(4) $K = k(\sqrt[3]{-P_1}\sqrt[6]{-P_2})$ *with* $\deg P_i = 1$, $q \equiv 1 \pmod 6$,
(5) $K = k(\sqrt{-P_1}, \sqrt[4]{-P_2})$ *with* $\deg P_i = 1$, $q \equiv 1 \pmod 4$,
(6) $K = k(\sqrt{-P_1}\sqrt[6]{-P_2})$ *with* $\deg P_i = 1$, $q \equiv 1 \pmod 6$,
(7) $K = k(\sqrt[3]{-P}, \alpha)$ *with* $\deg P = 1$, *where q is 4-power and α is an element of $K_{P^2}^+$ such that $k(\alpha)$ is any quadratic subfield of $K_{P^2}^+$,*
(8) $K = k(\sqrt{-P}, \beta)$ *with* $\deg P = 1$, *where q is 3-power and β is an element of $K_{P^2}^+$ such that $k(\beta)$ is any cubic subfield of $K_{P^2}^+$,*
(9) $K = k(\sqrt{-P_1}, \sqrt{-P_2}, \sqrt{-P_3})$ *with* $\deg P_i = 1$, $q \geq 3$ *odd.*

PROOF. By Lemma 4.1, we have $g_{K^+} = 0$. Thus K^+ is one of the followings ([5]);

(i) K^+ is a subfield of $K_P^+, \deg P = 2$,
(ii) K^+ is a subfield of $K_{P_1P_2}^+, \deg P_i = 1$,
(iii) K^+ is a subfield of $K_{P^2}^+, \deg P = 1$.
(iv) $K^+ = k(\sqrt{P_1P_2}, \sqrt{P_1P_3})$, odd q, $\deg P_i = 1$.

We write $\ell = [K : K^+]$ and $r = [K^+ : k]$.

Case (i) K^+ is a subfield of $K_P^+, \deg P = 2$: In this case K is a subfield of K_P. From the Riemann-Hurwitz formula for K/K^+, we have

$g_K = 1$ if and only if $0 = -2\ell + (\ell - 1)r + (\ell - 1)2$. Since $r \geq 2$, we have $r = \ell = 2$. Since ℓ is a divisor of $q - 1$, it is possible only for odd q. Since K_P is cyclic, K is the unique quartic subfield of K_P. Let $\mathrm{Gal}(K_P/k) = \langle\sigma\rangle$. Then $\mathrm{Gal}(K_P/K_P^+) = \langle\sigma^{q+1}\rangle$. We have $X_{K_P} = \langle\chi\rangle$, where χ is the character associated to σ. Then $X_K = \langle\chi^{(q^2-1)/4}\rangle$. If $4|(q+1) = [K_P^+ : k]$, K is real, which is a contradiction. Suppose $q \equiv 1 \pmod 4$. Then K is imaginary and K^+ is quadratic subfield of K_P^+. Therefore the (unique) quartic subfield of K_P with $\deg P = 2$, $q \equiv 1 \pmod 4$ is the required one. By Lemma 2.4, we have $K = k(\sqrt[4]{P})$.

Case (ii) K^+ is a subfield of $K_{P_1P_2}^+, \deg P_i = 1$: From the Riemann-Hurwitz formula for K/k, we have $g_K = 1$ if and only if $1 = \frac{1}{\ell} + \frac{1}{e_1} + \frac{1}{e_2}$. Thus $g_K = 1$ if and only if $(\ell, e_1, e_2) = (3,3,3), (2,4,4), (2,3,6), (4,2,4)$, $(3,2,6)$, or $(6,2,3)$. Note that $e(P_i, K_{P_1P_2}/k) = e(P_i, K_{P_i}/k) = q - 1$. Since $e(P_i, K_{P_1P_2}/K_{P_1P_2}^+) = 1$, as the number field case (for example, [9, Proposition 2.15]), we have $e(P_i, K_{P_1P_2}^+/k) = q - 1$, i.e., P_i is totally ramified in $K_{P_1P_2}^+/k$. Thus we have $r|e_i$ for $i = 1, 2$. Write $\mathrm{Gal}(K_{P_1P_2}/k) \cong \langle\sigma_1\rangle \times \langle\sigma_2\rangle$ and let χ_i be the character associated to σ_i. For $0 \leq a, b \leq q - 2$, consider $\chi_1^a\chi_2^b \in X_{K_{P_1P_2}}$. Note that $\chi_1^a\chi_2^b \in X_{K_{P_1P_2}}$ is real if and only if $a + b \equiv 0 \pmod{q-1}$. Here we assume that the generator of the sign group is mapped to (σ_1, σ_2). Assume that $(\ell, e_1, e_2) = (3,3,3)$. In this case, q must satisfy $q \equiv 1 \pmod 3$. Since $r|3$, we have $r = 3$. If $\chi_1^a\chi_2^b \in X_{K_{P_1P_2}} \in X_K$, we have $a, b \in \{0, (q-1)/3, 2(q-1)/3\}$. Since $[K : k] = \ell r = 9$, we have $X_K = \{\chi_1^a\chi_2^b | a, b = 0, (q-1)/3, 2(q-1)/3\}$. It is easy to check that this case satisfies $\ell = r = 3$ and by Lemma 2.4, we have $K = k(\sqrt[3]{-P_1}, \sqrt[3]{-P_2})$. Similarly, we have $K = k(\sqrt{-P_1}, \sqrt[4]{P_1P_2^3})$ with $q \equiv 1 \pmod 4$ (resp. $k(\sqrt[6]{-P_1^2P_2})$ with $q \equiv 1 \pmod 6$, $k(\sqrt{-P_1}, \sqrt[4]{-P_2})$ with $q \equiv 1 \pmod 4$, $k(\sqrt[6]{P_1^3P_2})$ with $q \equiv 1 \pmod 6$) for $(\ell, e_1, e_2) = (2,4,4)$ (resp. $(2, 3, 6)$, $(4, 2, 4)$, $(3, 2, 6)$). Assume $(\ell, e_1, e_2) = (6,2,3)$. In this case $r|2$ and $r|3$, that is, $r = 1$, which contradicts the fact that $r \geq 2$.

Case (iii) K^+ is a subfield of $K_{P^2}^+, \deg P = 1$: Note that $[K_{P^2} : k] = q(q-1), [K_{P^2}^+ : k] = q$. By the Riemann-Hurwitz formula for K/K^+, we have $g_K = 1$ if and only if $0 = -2\ell + (\ell - 1)r + (\ell - 1)$ if and only if $(r, \ell) = (2,3)$ or $(3,2)$.

Assume $(r, \ell) = (2,3)$. Since $r = 2$, q is 2-power. Since $l = 3$, $q \equiv 1 \pmod 3$. Thus q is 4-power. By Lemma 2.3, $\mathrm{Gal}(K_{P^2}/k) \cong$

$\mathrm{Gal}(K_P/k) \times \mathrm{Gal}(K_{P^2}^+/k) \cong A \times B$, where A is the cyclic group of order $q-1$ and B is an elementary abelian 2-group of order q. Thus a cubic subfield of K_{P^2}/k corresponds to a subgroup C of $A \times B$ with group index $[A \times B : C] = 3$. Since $(q, q-1) = 1$, it is easily checked that $B \subset C$. Thus a cubic subfield of K_{P^2} is in fact a subfield of K_P and by Lemma 2.4, it becomes $k(\sqrt[3]{-P})$. Let F be the unique cubic subfield of K/k. Then $F = k(\sqrt[3]{-P})$. Therefore K is the compositum of $k(\sqrt[3]{-P})$ and any quadratic subfield of $K_{P^2}^+$. Thus $K = k(\sqrt[3]{-P}, \alpha)$, where α is an element of $K_{P^2}^+$ such that $k(\alpha)$ is any quadratic subfield of $K_{P^2}^+$.

Assume $(r, \ell) = (3, 2)$. Then q is a 3-power. As above, we conclude that the quadratic subfield of K is $k(\sqrt{-P})$ and K is the compositum of $k(\sqrt{-P})$ and any cubic subfield of $K_{P^2}^+$. Therefore $K = k(\sqrt{-P}, \beta)$, where β is an element of $K_{P^2}^+$ such that $k(\beta)$ is a cubic subfield of $K_{P^2}^+$.

Case (iv) $K^+ = k(\sqrt{P_1P_2}, \sqrt{P_1P_3})$, odd q, $\deg P_i = 1$: In this case we have $r = 4$. From the Riemann-Hurwitz formula for K/k, we have $g_K = 1$ if and only if

$$2 = \frac{1}{\ell} + \frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3}.$$

Since $\ell, e_1, e_2, e_3 \geq 2$, we have $l = e_1 = e_2 = e_3 = 2$ and so $[K : k] = 8$. Let $X_K = \langle \chi_1 \rangle \times \langle \chi_2 \rangle \times \langle \chi_3 \rangle$. For $\chi_1^a \chi_2^b \chi_3^c \in X_K$, we have $a, b, c \in \{0, (q-1)/2\}$. Since $[K : k] = 8$, we have $\{(a, b, c)\} = \{(a, b, c) | a, b, c = 0, (q-1)/2\}$. Therefore K is the compositum of quadratic subfield of K_{P_i} for $i = 1, 2, 3$, that is, $K = k(\sqrt{-P_1}, \sqrt{-P_2}, \sqrt{-P_3})$. □

Next we consider the case $|S(K)| = |S(K^+)|+1$. Let K/k be an imaginary abelian extension with $K^+ \neq k$, $g_K = 1$ and $|S(K)| = |S(K^+)|+1$, say $S(K) = S(K^+) \cup \{P\}$. Let F be a subfield of K, as in Proposition 4.3. Then F is totally imaginary quadratic subfield and $\deg P = 1$, $P \in S(F)$. By Proposition 4.3, we see that q is odd.

LEMMA 4.5. *If $g_F = 0$, then $S(F) = \{P\}$. If $g_F = 1$, then $S(F) = \{P, Q\}$ with $\deg Q = 2$ or $S(F) = \{P, Q_1, Q_2\}$ with $\deg Q_i = 1$.*

PROOF. By the Riemann-Hurwitz formula for F/k, we have $g_F = 0 \Leftrightarrow \deg(\mathcal{D}(F/k)) = 2$ and $g_F = 1 \Leftrightarrow \deg(\mathcal{D}(F/k)) = 4$. But $\deg(\mathcal{D}(F/k)) \geq \deg(\infty\mathfrak{P}) = 2$. Here $\mathfrak{P}$ is the prime above P. Thus $g_F = 0 \Leftrightarrow \mathcal{D}(F/k) = \infty \cdot P \Leftrightarrow S(F) = \{P\}$. Suppose $g_F = 1$. We must have $|S(F)| \leq 3$. If $S(F) = \{P, Q\}$, $\deg(\mathcal{D}(F/k)) = \deg(\infty\mathfrak{P}\mathfrak{Q}) = 4$. Here $\mathfrak{Q}$ is the prime above Q. Thus $\deg Q = 2$. If $S(F) = \{P, Q_1, Q_2\}$, $\deg(\mathcal{D}(F/k)) = 2+\deg Q_1+\deg Q_2 = 4$ and so $\deg Q_1 = \deg Q_2 = 1$. □

THEOREM 4.6. *Let K/k be an imaginary abelian extension such that $K^+ \neq k$ and $|S(K)| = |S(K^+)| + 1$. Then $g_K = 1$ if and only if $K = k(\sqrt{-P}, \sqrt{Q})$, $\deg P = 1, \deg Q = 2$ or $K = k(\sqrt{-P}, \sqrt{P_1P_2})$, $\deg P = \deg P_1 = \deg P_2 = 1, (P \neq P_i)$.*

PROOF. Since $g_{K^+} = 0$ and $[K^+ : k] = 2$, from [5, Section 4] and Lemma 2.4, K^+ is one of the followings;

(i) $K^+ = k(\sqrt{Q})$ with $S(K^+) = \{Q\}$ and $\deg Q = 2$,
(ii) $K^+ = k(\sqrt{P_1P_2})$ with $S(K^+) = \{P_1, P_2\}$ and $\deg P_i = 1$,
(iii) $K^+ = k(\sqrt{Q})$ with $S(K^+) = \{Q\}$ and $\deg Q = 2$ or $K^+ = k(\sqrt{P_1P_2})$ with $S(K^+) = \{P_1, P_2\}$ and $\deg P_i = 1$.

Now consider F/k. F is totally imaginary quadratic extension of k. If $g_F = 0$, then $S(F) = \{P\}, \deg P = 1$ and so by [5, Theorem 3.6], $F = k(\sqrt{-P})$. If $g_F = 1$, then $S(F) = \{P, Q\}$ with $\deg Q = 2$ or $S(F) = \{P, Q_1, Q_2\}$ with $\deg Q_i = 1$. By Theorem 4.2, $F = k(\sqrt{-P})$ with $\deg P = 3$, $F = k(\sqrt{-P_1P_2})$ with $\deg P_1 = 1, \deg P_2 = 2$, or $F = k(\sqrt{-P_1P_2P_3})$ with $\deg P_i = 1$. Since $|S(F)| = 2$ or 3, the first case is impossible. Thus F is one of the followings;

(a) $F = k(\sqrt{-P}), \deg P = 1$,
(b) $F = k(\sqrt{-P_1P_2}), \deg P_1 = 1, \deg P_2 = 2$,
(c) $F = k(\sqrt{-P_1P_2P_3}), \deg P_i = 1$.

For each cases of K^+ and F, we check whether K satisfies $g_K = 1$.

Case (i)–(a) : $F = k(\sqrt{-P})$ with $\deg P = 1$ and $K^+ = k(\sqrt{Q})$ with $\deg Q = 2$. Let $L = k(\sqrt{-PQ})$. Then P and Q ramify in L. Thus K/L is an unramified extension. By the Riemann-Hurwitz formula for K/L, we have $g_K = 2g_L - 1$. By the Riemann-Hurwitz formula for L/k, $g_L = 1$ and so $g_K = 1$.

Case (i)–(b) : $F = k(\sqrt{-PQ})$ and $K^+ = k(\sqrt{Q})$ with $\deg P = 1$ and $\deg Q = 2$. Since $K = k(\sqrt{-PQ}, \sqrt{Q}) = k(\sqrt{-P}, \sqrt{Q})$, this case equals to the Case (i)–(a).

Case (i)–(c) : Since $|S(K)| \geq |S(F)| = 3$ and $|S(K^+)| = 1$, it is impossible.

Case (ii)–(a) : $F = k(\sqrt{-P})$ and $K^+ = k(\sqrt{P_1P_2})$ with $\deg P = \deg P_1 = \deg P_2 = 1$ and $P \neq P_1, P_2$. Let $L = k(\sqrt{-PP_1P_2})$. Note that we have the ramification indices $e(P, K/k) = e(P, L/k) = 2$ and $e(P_i, K/k) = e(P_i, L/k) = 2$. Thus K/L is an unramified extension, and so $\deg \mathcal{D}(K/L) = 0$. By the Riemann-Hurwitz formula for L/k, we have $g_L = 1$. By the Riemann-Hurwitz formula for K/L, we have $g_K = 1$ because $\deg \mathcal{D}(K/L) = 0$.

Case (ii) (b) : $F = k(\sqrt{-PP_1})$ and $K^+ = k(\sqrt{P_1P_2})$ with $\deg P = 2$ and $\deg P_i = 1$. Since $g_F = 1$, we have that $g_K = 1$ if and only if K/F is unramified. But P_2 is ramified in K/F because we have the ramification indices $e(P_2, K/k) = 2$ and $e(P_2, L/k) = 1$. Thus $g_K \neq 1$.

Case (ii) (c) : $F = k(\sqrt{-P_1P_2P_3})$ and $K^+ = k(\sqrt{P_1P_2})$ with $\deg P_i = 1$. Since $K = k(\sqrt{-P_1P_2P_3}, \sqrt{P_1P_2}) = k(\sqrt{-P_3}, \sqrt{P_1P_2})$, it returns to the Case (ii) (a). □

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, 1999.

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

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

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

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

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

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

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

Hwanyup Jung
Department of Mathematics Education
Chungbuk National University
Cheongju 361-763, Korea
E-mail: hyjung@chungbuk.ac.kr

Jachyun Ahn
Department of Mathematics
Chungnam National University
Daejon 305-764, Korea
E-mail: jhahn@cnu.ac.kr