GENUS FIELD OF REAL BIQUADRATIC FIELDS II

SUNGHAN BAE AND QIN YUE

Abstract. Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ be a real biquadratic field with $p \equiv 1 \mod 4$ or $p = 2$ and d a squarefree positive integer. The Hilbert genus field is described explicitly by Yue ([15]) in the case that $p \equiv 1 \mod 4$ and $d \equiv 3 \mod 4$. In this article we give the Hilbert genus field of K explicitly for the remaining cases. We also consider the function field analogue of this problem.

1. Introduction

Let K be a number field and let H be the Hilbert class class field of K, i.e. the maximal abelian unramified extension of K. Let $G = Gal(H/K)$ be the Galois group of H/K and let $C(K)$ be the class group of K, then there is a canonical isomorphism:

$$\phi_{H/K} : C(K) \to Gal(H/K),$$

where $\phi_{H/K}$ is the map induced by the Artin map (see [8]). Let E be the fixed field of G^2. Then

$$C(K)/C(K)^2 \cong G/G^2 \cong \mathrm{Gal}(E/K).$$

Hence

$$E = K(\sqrt{\Delta}), \quad K^{*2} \subset \Delta \subset K^*. \tag{1.1}$$

If K is the real biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{d})$ with $p \equiv 1 \mod 4$ a prime and d a squarefree positive integer prime to p, then E is the relative genus field of the extension K/K_0, where $K_0 = \mathbb{Q}(\sqrt{p})$.

In this paper, we will find a set of representatives of the set Δ/K^{*2}, when K is a real biquadratic field

Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field, then by [6] or [4] we know the genus field E of K explicitly. In fact, let $d = q_1 \cdots q_n$, where $q_1, \cdots, q_n$ are distinct primes,

---

1991 *Mathematics Subject Classification.* 11R58.

1st author is supported by Basic Science Research Program through NRF of Korea funded by Ministry of Education, Science and Technology (ASARC 2009-0063182).

2nd author is supported by NNSF of China (No. 10771100).

1) If $q_j \equiv 1 \mod 4$ for all $1 \leq j \leq n-1$, then

$$E = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, \cdots, \sqrt{q_n});$$

2) If $q_1 \equiv 3 \mod 4$, then

$$E = \mathbb{Q}(\sqrt{d}, \sqrt{q_2^*}, \cdots, \sqrt{q_n^*}),$$

where

$$q_j^* = \begin{cases} q_j & \text{if } q_j \equiv 1 \mod 4 \\ q_j q_1 & \text{if } q_j \equiv 3 \mod 4 \\ q_j q_1 & \text{if } q_j = 2 \text{ and } d/2 \equiv 3 \mod 4 \\ q_j & \text{if } q_j = 2 \text{ and } d/2 \equiv 1 \mod 4 \end{cases}, j = 2, \cdots, n.$$

Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ be a real biquadratic field, where p is a prime number and d is a squarefree positive integer prime to p. When $p \equiv 1 \mod 8$ and $d \equiv 3 \mod 4$, P. Sime ([10]) used Herglotz's results ([5]) to give the Hilber genus field of K, under the condition that 2-Sylow subgroups of the class groups of $K_0 = \mathbb{Q}(\sqrt{p})$, $K_1 = \mathbb{Q}(\sqrt{d})$, $K_2 = \mathbb{Q}(\sqrt{pd})$ are elementary. Later Q. Yue ([15]) improved Sime's result to $p \equiv 1 \mod 4$, $d \equiv 3 \mod 4$ and without the condition on the class groups. Recently Fouvry and Klüners [3] touched upon the genus field of K and gave strong evidence in the direction of a Stevenhagen's conjecture ([11]).

In this paper, we extend Yue's result to all real biquadratic number fields $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ with $p \equiv 1 \mod 4$ or $p = 2$, and a positive squarefree integer d prime to p. The assumption on p is to assure the existence of a fundamental unit $\epsilon \in K_0$ whose norm is -1.

In the final section we consider the analogous problem in the function field case, that is, we find the genus field of $k(\sqrt{P}, \sqrt{D})$, where $k = \mathbb{F}_q(T)$, P a monic irreducible polynomial of even degree and D a monic squarefree polynomial in $\mathbb{F}_q[T]$.

Notations:

$O_L :=$ the ring of integers of a number field L

$U_L :=$ the unit group of O_L

$C(L) :=$ the class group of L

$h(L) :=$ the class number of L

$v_{\mathfrak{p}}(x) :=$ the normalized valuation at a prime $\mathfrak{p}$ of L

$A_2 :=$ 2-Sylow subgroup of an abelian group A

${}_2A :=$ the subgroup of elements of order ≤ 2 of A

$r_2(A) :=$ 2-rank of an abelian group A

2. **Basic Facts**

In this section we recall some facts from [15] which will be used later. Let $K_0 = \mathbb{Q}(\sqrt{p})$, $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$, $K_1 = \mathbb{Q}(\sqrt{d})$ and $K_2 = \mathbb{Q}(\sqrt{pd})$. Let E be the Hilbert genus field of K. Then E can be expressed as

$$E = K(\sqrt{\Delta}), \quad K^{*2} \subset \Delta \subset K^{*}.$$

Define

$$D_K := \{x \in K^{*} | v_{\mathfrak{p}}(x) \equiv 0 \mod 2 \text{ for all finite primes } \mathfrak{p} \text{ of } K\},$$
$$D_K^{+} := \{x \in D_K | x \text{ totally positive}\}.$$

Lemma 2.1. ([15, Lemma 2.1]) *If $x \in D_K^{+}$, then all non-dyadic primes of K are unramified in $K(\sqrt{x})$. Moreover, $\Delta \subset D_K^{+}$.*

Let S be a finite set consisting of all infinite primes and the finite primes of K_0, which are ramified in K. Let $U_{K_0}^{S}$ be the group of S-units of K_0 and let $U_{K_0}^{S+}$ be the subgroup of all S-units that are positive at all real infinite primes of K_0.

Lemma 2.2. ([15, Lemma 2.2], or [13]) *There is an exact sequence*

$$0 \to \mathbb{Z}/2 \to U_{K_0}^{S+}/(U_{K_0}^{S})^2 \to D_K^{+}/K^{*2} \to 1.$$

Moreover,

$$r_2(D_K^{+}/K^{*2}) = s - 1,$$

where s is the cardinality of all finite primes in S.

Let U_{K_0} be the group of units in K_0 and NK the image of K under the norm map N_{K/K_0}.

Lemma 2.3. ([15, Lemma 2.3], or [7]) *Let $Am(K/K_0)$ be the subgroup of $C(K)$ consisting of all ambiguous ideal classes. Then*

$$r_2(C(K)) = r_2(Am(K/K_0)) = s - 1 - r_2(U_{K_0}/U_{K_0} \cap NK).$$

Proposition 2.1. ([15, Proposition 2.1]) *There is a decomposition of the multiplicative group*

$$D_K^{+}/K^{*2} = \Delta/K^{*2} \times A,$$

where $r_2(A) = r_2(U_{K_0}/U_{K_0} \cap NK)$.

In the following, we give some results of 2-adic local fields.

Lemma 2.4. *let $F = \mathbb{Q}_2(\sqrt{-3})$ be an extension over the local field $\mathbb{Q}_2$ and U the unit group of F. Then*
i) $U/U^2 = (3) \times (1 + 2w) \times (1 + 4w)$, where $w = \frac{-1+\sqrt{-3}}{2}$ is the third primitive unit root.

ii) $F(\sqrt{3}, \sqrt{1+2w})/F$ is a totally ramified extension, $F(\sqrt{1+4w})/F$ is an unramified extension.

Note: $3 \cdot (1+2w) \equiv 1+2w^2 \bmod 4$ and $F(\sqrt{1+2w^2})/F$ is ramified. Moreover, if $a \in U$ and $a \equiv w \cdot x$ or $a \equiv w^2 \cdot x \bmod 4$, $x \equiv 1 \bmod 2$, then $F(\sqrt{a})/F$ is unramified extension if and only if $x \equiv 1 \bmod 4$.

Lemma 2.5. *In the local field $\mathbb{Q}_2(\sqrt{-3})$,*
i) If a prime $p \equiv 13 \bmod 16$, then $\sqrt{p} \equiv \sqrt{-3} \bmod 8$.
ii) If a prime $p \equiv 5 \bmod 16$, then $\sqrt{p} \equiv \sqrt{-3}+4 \bmod 8$.

Proof. Since $p \equiv 5 \bmod 8$, $\sqrt{p} \in \mathbb{Q}_2(\sqrt{-3})$. In the local field $\mathbb{Q}_2(\sqrt{-3})$, we consider the root of polynomial $f(x) = x^2 - p$. By Newton's method (see [12, P. 76]), $a_0 = \sqrt{-3}$ satisfies the relation

$$v_2(\frac{f(a_0)}{f'(a_0)^2}) = v_2(\frac{-3-p}{4}) = r > 0,$$

Then we can construct the sequence

$$a_{i+1} = a_i - \frac{f(a_i)}{f'(a_i)}, a_0 = \sqrt{-3}, i = 0, 1, 2, \cdots,$$

which converges to a root $\sqrt{p}$ of $f(x)$, i.e. $\lim_{x\to\infty} a_i = \sqrt{p}$. Moreover $v_2(a_{i+1} - a_i) \geq 2^i r$.

If $p \equiv 13 \bmod 16$, then $r \geq 2$ and

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = \sqrt{-3} - \frac{-3-p}{2\sqrt{-3}} \equiv \sqrt{-3} \bmod 8,$$

Hence $v_2(\sqrt{p} - a_1) \geq 2^1 \cdot 2 = 4$ and $\sqrt{p} \equiv a_1 \equiv \sqrt{-3} \bmod 8$.

If $p \equiv 5 \bmod 16$, then $r = 1$ and $v_2(a_3 - a_2) \geq 2^2 \cdot 1 = 4$,

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_o)} = \sqrt{-3} - \frac{-3-p}{2\sqrt{-3}} = \sqrt{-3} + \frac{3+p}{2\sqrt{-3}} = \frac{p-3}{2\sqrt{-3}},$$

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = \frac{p-3}{2\sqrt{-3}} + \frac{(p+3)^2\sqrt{-3}}{12(p-3)} \equiv \frac{p-3}{2\sqrt{-3}} \bmod 8,$$

Hence, $v_2(\sqrt{p} - a_2) \geq 4$ and by $\sqrt{-3} = 1 + w \cdot 2$,

$$\sqrt{p} \equiv a_2 \equiv \sqrt{-3} + \frac{p+3}{2\sqrt{-3}} \equiv \sqrt{-3} + 4 \bmod 8. \blacksquare$$

Lemma 2.6. *Let p be a prime and q a positive integer prime to p with $p \equiv q \equiv 1 \bmod 4$. Suppose that the Diophantine equation $qz^2 = x^2 - py^2$ has a relatively prime and positive integral solution (x_0, y_0, z_0). Take $\alpha = x_0 + \sqrt{p}y_0$ if $2 \not| z_0$ and $\alpha = \frac{x_0+\sqrt{p}y_0}{2}$ if $2|z_0$.*
i) If $2 \not| z_0$, then $\alpha \equiv x_0 + y_0 \bmod 4$.
ii) If $p \equiv 5 \bmod 8$ and $2|z_0$, then in the local field $\mathbb{Q}_2(\sqrt{p})$, $\alpha \equiv w(-x_0)$ or $w^2(-x_0) \bmod 4$, where $w = \frac{-1+\sqrt{-3}}{2}$.

iii) If $p \equiv 1 \mod 8$ and $2|z_0$, then $\alpha \equiv x_0 \mod {D'}^2$ and $\alpha \equiv 2^e \cdot x_0 \mod D^2$, where D and D' are dyadic primes of $K_0 = \mathbb{Q}(\sqrt{p})$ and e is an even integer.

Proof. i) If $2 \nmid z_0$, then $2 \nmid x_0$ and $2|y_0$. Hence

$$\alpha = x_0 + y_0 + \frac{-1+\sqrt{p}}{2} \cdot 2y_0 \equiv x_0 + y_0 \mod 4.$$

ii) If $p \equiv 5 \mod 8$ and $2|z_0$, then $2||z_0$. Suppose first that $p \equiv 13 \mod 16$, then $\sqrt{p} - \sqrt{-3} \equiv 0 \mod 8$. Hence

$$\alpha - wy_0 = \frac{x_0 + \sqrt{p}y_0}{2} - \frac{-1+\sqrt{-3}}{2} \cdot y_0 = \frac{x_0+y_0}{2} + \frac{\sqrt{p}-\sqrt{-3}}{2} y_0 \equiv \frac{x_0+y_0}{2} \mod 4.$$

Since $x_0^2 - py_0^2 = qz_0^2 \equiv 4 \mod 16$ and $p \equiv 13 \mod 16$, $x_0^2 \equiv y_0^2 \mod 16$. If $x_0 \equiv -y_0 \mod 8$, then $\frac{x_0+y_0}{2} \equiv 0 \mod 4$ and $\alpha \equiv wy_0 \equiv w(-x_0) \mod 4$; if $x_0 \equiv y_0 \mod 8$, then $\frac{x_0+y_0}{2} \equiv y_0 \mod 4$ and $\alpha \equiv (1+w)y_0 = w^2(-y_0) \equiv w^2(-x_0) \mod 4$.

Suppose that $p \equiv 5 \mod 16$. Then $\sqrt{p} - \sqrt{-3} \equiv 4 \mod 8$. Hence

$$\alpha - wy_0 = \frac{x_0+y_0}{2} + \frac{\sqrt{p}-\sqrt{-3}}{2} \cdot y_0 \equiv \frac{x_0+y_0}{2} + 2y_0 \equiv \frac{x_0+y_0}{2} + 2 \mod 4,$$

since y_0 is odd. Since $x_0^2 - py_0^2 = qz_0^2 \equiv 4 \mod 16$ and $p \equiv 5 \mod 16$, $x_0^2 \equiv y_0^2 + 8 \mod 16$. If $x_0 \equiv -y_0 + 4 \mod 8$, then $\frac{x_0+y_0}{2} \equiv \frac{4}{2} \equiv 2 \mod 4$ and $\alpha \equiv wy_0 \equiv w(-x_0) \mod 4$; if $x_0 \equiv y_0 + 4 \mod 8$, then $\frac{x_0+y_0}{2} \equiv y_0 + 2 \mod 4$ and $\alpha \equiv (1+w)y_0 = w^2(-y_0) \equiv w^2(-x_0) \mod 4$.

iii) If $p \equiv 1 \mod 8$ and $2|z_0$, then $4|z_0$ and

$$\frac{x_0 + y_0\sqrt{p}}{2} \cdot \frac{x_0 - y_0\sqrt{p}}{2} = \frac{z_0^2}{4} \equiv 0 \mod 4.$$

Let $D = (2, \frac{x_0+\sqrt{p}y_0}{2})$ and $D' = (2, \frac{x_0-\sqrt{p}y_0}{2})$ be two dyadic primes of $K_0 = \mathbb{Q}(\sqrt{p})$, then $\alpha = \frac{x_0+y_0\sqrt{p}}{2} \in D^2$, $\alpha' = \frac{x_0-y_0\sqrt{p}}{2} \in {D'}^2$, and

$$\alpha = \frac{x_0 + y_0\sqrt{p}}{2} = x_0 - \frac{x_0 - y_0\sqrt{p}}{2} \equiv x_0 \mod {D'}^2,$$

also $\alpha' \equiv x_0 \mod D^2$. Let $2^e||z_0$, $e \geq 2$, then by $\alpha \cdot \alpha' \cdot 2^{-2(e-1)} = \frac{z_0^2}{2^{2e}} \equiv 1 \mod D^2$,

$$\alpha \cdot 2^{-2(e-1)} \equiv (\alpha')^{-1} \equiv x_0 \mod D^2. \blacksquare$$

An element α of O_{K_0} is called *primary* if $X^2 \equiv \alpha \mod D^2$ is solvable for any dyadic prime D of K_0. By Lemma 2.6, we get the following result.

Corollary 2.1. *The assumptions are as in Lemma 2.6.*
i) Suppose that $\alpha = x_0 + \sqrt{p}y_0$ with $2 \nmid z_0$, then α is primary if and only if $x_0 + y_0 \equiv 1 \mod 4$.
ii) Suppose that $\alpha = \frac{x_0+\sqrt{p}y_0}{2}$ with $2|z_0$, then α is primary if and only if $x_0 + z_0 \equiv 1 \mod 4$.
Moreover, we have that α is not primary if and only if $\alpha \cdot 3$ is primary. $\blacksquare$

Proposition 2.2. *Let p, q be distinct primes with $p \equiv q \equiv 1$ mod 4 and $(\frac{p}{q}) = 1$ and let ϵ be a fundamental unit of $K_0 = \mathbb{Q}(\sqrt{p})$. If (x_0, y_0, z_0) is a relatively prime and positive integral solution of the Diophantine equation $qz^2 = x^2 - py^2$, set $\alpha = x_0 + \sqrt{p}y_0$ if $2 \not| z_0$ or $\alpha = \frac{x_0+\sqrt{p}y_0}{2}$ if $2|z_0$. Then $2|h(\mathbb{Q}(\sqrt{p}, \sqrt{q}))$ if and only if $q \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ if and only if the local Hilbert symbol $(\epsilon, q)_Q = 1$, where $QQ' = qO_{K_0}$, if and only if α is primary.*

Proof. Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and $K_0 = \mathbb{Q}(\sqrt{p})$, then by Lemma 2.3 $r_2(C(K)) = 2 - 1 - r_2(U_{K_0}/(U_{K_0} \cap NK))$. It is clear that $-1 \in NK$. Hence we conclude that $2|h(K)$ if and only if $\epsilon \in NK$ if and only if $q \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ if and only if the local Hilbert symbol $(\epsilon, q)_Q = 1$, where $QQ' = qO_{K_0}$ (see [2, Lemma 21.8]).

Let $\alpha = x_0 + \sqrt{p}y_0$ if $2 \not| z_0$ (or $\alpha = \frac{x_0+\sqrt{p}y_0}{2}$ if $2|z_0$), then $\alpha \in D_K^+$. By Proposition 2.1 and Lemma 2.1, we conclude that $2|h(K)$ if and only if $K(\sqrt{\alpha})/K$ is an unramified extension if and only if $K(\sqrt{\alpha})/K$ is an unramified extension at all dyadic primes of K if and only if α is a primary element by Lemma 2.6. ■

Let $K_0 = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, where $p \equiv q \equiv 1 \mod 4$ be distinct primes with $(\frac{p}{q}) = -1$. Let ϵ be a fundamental unit of $K_0 = \mathbb{Q}(\sqrt{p})$. Then, by Lemma 2.3, $r_2(C(K)) = 0$, and thus, $\epsilon \in N_{K/K_0}(K)$, which implies that $q \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$,

For the rest of the paper we write $d = \varepsilon \prod_{j=1}^{n} q_j$, where q_j's are distinct odd primes and $\varepsilon \in \{1, 2\}$. By rearranging the primes, we let $m \leq n$ be an integer so that

$$\left(\frac{p}{q_j}\right) = 1 \text{ for } 1 \leq j \leq m \quad \text{and} \quad \left(\frac{p}{q_j}\right) = -1 \text{ for } m+1 \leq j \leq n.$$

3. The case $p \equiv 1 \mod 4$ and $d \equiv 1 \mod 4$

In this section, let $K_0 = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$, where $p \equiv 1 \mod 4$ and $d = \prod_{j=1}^{n} q_j \equiv 1 \mod 4$. Then no dyadic primes are unramified in K/K_0, and so $m + n$ finite primes are ramified in K/K_0. Thus by Lemma 2.3

$$r_2(C(K)) = m + n - 1 - r_2(U_{K_0}/U_{K_0} \cap NK). \tag{3.1}$$

Lemma 3.1. *Suppose that $p \equiv 1 \mod 4$ and $d = \prod_{j=1}^{n} q_j \equiv 1 \mod 4$.*
i) If $q_i \equiv 1 \mod 4$ for all $i \leq n$, and $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for $1 \leq j \leq m$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 0.$$

ii) If either $q_i \equiv 1 \mod 4$ for all $1 \leq i \leq n$ and $q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for some $j \leq m$, or $q_j \equiv 1 \mod 4$ for $1 \leq j \leq m$ and $q_n \equiv 3 \mod 4$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 1.$$

iii) If $q_1 \equiv 3 \mod 4$ and $(\frac{q_1}{p}) = 1$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 2.$$

Proof. i) Since $q_j \equiv 1 \mod 4$ for $1 \leq j \leq n$, the local Hilbert symbol $(-1, d)_Q = 1$ at all primes Q of K_0. Hence $-1 \in NK$. For $1 \leq j \leq m$, let $Q_jQ'_j = q_jO_{K_0}$, the local Hilbert symbol $(\epsilon, d)_{Q_j} = (\epsilon, q_j)_{Q_j} = 1$ by Proposition 2.2; for $m+1 \leq j \leq n$, let $Q_j = q_jO_{K_0}$, the local Hilbert symbol $(\epsilon, d)_{Q_j} = 1$ by [14, Lemma 3.3]. Hence $-1, \epsilon \in NK$.

ii) By the conditions and [14, Lemma 3.3], we know $-1 \in NK$. If $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$, then by Proposition 2.2 the local Hilbert symbol $(\epsilon, d)_{Q_1} = -1$, where $Q_1Q'_1 = q_1O_{K_0}$. If $q_n \equiv 3 \mod 4$ and $(\frac{p}{q_n}) = -1$, then $(\epsilon, d)_{Q_n} = -1$ by [14, Lemma 3.3], where $Q_n = q_nO_{K_0}$. Hence $\epsilon \notin NK$.

iii) If $q_1 \equiv 3 \mod 4$ and $(\frac{q_1}{p}) = 1$, then the local Hilbert symbol $(-1, d)_{Q_1} = (\frac{-1}{q_1}) = -1$, where $Q_1Q'_1 = q_1O_{K_0}$; and $-1 = (-1, d)_{Q_1} = (\epsilon, d)_{Q_1}(\epsilon', d)_{Q_1} = (\epsilon, d)_{Q_1}(\epsilon, d)_{Q'_1}$, where ϵ' is the complex conjugate of ϵ. Hence $-1, \epsilon \notin NK$. ∎

Let, for $1 \leq j \leq m$ and $q_j \equiv 1 \mod 4$, (x_j, y_j, z_j) be a relatively prime and positive integral solution of Diophantine equation $q_jz^2 = x^2 - py^2$, and let $\alpha_j = x_j + \sqrt{p}y_j$ if $2 \nmid z_j$ or $\alpha_j = \frac{x_j + \sqrt{p}y_j}{2}$ if $2 | z_j$.

Theorem 3.1. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ with $p \equiv 1 \mod 4$ and $d = \prod_{j=1}^{n} q_j \equiv 1 \mod 4$.*
i) If $q_i \equiv 1 \mod 4$ for all $i \leq n$ and $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for $1 \leq j \leq m$, then the genus field E of K is given by

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m}).$$

ii) If $q_i \equiv 1 \mod 4$ for all $1 \leq i \leq n$ and $q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for some $j \leq m$, say, $j = 1$, then the genus field E of K is given by

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_j\alpha_1 & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})). \end{cases}$$

iii) If $q_j \equiv 1 \mod 4$ for all $1 \leq j \leq m$ and $q_n \equiv 3 \mod 4$, then the genus field E of K is given by

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q_1^*}, \cdots, \sqrt{q_{n-1}^*}, \sqrt{\alpha_1^*}, \cdots, \sqrt{\alpha_m^*}),$$

where, for $1 \leq j \leq m$

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_jq_n & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})), \end{cases}$$

and, for $1 \le i \le n-1$

$$q_i^* = \begin{cases} q_i & \text{if } q_i \equiv 1 \mod 4 \\ q_i q_n & \text{if } q_i \equiv 3 \mod 4. \end{cases}$$

iv) If $q_1 \equiv 3$ *mod 4 and* $(\frac{q_1}{p}) = 1$*, then the genus field* E *of* K *is given by*

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q_2^*}, \cdots, \sqrt{q_n^*}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$q_i^* = \begin{cases} q_i & \text{if } q_i \equiv 1 \mod 4 \\ q_1 q_i & \text{if } q_i \equiv 3 \mod 4, \end{cases}$$

for $2 \le j \le m$, $\alpha_j = x_j + \sqrt{p} y_j$ *if* $2 \not| z_j$ *(or* $\alpha_j = \frac{x_j + \sqrt{p} y_j}{2}$ *if* $2 | z_j$*),* (x_j, y_j, z_j) *a relatively prime and positive integer solution of a Diophantine equation* $q_j^* z^2 = x^2 - py^2$*, and*

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } \alpha_j \text{ is primary} \\ q_1 \alpha_j & \text{if } \alpha_j \text{ is not primary.} \end{cases}$$

Remark 3.1. *By Corollary 2.1 and Proposition 2.2, it is easy to determine whether either* $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ *or* α_j *is primary.*

Proof. i) By Lemma 3.1 and Proposition 2.1, $r_2(U_{K_0}/U_{K_0} \cap NK) = 0$, and so $D_K^+/K^{*2} = \Delta/K^{*2}$. Hence $r_2(C(K)) = m + n - 1 = r_2(\Delta/K^{*2}) = r_2(D_K^+/K^{*2})$. It is clear that

$$\{q_2, \cdots, q_n, \alpha_1, \cdots, \alpha_m\}$$

is a subset of D_K^+. In order to prove that this set is a set of representatives of D_K^+/K^{*2}, we need to verify that its elements are independent modulo K^{*2}.

Let $K_2 = \mathbb{Q}(\sqrt{pd})$. Consider $\beta = \prod_{k=1}^{u} q_{i_k} \prod_{l=1}^{v} \alpha_{i_l}$, where $\{q_{i_1}, \cdots, q_{i_u}\} \subset \{q_2, \cdots, q_n\}$ and $\{\alpha_{i_1}, \cdots, \alpha_{i_v}\} \subset \{\alpha_1, \cdots, \alpha_m\}$. If $v = 0$ and $u \ge 1$, then $\beta = \prod_{k=1}^{u} q_{i_k} \notin K^2$. Suppose that $v \ge 1$ and $\beta \in K^2$, then

$$N_{K/K_2}(\beta) = a^2 \prod_{l=1}^{v} q_{i_l} \in K_2^2, a \in K_2,$$

which is a contradiction. Therefore it is a set of representatives of D_K^+/K^{*2}. Hence E is the genus field of K.

ii) By Lemma 3.1 and Proposition 2.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK)) = 1$, and so $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 1 = m + n - 1$. By Lemma 2.6 and Proposition 2.2, we conclude that α_j is not primary if and only if $\alpha_1 \equiv a^2 \cdot 3 \mod D^2$, $a \in K_0$ and D any dyadic ideal of K_0, if and only if $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ if and only if $K(\sqrt{\alpha_1})/K$ is ramified at a dyadic prime D. Hence by construction, $\alpha_j^* \equiv 1 \mod D^2$ for $1 \le j \le m$ and

$$\{q_2, \cdots, q_n, \alpha_2^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2}. So E is the genus field of K.

iii) Similarly, we know that $r_2(U_{K_0}/U_{K_0}\cap NK)) = 1$ and $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2})+1 = m+n-1$. By construction, we know that $q_j^* \equiv 1 \mod 4$ for $1 \le j \le n-1$ and $\alpha_j^* \equiv a^2 \mod D^2$ for $1 \le j \le m$, where $a \in K_0$ and D is a dyadic prime of K_0. Hence the set

$$\{q_2^*, \cdots, q_{n-1}^*, \alpha_1^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2} and E is the genus field of K.

iv) In this case $r_2(U_{K_0}/U_{K_0}\cap NK)) = 2$, and so $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2})+2 = m+n-1$. For $2 \le j \le m$, we can see easily that $\alpha_j^* \equiv a^2 \mod D^2$ by Lemma 2.6, where $a \in K_0$ and D is a dyadic prime of K_0. Thus $K(\sqrt{\alpha_j^*})/K$ is an unramified extension. Hence

$$\{q_2^*, \cdots, q_{n-1}^*, \alpha_2^*, \cdots, \alpha_m^*\}$$

is a set of representatives of D/K^{*2} and E is the genus field of K. ■

4. **The case** $p = 2$

In this section, let $K_0 = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{d})$, $d = \prod_{j=1}^{n} q_j$ with

$$q_j \equiv \pm 1 \mod 8, 1 \le j \le m, q_j \equiv \pm 5 \mod 8, m+1 \le j \le n.$$

Let $\epsilon = 1+\sqrt{2}$ be the fundamental unit of K_0. Note that, if $d \equiv 1$ (resp. 3) $\mod 4$, $m+n$ (resp. $m+n+1$) primes are ramified in K/K_0. For a prime $q \equiv 1 \mod 8$, there exist positive integers u, w such that

$$q = u^2 - 2w^2,$$

and u is odd, $w \equiv 0 \mod 4$ by multiplying the totally positive unit $3+2\sqrt{2}$, if necessary.

Lemma 4.1. *Let $q \equiv 1 \mod 8$ be a prime and let ϵ_1 be the fundamental unit of $L = \mathbb{Q}(\sqrt{q})$. Then the following statements are equivalent*
i) $q = a^2 + 32b^2$ for some $a, b \in \mathbb{Z}$, which we denote by $q \in A^+$;
ii) $q = u^2 - 2w^2, u, w \in \mathbb{N}, u \equiv 1 \mod 4$, $w \equiv 0 \mod 4$;
iii) the local Hilbert symbol $(1+\sqrt{2}, q)_Q = 1$, where $QQ' = qO_{K_0}$, $K_0 = \mathbb{Q}(\sqrt{2})$;
iv) the local Hilbert symbol $(\epsilon_1, 2)_D = 1$, where $DD' = 2O_L$.

Proof. We know from [1] that i), ii), iii) are equivalent conditions. Now we prove that iii) is equivalent to iv). Consider $F = \mathbb{Q}(\sqrt{2}, \sqrt{q})$. Let $\epsilon = 1+\sqrt{2}$ and ϵ_1 a fundamental unit of L. By Lemma 2.3 and [2, Theorem 10.3], we conclude that the local Hilbert symbol $(1+\sqrt{2}, q)_Q = 1$ in L if and only if $1+\sqrt{2} \in N_{F/K_0}(F)$ if and only if $2|h(F)$ if and only if $\epsilon_1 \in N_{F/L}(F)$ if and only if the local Hilbert symbol $(\epsilon_1, 2)_D = 1$ in L, where $DD' = 2O_L$. ■

Lemma 4.2. *Let* $p=2$, $d=\prod_{j=1}^{n} q_j$, $K_0=\mathbb{Q}(\sqrt{2})$, $K=\mathbb{Q}(\sqrt{2},\sqrt{d})$.
i) If $q_i \in A^+$ *for all* $1 \le i \le m$ *and* $q_j \equiv 5 \mod 8$ *for all* $m+1 \le j \le n$, *then*

$$r_2(U_{K_0}/U_{K_0} \cap NK)) = 0.$$

ii) If either $q_j \equiv 1 \mod 4$ *for all* $1 \le j \le n$, $q_1 \equiv 1 \mod 8$ *and* $q_1 \notin A^+$, *or* $q_j \equiv 1 \mod 8$ *for all* $1 \le j \le m$ *and* $q_n \equiv 3 \mod 8$, *then*

$$r_2(U_{K_0}/U_{K_0} \cap NK)) = 1.$$

iii) If $q_1 \equiv 7 \mod 8$, *then*

$$r_2(U_{K_0}/U_{K_0} \cap NK)) = 2.$$

Proof. i) It is clear from the conditions that $-1 \in NK$. By Lemma 4.1, we know that the local Hilbert symbol $(\epsilon, d)_{Q_j} = 1$, where $\epsilon = 1+\sqrt{2}$ and $Q_jQ_j' = q_jO_{K_0}$ for $1 \le j \le m$. By [14, Lemma 3.3], we know that the local Hilbert symbol $(\epsilon, d)_{Q_j} = 1$, where $Q_j = q_jO_{K_0}$, for $m+1 \le j \le n$. By Minkowski-Hasse theorem, we have $\epsilon \in NK$. Hence $r_2(U_{K_0}/U_{K_0} \cap NK)) = 0$.

ii) In this case we easily see that $-1 \in NK$. If $q_1 \equiv 1 \mod 8$ and $q_1 \notin A^+$, then the local Hilbert symbol $(\epsilon, d)_{Q_1} = -1$, where $Q_1Q_1' = q_1O_{K_0}$ by Lemma 4.1. If $q_n \equiv 3 \mod 4$, then the local Hilbert symbol $(\epsilon, d)_{Q_n} = -1$, $Q_n = q_nO_{K_0}$ by [14, Lemma 3.3]. Hence $\epsilon \notin NK$.

iii) Since $q_1 \equiv 7 \mod 8$, the local Hilbert symbol $(-1, d)_{Q_1} = (\frac{-1}{q_1}) = -1$, where $Q_1Q_1' = q_1O_{K_0}$, so $-1 \notin NK$. On the other hand, $-1 = (-1,d)_{Q_1} = (\pm\epsilon, d)_{Q_1}(\pm\epsilon, d)_{Q_1'}$, so $\pm\epsilon \notin NK$. ■

Let, for $q_j \equiv 1 \mod 8$, (x_j, y_j) be positive integers satisfying $x_j^2 - 2y_j^2 = q_j$ and $4|y_j$. Let $\alpha_j = x_j + y_j\sqrt{2}$.

Theorem 4.1. *Let* $K=\mathbb{Q}(\sqrt{2},\sqrt{d})$ *with* $d=\prod_{i=1}^{n} q_i$.
i) If $q_j \in A^+$ *for all* $1 \le j \le m$ *and* $q_j \equiv 5 \mod 8$ *for all* $m+1 \le j \le n$, *then the genus field* E *of* K *is given by*

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m}).$$

ii) If $q_i \equiv 1 \mod 4$ *for all* $1 \le i \le n$ *and* $q_1 \equiv 1 \mod 8$ *with* $q_1 \notin A^+$, *then the genus field* E *of* K *is given by*

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in A^+ \\ \alpha_j\alpha_1 & \text{if } q_j \notin A^+. \end{cases}$$

iii) If $q_j \equiv 1 \mod 8$ *for all* $1 \le j \le m$ *and* $q_n \equiv 3 \mod 8$*, then the genus field* E *of* K *is given by*

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{q_1^*}, \cdots, \sqrt{q_{n-1}^*}, \sqrt{a}, \sqrt{\alpha_1^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$q_j^* = \begin{cases} q_j & \text{if } q_j \equiv 1 \mod 4 \\ q_j q_n & \text{if } q_j \equiv 3 \mod 4, \end{cases} \quad a = \begin{cases} q_n & \text{if } d \equiv 3 \mod 4 \\ 1 & \text{if } d \equiv 1 \mod 4, \end{cases} \quad \alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in A^+ \\ \alpha_j q_n & \text{if } q_j \notin A^+. \end{cases}$$

iv) If $q_1 \equiv 7 \mod 8$*, then the genus field* E *of* K *is given by*

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{a}, \sqrt{q_2^*}, \cdots, \sqrt{q_n^*}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where, for $2 \le i \le n$*,*

$$a = \begin{cases} q_1 & \text{if } d \equiv 3 \mod 4 \\ 1 & \text{if } d \equiv 1 \mod 4, \end{cases} \quad q_i^* = \begin{cases} q_i & \text{if } q_i \equiv 1 \mod 4 \\ q_i q_1 & \text{if } q_i \equiv 3 \mod 4, \end{cases}$$

and, for $2 \le j \le m$*,* $\alpha_j = x_j + y_j\sqrt{2}$*, positive integers* (x_j, y_j) *satisfying* $q_j^* = x_j^2 - 2y_j^2$ *with* $4|y_j$*, and*

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } x_j \equiv 1 \mod 4 \\ \alpha_j q_1 & \text{if } x_j \equiv 3 \mod 4. \end{cases}$$

Proof. i) By conditions, $d \equiv 1 \mod 4$ and the dyadic prime of K_0 is unramified in K. Hence by Lemma 4.2 and Proposition 2.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK)) = 0$, $m + n$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) = m + n - 1$. By the similar process of the proof of Theorem 3.1, we see that the set

$$\{q_2, \cdots, q_n, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2} and E is the genus field of K.

ii) By Lemma 4.2 and Proposition 2.1, we see that $r_2(U_{K_0}/U_{K_0} \cap NK)) = 1$, $m+n$ primes of K_0 are ramified in K, and $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 1 = m + n - 1$. As before, we see that the set

$$\{q_2, \cdots, q_n, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}. By Lemma 4.1, we have that $q_1 \notin A^+$ if and only if $\alpha_1 \equiv 3 \mod 4$ if and only if $K(\sqrt{\alpha_1})/K$ is ramified at dyadic prime. By construction, we have that $\alpha_j^* \equiv 1 \mod 4$ for $2 \le j \le m$ and the set

$$\{q_2, \cdots, q_n, \alpha_2^*, \cdots, \alpha_m^*\}$$

is a set of representatives of D_K^+/K^{*2}. Hence E is the genus field of K.

iii) Suppose that $d \equiv 1 \mod 4$ and $q_n \equiv 3 \mod 4$, then $dq_n^e = q_1^* \cdots q_{n-1}^*$, e even, where $q_j^* = q_j$ if $q_j \equiv 1 \mod 4$ and $q_j^* = q_j q_n$ if $q_j \equiv 3 \mod 4$, and the dyadic prime of K_0 is unramified in K. By Lemma 4.2 and Proposition 2.1, $r_2(U_{K_0}/U_{K_0} \cap NK)) = 1$, $m + n$

primes of K_0 are ramified in K, and $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 1 = m+n-1$. We see that the set

$$\{q_1, \cdots, q_{n-2}, q_{n-1}, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}. By construction, we have that $\alpha_j^* \equiv 1 \mod 4$ for $1 \le j \le m$ and the set

$$\{q_1^*, \cdots, q_{n-2}^*, \alpha_1^*, \cdots, \alpha_m^*\}$$

is a set of representatives of D_K^+/K^{*2}. Hence E is the genus field of K.

Suppose that $d \equiv 3 \mod 4$ and $q_n \equiv 3 \mod 4$, then $dq_n^e = q_1^* \cdots q_{n-1}^*$, e odd, and the dyadic prime of K_0 is ramified in K. By Lemma 4.2 and Proposition 2.1, we have that $r_2(U_{K_0}/U_{K_0} \cap NK) = 1$, $m+n+1$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 1 = m+n$. We see that the set

$$\{2, q_1, \cdots, q_{n-1}, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}. Hence by construction,

$$\{q_1^*, \cdots, q_{n-1}^*, \alpha_1^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2}. So E is the genus field of K.

iv) Suppose that $d \equiv 1 \mod 4$ and $q_1 \equiv 7 \mod 8$, then $dq_1^e = q_2^* \cdots q_n^*$, e even, where $q_j^* = q_j$ if $q_j \equiv 1 \mod 4$ and $q_j^* = q_j q_1$ if $q_j \equiv 3 \mod 4$, and the dyadic prime of K_0 is unramified in K. By Lemma 4.2 and Proposition 2.1, we see that $r_2(U_{K_0}/U_{K_0} \cap NK) = 2$, $m+n$ primes of K_0 are ramified in K, and $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 2 = m+n-1$. We see that the set

$$\{q_1, q_2^*, \cdots, q_{n-1}^*, \alpha_1, \alpha_2, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}, where $\alpha_1 = x_1 + \sqrt{2}y_1$ with positive integers (x_1, y_1) satisfying $x_1^2 - 2y_1^2 = q_1$, and for $2 \le j \le m$, $\alpha_j = x_j + \sqrt{2}y_j$ with positive integers (x_j, y_j) satisfying $q_j^* = x_j^2 - 2y_j^2$ with $4|y_j$. By construction, we know that $\alpha_j^* \equiv 1 \mod 4$ for $2 \le j \le m$. Hence the set

$$\{q_2^*, \cdots, q_{n-1}^*, \alpha_2^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2}. So E is the genus field of K.

Suppose $d \equiv 3 \mod 4$ and $q_1 \equiv 7 \mod 8$, then $dp_1^e = p_2^* \cdots p_n^*$, e odd, and the dyadic prime of K_0 is ramified in K. By Lemma 4.2, $r_2(U_{K_0}/U_{K_0} \cap NK) = 2$, $m+n+1$ primes of K_0 are ramified in K, and $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 2 = m+n$. We see that the set

$$\{2, q_2^*, \cdots, q_n^*, \alpha_1, \alpha_2, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}, where q_j^* and α_j are defined as above. Since $\alpha_j \equiv x_j \mod 4$ for $2 \leq j \leq m$, the set

$$\{q_2^*, \cdots, q_n^*, \alpha_2^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2} and E is the genus field of K. ■

5. The case $p \equiv 1 \mod 4$ and $d \equiv 2 \mod 4$

In this section, let $K_0 = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$, a prime $p \equiv 1 \mod 4$ and $d = 2\prod_{j=1}^{n} q_j$ with

$$\left(\frac{p}{q_j}\right) = 1 \text{ for } 1 \leq j \leq m \tag{5.1}$$

$$\left(\frac{p}{q_j}\right) = -1 \text{ for } m+1 \leq j \leq n. \tag{5.2}$$

Note that $m+n$ odd primes are ramified in K/K_0. If $p \equiv 1 \mod 8$, then two dyadic primes are ramified in K/K_0; if $p \equiv 5 \mod 8$, then one dyadic prime is ramified in K/K_0. Let $p \equiv 1 \mod 8$, then $u^2 - 2w^2 = p$, $u, w \in \mathbb{N}, w \equiv 0 \mod 4$, and set $\alpha_0 = \frac{u+\sqrt{p}}{2}$.

Lemma 5.1. *Let $p \equiv 1 \mod 4$ and $d = 2\prod_{j=1}^{n} q_j \equiv 2 \mod 4$. Let ϵ be a fundamental unit of K_0.*

i) If either $p \in A^+$ or $p \equiv 5 \mod 8$, all $q_i \equiv 1 \mod 4$ for $1 \leq i \leq n$ and all $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for $1 \leq j \leq m$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 0.$$

ii) If one of the following four conditions holds,

(1) $p \equiv 1 \mod 8$, all $q_j \equiv 1 \mod 4$ for $1 \leq j \leq n$, and either $p \notin A^+$ or $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$;

(2) $p \equiv 5 \mod 8$, all $q_j \equiv 1 \mod 4$ for $1 \leq j \leq n$, and $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$;

(3) $d/2 \equiv 1 \mod 4$, $q_j \equiv 1 \mod 4$ for $1 \leq j \leq m$, and $q_n \equiv 3 \mod 4$;

(4) $p \equiv 5 \mod 8$, $d/2 \equiv 3 \mod 4$, all $q_j \equiv 1 \mod 4$ for $1 \leq j \leq m$;

then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 1.$$

iii) If either $p \equiv 1 \mod 8$, $d/2 \equiv 3 \mod 4$, $q_j \equiv 1 \mod 4$ for all $1 \leq j \leq m$, or $q_1 \equiv 3 \mod 4$ and $(\frac{q_1}{p}) = 1$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 2.$$

Proof. i) Suppose that $p \in A^+$ and $q_i \equiv 1 \mod 4$ for any $1 \le i \le n$, and $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for all $1 \le j \le m$. Then $-1 \in NK$. Since $p \in A^+$, by Lemma 4.1 the local Hilbert symbol $(\epsilon, d)_D = (\epsilon, 2)_D = 1$, where D is any dyadic prime of K_0. From the fact that $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for $1 \le j \le m$ and Proposition 2.2, the local Hilbert symbol $(\epsilon, d)_{Q_j} = (\epsilon, q_j)_{Q_j} = 1$, where $Q_jQ'_j = q_jO_{K_0}$. For $m+1 \le j \le n$, by [14, Lemma 3.3] the local Hilbert symbol $(\epsilon, d)_{Q_j} = 1$, where $Q_j = q_jO_{K_0}$. Hence $\epsilon \in NK$.

Suppose that $p \equiv 5 \mod 8$, by [14, Lemma 3.3] the local Hilbert symbol $(\epsilon, d)_D = 1$, where D is a dyadic prime of K_0. Similarly, we get $\epsilon \in NK$.

ii)-(1) It is clear that $-1 \in NK$. Suppose that $p \notin A^+$, then the local Hilbert symbol $(\epsilon, d)_D = (\epsilon, 2)_D = -1$ by Lemma 4.1, where D is a dyadic prime of K_0. Suppose that $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$, then the local Hilbert symbol $(\epsilon, d)_{Q_1} = -1$ by Proposition 2.2, where $Q_1Q'_1 = q_1O_{K_0}$. Hence $\epsilon \notin NK$.

Similarly, we can get the results in cases (2), (3), (4).

iii) suppose that $p \equiv 1 \mod 8$, $d/2 \equiv 3 \mod 4$, $q_j \equiv 1 \mod 4$ for all $1 \le j \le m$. Since $d/2 \equiv 3 \mod 4$ and $p \equiv 1 \mod 8$, the local Hilbert symbol $(-1, d)_D = -1$, where $DD' = 2O_{K_0}$. Similarly we can prove that $\epsilon \notin NK$.

Now Suppose that $q_1 \equiv 3 \mod 4$ and $(\frac{q_1}{p}) = 1$. Since $q_1 \equiv 3 \mod 4$ and $(\frac{q_1}{p}) = 1$, the local Hilbert symbol $(-1, d)_{Q_1} = -1$, where $Q_1Q'_1 = q_1O_{K_0}$. Similarly, we can prove that $\epsilon \notin NK$. ■.

Let, for $1 \le j \le m$ and $q_j \equiv 1 \mod 4$, (x_j, y_j, z_j) be a relatively prime and positive integral solution of Diophantine equation $q_jz^2 = x^2 - py^2$, and let $\alpha_j = x_j + \sqrt{p}y_j$ if $2 \nmid z_j$ or $\alpha_j = \frac{x_j+\sqrt{p}y_j}{2}$ if $2|z_j$. Let $p \equiv 1 \mod 8$, then $u^2 - 2w^2 = p$, $u, w \in \mathbb{N}, w \equiv 0 \mod 4$, and set $\alpha_0 = \frac{u+\sqrt{p}}{2}$.

Theorem 5.1. *Let* $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ *with* $p \equiv 1$ *mod 4 and* $d = 2\prod_{j=1}^{n} q_j \equiv 2$ *mod 4.*

i) If either $p \in A^+$ *or* $p \equiv 5$ *mod 8, all* $q_j \equiv 1$ *mod 4 for* $1 \le j \le n$ *and all* $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ *for* $1 \le j \le m$*, then*

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{2}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{a}, \sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m}),$$

where

$$a = \begin{cases} \alpha_0 & \text{if } p \in A^+ \\ 1 & \text{if } p \equiv 5 \text{ mod } 8. \end{cases}$$

ii) If $p \equiv 1$ *mod 8, all* $q_j \equiv 1$ *mod 4 for* $1 \le j \le n$*, and either* $p \notin A^+$ *or* $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$*, then*

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{2}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{a}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$a = \begin{cases} \alpha_0 & \text{if } p \in A^+ \\ \alpha_1 & \text{if } q_1 \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_0\alpha_1 & \text{if } p \notin A^+, q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})), \end{cases}$$

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_j b & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})), \end{cases} \quad b = \begin{cases} \alpha_1 & \text{if } p \in A^+ \\ \alpha_0 & \text{if } p \notin A^+. \end{cases}$$

iii) If $p \equiv 5 \mod 8$, all $q_j \equiv 1 \mod 4$ for $1 \le j \le n$, and $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$, then

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{2}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_j\alpha_1 & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})), \end{cases}$$

iv) If $d/2 \equiv 1 \mod 4$, $q_j \equiv 1 \mod 4$ for $1 \le j \le m$, and $p_n \equiv 3 \mod 4$, then

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{2}, \sqrt{q_1^*}, \cdots, \sqrt{q_{n-1}^*}, \sqrt{\alpha_0^*}, \sqrt{\alpha_1^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$q_j^* = \begin{cases} q_j & \text{if } q_j \equiv 1 \mod 4 \\ q_jq_n & \text{if } q_j \equiv 3 \mod 4 \end{cases} \quad \text{for } 1 \le j \le n-1,$$

$$\alpha_0^* = \begin{cases} 1 & \text{if } p \equiv 5 \mod 8 \\ \alpha_0 & \text{if } p \in A^+ \\ \alpha_0 q_n & \text{if } p \notin A^+ \text{ and } p \equiv 1 \mod 8, \end{cases}$$

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_j q_n & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \end{cases} \quad \text{for } 1 \le j \le m.$$

v) If $p \equiv 5 \mod 8$, $d/2 \equiv 3 \mod 4$, $q_j \equiv 1 \mod 4$ for $1 \le j \le m$, then

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q_1^*}, \cdots, \sqrt{q_n^*}, \sqrt{\alpha_1^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$q_j^* = \begin{cases} q_j & \text{if } q_j \equiv 1 \mod 4 \\ 2q_j & \text{if } q_j \equiv 3 \mod 4, \end{cases} \quad \alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ 2\alpha_j & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})). \end{cases}$$

vi) If $p \equiv 1 \mod 8$, $d/2 \equiv 3 \mod 4$, all $q_j \equiv 1 \mod 4$ for $1 \le j \le m$, then

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{q_1^*}, \cdots, \sqrt{q_n^*}, \sqrt{\alpha_1^*}, \cdots, \sqrt{\alpha_m^*}),$$

where each q_j^* and α_j^* are defined as Case v).

vii) If $q_1 \equiv 3$ mod 4 and $(\frac{q_1}{p}) = 1$, then

$$E = \mathbb{Q}(\sqrt{p}, \sqrt{a}, \sqrt{q_2^*}, \cdots, \sqrt{q_n^*}, \sqrt{b}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$a = \begin{cases} 2 & \text{if } d/2 \equiv 1 \mod 4 \\ 2q_1 & \text{if } d/2 \equiv 3 \mod 4, \end{cases} \quad q_i^* = \begin{cases} q_i & \text{if } q_i \equiv 1 \mod 4 \\ q_1 q_i & \text{if } q_i \equiv 3 \mod 4, \end{cases}$$

$$b = \begin{cases} \alpha_0 & \text{if } p \in A^+ \\ q_1\alpha_0 & \text{if } p \notin A^+ \text{ and } p \equiv 1 \mod 8 \\ 1 & \text{if } p \equiv 5 \mod 8, \end{cases}$$

for $2 \le j \le m$, $\alpha_j = x_j + \sqrt{p}y_j$ if $2 \not| z_j$ (or $\alpha_j = \frac{x_j + \sqrt{p}y_j}{2}$ if $2|z_j$), (x_j, y_j, z_j) a relatively prime and positive integral solution of a Diophantine equation $q_j^* z^2 = x^2 - py^2$, and

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } \alpha_j \text{ is primary} \\ q_1\alpha_j & \text{if } \alpha_j \text{ is not primary.} \end{cases}$$

Proof. i) Suppose that $p \in A^+$ and $d \equiv 2 \mod 4$, two dyadic primes of K_0 are ramified in K. By the conditions and Lemma 5.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK) = 0$, $m + n + 2$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) = m + n + 1$. Hence we see that the set

$$\{2, q_1, \cdots, q_{n-1}, \alpha_0, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}. Hence E is the genus field of K.

Suppose $p \equiv 5$ mod 8 and $d \equiv 2 \mod 4$, then the dyadic prime of K_0 is ramified in K. By conditions and Lemma 5.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK) = 0$, $m + n + 1$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) = m + n$. Hence we see that the set

$$\{2, q_1, \cdots, q_{n-1}, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2} and E is the genus field of K.

ii) Since $p \equiv 1$ mod 8 and $d \equiv 2 \mod 4$, two dyadic primes of K_0 are ramified in K. By conditions and Lemma 5.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK) = 1$, $m + n + 2$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 1 = m + n + 1$. Hence we see that the set

$$\{2, q_1, \cdots, q_{n-1}, \alpha_0, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}.

Suppose that $p \in A^+$ and $q_1 \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$. Let $p = u^2 - 2w^2, u, w \in \mathbb{N}, w \equiv 0$ mod 4. By Lemma 4.1 we have that $p \in A^+$ if and only if $u \equiv 1$ mod 4. Let $D = (2, \frac{u-\sqrt{p}}{2})$, $D' = (2, \frac{u+\sqrt{p}}{2})$ be dyadic primes of K_0. Since $w \equiv 0 \mod 4$,

$$\frac{u + \sqrt{p}}{2} \cdot \frac{u - \sqrt{p}}{2} = \frac{w^2}{4} \equiv 0 \mod 4$$

and $\alpha_0' = \frac{u-\sqrt{p}}{2} \in D^2$. Hence

$$\alpha_0 = \frac{u+\sqrt{p}}{2} = u - \frac{u-\sqrt{p}}{2} \equiv u \mod D^2.$$

Let $\frac{w^2}{4} = 2^e \cdot f^2$, $e, f \in \mathbb{N}$, $2 \not| f, e$ even, then $\alpha_0 \cdot \alpha_0'/2^e \equiv f^2 \mod D^2$ and $\alpha_0'/2^e \equiv u \mod D^2$, i.e. $\alpha_0/2^e \equiv u \mod (D')^2$, where $\alpha_0' = \frac{u-\sqrt{p}}{2}$. Hence we see that the set

$$\{2, q_1, \cdots, q_{n-1}, \alpha_0, \alpha_2^*, \cdots, \alpha_n^*\}$$

is a set of representatives of Δ/K^{*2}, where $\alpha_j^* = \alpha_j$ if $q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ and $\alpha_j^* = \alpha_j \cdot \alpha_1$ if $q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$. Similarly we can prove other cases.

iii), iv) They are clear from ii).

v) Since $p \equiv 5 \mod 8$ and $d/2 \equiv 3 \mod 4$, one dyadic prime of K_0 is ramified in K and $d2^e = q_1^* \cdots q_n^*$, e even, where for $1 \le j \le n$, $q_j^* = q_j$ if $q_j \equiv 1 \mod 4$ and $q_j^* = 2q_j$ if $q_j \equiv 3 \mod 4$. By Lemma 5.1 and Proposition 2.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK) = 1$, $m+n+1$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 1 = m+n$. Hence we see that the set

$$\{2, q_1, \cdots, q_{n-1}, \alpha_1, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}. Thus by construction,

$$\{q_1^*, \cdots, q_{n-1}^*, \alpha_1^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2}, where each q_j^* and α_j^* are defined as above. Hence E is the genus field of K.

vi) It is clear from v).

vii) Suppose that $p \equiv 1 \mod 8$, $d/2 \equiv 1 \mod 4$ and $q_1 \equiv 3 \mod 4$, then two dyadic primes of K_0 are ramified in K and $dq_1^e = q_2^* \cdots q_n^*$, e even. By Lemma 5.1 and Proposition 2.1, we know that $r_2(U_{K_0}/U_{K_0} \cap NK) = 2$, $m+n+2$ primes of K_0 are ramified in K, $r_2(D_K^+/K^{*2}) = r_2(\Delta/K^{*2}) + 2 = m+n+1$. Hence we see that the set

$$\{2, q_1, q_2^*, \cdots, q_{n-1}^*, \alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_m\}$$

is a set of representatives of D_K^+/K^{*2}. By the same process of proving Theorem 3.1 iii), we see that the set

$$\{2, q_2^*, \cdots, q_{n-1}^*, \alpha_0^*, \alpha_2^*, \cdots, \alpha_m^*\}$$

is a set of representatives of Δ/K^{*2}. Hence E is the genus field of K. Similarly, we can prove the other case. ∎

6. Function Fields

In this section we study the case of function fields. Let q be a power of an odd prime p and $\mathbb{F}_q$ be a finite field with q elements. Let $k = \mathbb{F}_q(T)$, $\mathbb{A} = \mathbb{F}_q[T]$ and $\mathbb{A}^+$ be the subset of $\mathbb{A}$ consisting of monic polynomials. Let ∞ be the place associated to the place $(\frac{1}{T})$. By a function field K we mean a finite extension of k. The places of K lying over ∞ are called the *infinite places*. The Hilbert class field of K is defined to be the maximal unramified abelian extension H_K of K, in which the infinite places of K splits completely. For more details for genus fields of function fields, we refer to [9].

Let $P \in \mathbb{A}^+$ be an irreducible polynomial of even degree, and $D = \prod_{i=1}^{n} Q_i$ be a squarefree monic polynomial with $Q_i \in \mathbb{A}^+$ irreducible. In this section we are going to describe the genus field E of $K = k(\sqrt{P}, \sqrt{D})$ over $K_0 = k(\sqrt{P})$ explicitly. We will see that the case that $\deg D$ is odd (resp. even) corresponds to the case that $d \equiv 3 \mod 4$ (resp. $d \equiv 1 \mod 4$) in the number field case.

Let $k_\infty := \mathbb{F}_q((\frac{1}{T}))$ and sgn be the usual sign function on k_∞. For a finite extension L of k and a place v lying over ∞, sgn_v is defined to be $sgn \circ N_v$, where N_v is the local norm map from L_v to k_∞. Let

$$\overline{sgn}_v := sgn_v^{\frac{q-1}{2}}.$$

An element $a \in L^*$ is said to be *positive at* v if $\overline{sgn}_v(a) = 1$, and is called *totally positive* if it is positive at every infinite place v of L. Let π_v be the uniformizer of L_v. For $a \in L$, the degree of a at v, written $\deg_v(a)$, is defined to be i if $a = \pi_v^{-i}u$, where u is a local unit at v.

Let $K_0 = k(\sqrt{P})$. Then there exists a fundamental unit ϵ with $N\epsilon = \gamma$, where N is the norm map from K_0 to k and γ is a generator of $\mathbb{F}_q^*$. Assume that $\left(\frac{Q_j}{P}\right) = 1$ for $1 \le j \le m$ and $\left(\frac{Q_j}{P}\right) = -1$ for $m+1 \le j \le n$. Define

$$D_K := \{x \in K^* | v_{\mathfrak{p}}(x) \equiv 0 \mod 2 \text{ for all finite places } \mathfrak{p} \text{ of } K\},$$

$$D_K^+ := \{x \in D_K | x \text{ totally positive}\},$$

and

$$\Delta := \{x \in D_K^+ : \deg_v(x) \text{ is even for every infinite place } v \text{ of } K\}.$$

Then we clearly have the genus field E of K is $K(\sqrt{\Delta})$.

We can show that the function field analogues of Lemma 2.2, 2.3 and Proposition 2.1 remain true. We remark that for $x \in D_K^+$, $K(\sqrt{x})/K$ is unramified at all places, but the infinite places can be inert, that is, may not split. If $x \in \Delta$ then the infinite places of K splits in $K(\sqrt{x})/K$. For $\left(\frac{Q_j}{P}\right) = 1$, there exist $(x_j, y_j, z_j) \in \mathbb{A}^3$ such that $\alpha_j := x_j + y_j\sqrt{P}$ is totally positive. Let v_1 and v_2 be the infinite places of K_0. In the case $\deg Q_j$ is odd, we put an additional condition that $\deg_{v_1}(\alpha_j)$ is even and $\deg_{v_2}(\alpha_j)$ is odd, which is possible because

$$\deg_{v_1}(\alpha_j) + \deg_{v_2}(\alpha_j) = \deg_{v_1}(\alpha_j) + \deg_{v_1}(\alpha_j') = \deg(Q_j z_j^2),$$

which is odd. Here α' means the conjugate of α in K_0 over k.

Remark 6.1. *In the case of function field no dyadic primes arise, and this fact makes the situation easier than number field case. But one needs to deal the infinite places more carefully, because, for an infinite place v to split in $K(\sqrt{\alpha})$, α should be positive at v and $\deg_v(\alpha)$ should be even.*

Theorem 6.1. *Suppose that $\deg D$ is odd. Then the genus field of $K = \mathbb{F}_q(\sqrt{P}, \sqrt{D})$ is given by*

$$\mathbb{F}_q(\sqrt{P}, \sqrt{Q}_1, \ldots, \sqrt{Q}_n, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m}).$$

Proof. Since *degD* is odd, ∞ is ramified in K. Thus $\deg_v(\alpha_j)$ is even for every infinite place v of K. The rest are the same as in the number field case. (See [15]) ■

To consider the case when $\deg D$ is even we need the following analogue of Proposition 2.2, whose proof is similar.

Proposition 6.1. *Let P, Q be a monic primes of even degree. Assume that $(\frac{P}{Q}) = 1$ and let ϵ be a fundamental unit of $K_0 = k(\sqrt{P})$. If $(x_0, y_0, z_0) \in \mathbb{A}^3$ is a relatively prime solution of the Diophantine equation $Qz^2 = x^2 - Py^2$ so that $\alpha = x_0 + \sqrt{P}y_0$ is totally positive. Then $2|h(k(\sqrt{P}, \sqrt{Q}))$ if and only if $Q \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ if and only if $\deg_v(\alpha)$ is even for every infinite place v of K.*

Note that $\deg_v(\alpha)$ is even for every infinite place v of K is equivalent to $\deg_v(\alpha)$ is even for some infinite place v of K, since $\deg Q$ is even. We also need the following analogue of Lemma 3.1.

Lemma 6.1. *Suppose that $\deg P$ and $\deg(D = \prod_{i=1}^n Q_i)$ are even.*
i) If $\deg Q_i$ is even for every $i \leq n$, and $Q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for $1 \leq j \leq m$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 0.$$

ii) If either $\deg Q_i$ is even for every $1 \leq i \leq n$ and $Q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for some $j \leq m$, or $\deg Q_j$ is even for every $1 \leq j \leq m$ and $\deg Q_n$ is odd, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 1.$$

iii) If $\deg Q_1$ is odd and $(\frac{Q_1}{P}) = 1$, then

$$r_2(U_{K_0}/U_{K_0} \cap NK) = 2.$$

We finally get;

Theorem 6.2. *Let $K = k(\sqrt{P}, \sqrt{D})$ with $\deg P$ and $\deg D$ even.*
i) If $\deg Q_i$ is even for every $1 \le i \le n$ and $Q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for $1 \le j \le m$, then the genus field E of K is given by

$$E = k(\sqrt{P}, \sqrt{Q_1}, \cdots, \sqrt{Q_n}, \sqrt{\alpha_1}, \cdots, \sqrt{\alpha_m}).$$

ii) If $\deg Q_i$ is even for every $1 \le i \le n$ and $Q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon}))$ for some $j \le m$, say, $j = 1$, then the genus field E of K is given by

$$E = k(\sqrt{P}, \sqrt{Q_1}, \cdots, \sqrt{Q_n}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where, for $2 \le j \le m$,

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_j\alpha_1 & \text{if } q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})). \end{cases}$$

iii) If $\deg Q_j$ is even for every $1 \le j \le m$ and $\deg Q_n$ is odd, then the genus field E of K is given by

$$E = k(\sqrt{P}, \sqrt{Q_1^*}, \cdots, \sqrt{Q_{n-1}^*}, \sqrt{\alpha_1^*}, \cdots, \sqrt{\alpha_m^*}),$$

where, for $1 \le j \le m$,

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } Q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_j Q_n & \text{if } Q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})), \end{cases}$$

and, for $1 \le i \le n$

$$Q_i^* = \begin{cases} Q_i & \text{if } \deg Q_i \text{ is even} \\ Q_i Q_n & \text{if } \deg Q_i \text{ is odd.} \end{cases}$$

iv) If $\deg Q_1$is odd and $(\frac{Q_1}{P}) = 1$, then the genus field E of K is given by

$$E = k(\sqrt{P}, \sqrt{Q_2^*}, \cdots, \sqrt{Q_n^*}, \sqrt{\alpha_2^*}, \cdots, \sqrt{\alpha_m^*}),$$

where

$$Q_i^* = \begin{cases} Q_i & \text{if } \deg Q_i \text{ is even} \\ Q_1 Q_i & \text{if } \deg Q_i \text{ is odd} \end{cases}$$

and for $2 \le j \le m$,

$$\alpha_j^* = \begin{cases} \alpha_j & \text{if } \deg Q_j \text{ is even and } Q_j \in N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ Q_1\alpha_j & \text{if } \deg Q_j \text{ is even and } Q_j \notin N_{K_0(\sqrt{\epsilon})/K_0}(K_0(\sqrt{\epsilon})) \\ \alpha_1\alpha_j & \text{if } \deg Q_j \text{ is odd.} \end{cases}$$

Proof. The proof is almost the same as that of Theorem 3.1, except the last assertion. This comes from our choice of α_j so that $\alpha_1\alpha_j$ has even degree at every infinite place of K. ■

References

[1] Barrucand, P. and Cohn, H., *Note on primes of type x^2+32y^2, class number, and residuality*, J. reine angew. Math. 238 (1969), 67-70

[2] Conner, P. E. and Hurrelbrink, J., *Class Number parity*, Series in Pure Math. vol. 8, World Scientific, Singapore-New Jersey-Hong Kong

[3] Fouvry, E. and Klüners, J., *On the negative Pell equation*, To appear in Ann. Math.

[4] Fröhlich, A., *Central extensions, Galois groups, and ideal class groups of number fields*, Contemporary Math. v. 24, Amer. Math. Soc. (1983)

[5] Herglotz, G., *Über einen Dirichletschen Satz*, Math. Z. 12(1922), 225-261.

[6] Janusz, G., *Algebraic Number Fields*, Springer-Verlag, New York-Heidelberg-Berlin, 1987

[7] Lang, S., *Cyclotomic fields I and II*, GTM 121, Springer-Verlag, New York-Heidelberg-Berlin, 1990

[8] Neukirch, J., *Class field theory*, Springer-Verlag, New York-Heidelberg-Berlin, 1980

[9] Peng, G., *The genus field of Kummer function fields*, J. Number Th. 98 (2003), 221-227

[10] Sime, P., *Hilber class fields of real biquadratic fields*, J. Number Th. 50 (1995), 154-166

[11] Stevenhagen, P., *The number of real quadratic fields with units of negative norms. Experiment. Math.*, 2 (1993), 121-136

[12] Weiss, E., *Algebraic Number Theory*, McGraw-Hill Book Company. Inc, 1963.

[13] Yue, Q., *Tame kernels for biquadratic number fields*, K-Theory 35(2005), 69-91

[14] Yue, Q., *The generalized Redei matrix*, Math. Zeit. 261 (2009), 23-37

[15] Yue, Q., *Genus fields of real biquadratic feilds*, to appear in the Ramanujan Journal.

Department of Mathematics, KAIST, Taejon 305-701, Korea
shbae(at)kaist.ac.kr

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, P.R. China
yueqin(at)nuaa.edu.cn