Ramanujan J (2015) 37:345–363
DOI 10.1007/s11139-014-9558-7

Hilbert genus fields of real biquadratic fields

Yi Ouyang · Zhe Zhang

Received: 8 September 2013 / Accepted: 11 January 2014 / Published online: 14 May 2014

Abstract The Hilbert genus field of the real biquadratic field $K = \mathbb{Q}(\sqrt{\delta}, \sqrt{d})$ is described by Yue (Ramanujan J 21:17–25, 2010) and by Bae and Yue (Ramanujan J 24:161–181, 2011) explicitly in the case $\delta = 2$ or p with $p \equiv 1 \bmod 4$ a prime and d a squarefree positive integer. In this article, we describe explicitly the case that $\delta = p, 2p$ or $p_1 p_2$ where p, p_1, and p_2 are primes congruent to 3 modulo 4, and d is any squarefree positive integer, thus complete the construction of the Hilbert genus field of real biquadratic field $K = K_0(\sqrt{d})$ such that $K_0 = \mathbb{Q}(\sqrt{\delta})$ has an odd class number.

Keywords Class group · Hilbert symbol · Hilbert genus field

Mathematics Subject Classification 11R65 · 11R37

1 Introduction

For a number field K, the *Hilbert genus field of K* is the subfield E of the Hilbert class field H invariant under Gal $(H/K)^2$. Note that the Galois group $G =$ Gal (H/K) is isomorphic to the ideal class group $C(K)$ of K via Artin's reciprocity map. Then by Galois theory

This work was partially supported by the National Key Basic Research Program of China (Grant 2013CB834202) and the National Natural Science Foundation of China (Grant 11171317).

Y. Ouyang · Z. Zhang (✉)
Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences,
University of Science and Technology of China, Hefei 230026,
Anhui, People's Republic of China
e-mail: lmlz@mail.ustc.edu.cn

Y. Ouyang
e-mail: yiouyang@ustc.edu.cn

$$\text{Gal}\,(E/K) \simeq G/G^2 \simeq C(K)/C(K)^2.$$

Let Δ be the unique multiplicative group such that $K^{*2} \subset \Delta \subset K^*$ and

$$E = H \cap K(\sqrt{K^*}) = K(\sqrt{\Delta}). \tag{1}$$

Given K, a natural question to ask is how to explicitly construct the Hilbert genus field E of K, or equivalently, how to give a set of generators for the finite group Δ/K^{*2}.

Suppose δ and d are squarefree integers, and K is the biquadratic field $\mathbb{Q}(\sqrt{\delta}, \sqrt{d})$. Recently much work has been done on explicit construction of the Hilbert genus field E of K. Bae and Yue [1] worked out the case for real biquadratic fields $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ with prime $p \equiv 1 \bmod 4$ or 2, following earlier work of Sime [6] and Yue [8]. Note that in their case, $\mathbb{Q}(\sqrt{p})$ has odd ideal class number. In [5], we worked out the case that K is biquadratic and $K_0 = \mathbb{Q}(\sqrt{\delta})$ is imaginary with odd ideal class number, i.e., $\delta = -1, -2$ or $-p$ with $p \equiv 3 \bmod 4$.

In this paper, we shall work out the construction of the Hilbert genus field of $K = K_0(\sqrt{d})$ for $\delta = p, 2p$ or p_1p_2 where p, p_1, p_2 are primes $\equiv 3 \bmod 4$ and d a squarefree positive integer. Combining with the results of Bae and Yue [1], this completes the construction of the Hilbert genus field of real biquadratic fields $K = K_0(\sqrt{d})$ such that K_0 has odd class number.

Our strategy to explicitly construct E follows from [1,5,8]. From now on, we suppose

(1) $K = \mathbb{Q}(\sqrt{\delta}, \sqrt{d})$ where $\delta = p, 2p$ or p_1p_2 with p, p_1, p_2 primes $\equiv 3 \bmod 4$, and d a squarefree positive integer;
(2) $K_0 = \mathbb{Q}(\sqrt{\delta})$ which has odd class number in our case (see [2, page. 134]);
(3) $E = K(\sqrt{\Delta})$ the Hilbert genus field of K where $K^{*2} \subset \Delta \subset K^*$;
(4) s is the number of finite primes of K_0 ramified in K.
(5) $t = r_2(U_{K_0}/U_{K_0} \cap N_{K/K_0}K)$ where N_{K/K_0} is the norm map and for a finite abelian group A, $r_2(A)$ is the 2-rank of A.
(6) $D_K^+ = \{x \in K^* \mid x \text{ totally positive and } v_{\mathfrak{p}}(x) \equiv 0 \bmod 2 \text{ for all finite primes } \mathfrak{p} \text{ of } K\}$.

We shall use the following facts from time to time.

Proposition 1.1 *Assume K and K_0 are given above.*

(1) For any $x \in D_K^+$, all nondyadic primes of K are unramified in $K(\sqrt{x})$. Moreover, $\Delta \subset D_K^+$.
(2) We have

$$r_2(C(K)) = r_2(\Delta/K^{*2}) = s - 1 - t. \tag{2}$$

Proof (1) The proof is similar to that of [8], Lemma 2.1.
(2) The second equality follows from (i) $r_2(C(K)) = r_2\left(C(K)^{\text{Gal}\,(K/K_0)}\right)$, (ii) $C(K)^{\text{Gal}\,(K/K_0)}$ has no 4-torsion, since K_0 has odd class number, and (iii) by the class number formula [3, Lemma 4.1, P.307] for cyclic extensions,

$$\left|C(K)^{\mathrm{Gal}(K/K_0)}\right| = |C(K_0)| \cdot \frac{2^{s-1}}{[U_{K_0} : U_{K_0} \cap NK]}.$$

□

By Proposition 1.1. we first study the group $U_{K_0}/U_{K_0} \cap N_{K/K_0}K$ to obtain the 2-ranks of Δ/K^{*2}. Then we find a set of representatives of Δ/K^{*2}. Our results are stated in Theorem 3.5 ($\delta = p$ case), Theorem 4.4 ($\delta = 2p$ case) and Theorems 5.4, 5.7, 5.9, 5.12, and 5.15 ($\delta = p_1 p_2$ case). To illustrate our results, we give three examples here.

Example 1.2 (Theorem 3.5) Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{115115})$. It is clear that $115115 = 5 \times 7 \times 11 \times 13 \times 23 \equiv 3 \bmod 4$, $\left(\frac{3}{5}\right) = \left(\frac{3}{7}\right) = -1$ and $\left(\frac{3}{11}\right) = \left(\frac{3}{13}\right) = \left(\frac{3}{23}\right) = 1$. Then $n = 5$, $m = 3$, $Q_+ = \{11, 13, 23\}$, and $r_2(Q_+) = 2$. Let $q_1 = 11$, $q_2 = 13$. We see that $\sigma(23) = \sigma(q_1)\sigma(q_2)$, thus, $\widetilde{q}_3 = 11 \times 13 \times 23 = 3289$. By computation, $3289 = 709^2 - 3 \times 408^2$, let $\alpha_3 = 709 + 408\sqrt{3}$, then

$$E = \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{23}, \sqrt{\alpha_3}).$$

Example 1.3 (Theorem 4.4) Let $K = \mathbb{Q}(\sqrt{14}, \sqrt{1921})$. It is clear that $1921 = 17 \times 113 \equiv 1 \bmod 4$, $\left(\frac{14}{17}\right) = -1$, and $\left(\frac{14}{113}\right) = 1$. Then $n = 2$, $m = 1$, $Q_+ = \{113\}$, $r_2(Q_+) = 0$, and $\widetilde{q}_1 = 113$. By computation, $113 = 307^2 - 14 \times 82^2$, let $\alpha_1 = 307 + 82\sqrt{14}$, then

$$E = \mathbb{Q}(\sqrt{14}, \sqrt{17}, \sqrt{113}, \sqrt{\alpha_1}).$$

Example 1.4 (Theorem 5.4) Let $K = \mathbb{Q}(\sqrt{21}, \sqrt{12155})$. It is clear that $12155 = 5 \times 11 \times 13 \times 17 \equiv 3 \bmod 4$, $\left(\frac{21}{11}\right) = \left(\frac{21}{13}\right) = -1$, and $\left(\frac{21}{5}\right) = \left(\frac{21}{17}\right) = 1$. Then $n = 4$, $m = 2$, $Q_+ = \{5, 17\}$, $r_2(Q_+) = 1$, $q_1 = 5$ and $\widetilde{q}_2 = 5 \times 17 = 85$. By computation, $85 = 1219^2 - 21 \times 266^2$, let $\alpha_2 = 1219 + 266\sqrt{21}$, then

$$E = \mathbb{Q}(\sqrt{3}, \sqrt{7}, \sqrt{5}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{\alpha_2}).$$

2 Preliminary results

We fix the following notations in this section:

For a number field or local field F, we let $\mathcal{O}_F$ be the ring of integers of F and U_F the unit group of $\mathcal{O}_F$. If F is a number field and $\mathfrak{p}$ a prime of F, we let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$. If F is a local field, let $U_F^{(n)} = 1 + \pi^n \mathcal{O}_F$ where π is a uniformizer of F. A (homogeneous) Diophantine equation is *solvable* if it has (non-zero) integer solutions. An integer solution of a Diophantine equation is called *primitive* if the greatest common divisor of the components is 1.

2.1 Local computations

We first give several results about properties of extensions of the local field $\mathbb{Q}_2$. The proofs of these results are routine, which we omit here.

Lemma 2.1 *([1], Lemma 2.4) Suppose $F = \mathbb{Q}_2(\sqrt{-3})$ and $\omega = (-1+\sqrt{-3})/2 \in F$. Then*

(1) $U_F/U_F^2 = (\overline{3}) \times (\overline{1+2\omega}) \times (\overline{1+4\omega})$.
(2) The extension $F(\sqrt{3}, \sqrt{1+2\omega})/F$ is totally ramified, and $F(\sqrt{1+4\omega})/F$ is unramified.
(3) For $a \in U_F$, if $a \equiv 1$ or $3 \mod 4$, then $F(\sqrt{3}, \sqrt{a})/F(\sqrt{3})$ is an unramified extension; if $a \equiv 1 + 2\omega$ or $1 + 2\omega^2 \mod 4$, then $F(\sqrt{3}, \sqrt{a})/F(\sqrt{3})$ is a ramified extension.
(4) If $a \in U_F$ and $a \equiv x$ or $\omega \cdot x$ or $\omega^2 \cdot x \bmod 4$ for some odd integer x, then $F(\sqrt{a})/F$ is unramified if and only if $x \equiv 1 \bmod 4$.

Lemma 2.2 *Suppose $F = \mathbb{Q}_2(\sqrt{-1})$. Then $\pi = -1 + \sqrt{-1}$ is a uniformizer of F and*

(1) $U_F^{(5)} = \left(U_F^{(3)}\right)^2$.
(2) $F(\sqrt{3}) = F(\sqrt{-3})$ is unramified over F.

Lemma 2.3 *Suppose $F = \mathbb{Q}_2(\sqrt{3})$. Then $-1 + \sqrt{3}$ is a uniformizer of F and*

(1) $U^{(5)} = \left(U^{(3)}\right)^2$.
(2) $F(\sqrt{-1}) = F(\sqrt{-3})$ is unramified over F.

Lemma 2.4 *Suppose $F = \mathbb{Q}_2(\sqrt{2n})$ where n is an odd integer. Then $\pi = \sqrt{2n}$ is a uniformizer of F and*

(1) $U_F^{(5)} = \left(U_F^{(3)}\right)^2$ *and* $U_F^2 = U_F^{(5)} \bigcup (1 + \pi^2 + \pi^3) U_F^{(5)}$.
(2) $F(\sqrt{1 + \pi^2 + \pi^3 + \pi^4}) = F(\sqrt{1 + \pi^4}) = F(\sqrt{5})$ is unramified over F.

Lemma 2.5 *Suppose that $p \equiv 3 \bmod 4$ is a prime, then*

(1) If $p \equiv 3 \bmod 8$, then in the field $\mathbb{Q}_2(\sqrt{3})$, $\sqrt{p} \equiv \sqrt{3} \bmod \pi^4$, where $\pi = -1+\sqrt{3}$.
(2) If $p \equiv 7 \bmod 8$, then in the field $\mathbb{Q}_2(\sqrt{-1})$, $\sqrt{p} \equiv \sqrt{-1} \bmod \pi^4$, where $\pi = -1 + \sqrt{-1}$.

2.2 Fundamental units of real quadratic fields

We need the following proposition about fundamental units of real quadratic fields, for the proof see [4, p. 91] and [9, Theorem 1.1].

Proposition 2.6 *Suppose $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field with odd class number. Let $\epsilon_d = x + y\sqrt{d} > 1$ be the fundamental integral unit of K. We have*

(1) *If* $d = p$ *with* $p \equiv 3 \bmod 4$*, then* $\epsilon_p = 2u_p^2$ *with* $u_p \in K$*, and* $x \equiv 0 \bmod 2$*. More precisely, if* $p \equiv 3 \bmod 8$*, then* $x \equiv 2 \bmod 4$*; if* $p \equiv 7 \bmod 8$*, then* $x \equiv 0 \bmod 4$*.*
(2) *If* $d = 2p$ *with* $p \equiv 3 \bmod 4$*, then* $\epsilon_{2p} = 2u_{2p}^2$ *with* $u_{2p} \in K$*,* $y \equiv 0 \bmod 2$ *and* $x + y \equiv 3 \bmod 4$*.*
(3) *If* $d = p_1p_2$ *with* $p_1 \equiv p_2 \equiv 3 \bmod 4$*, then* $\epsilon_{p_1p_2} = p_1u_{p_1p_2}^2$ *with* $u_{p_1p_2} \in K$*,* $x \equiv 3 \bmod 4$ *and* $y \equiv 0 \bmod 4$*.*

2.3 Solutions of quadratic Diophantine equations

Lemma 2.7 *Suppose that* $p_1 \equiv p_2 \equiv 7$ *are odd primes, then there exists a primitive positive integer solution* (x_0, y_0, z_0) *of* $2z^2 = x^2 - p_1p_2y^2$ *such that* $(x_0, z_0) \equiv (1, 0) \bmod 4$*.*

Proof The solvability follows by checking the corresponding Hilbert symbols. Let $\epsilon_{p_1p_2} = u + v\sqrt{p_1p_2} > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{p_1p_2})$. Then according to Proposition 2.6 (3), $u \equiv 3 \bmod 4$, $v \equiv 0 \bmod 4$. First, we show that $-p_i = x^2 - 2z^2$ $(i = 1, 2)$ has a primitive positive solution (x_i, z_i) such that $4 \mid z_i$. Any integral solution is clearly primitive, and moreover, x_i is odd and z_i even. Replacing (x_i, z_i) by $(3x_i + 4z_i, 2x_i + 3z_i)$ if necessary, we can get z_i such that $4 \mid z_i$. Then $(x_0, 1, z_0) = (x_1x_2 + 2z_1z_2, 1, x_1z_2 + x_2z_1)$ is a primitive solution of $p_1p_2y^2 = x^2 - 2z^2$ with $4 \mid z_0$. If $x_0 \equiv 1 \bmod 4$, there is nothing left to prove, if $x_0 \equiv 3 \bmod 4$, then $(x_0u + p_1p_2v, x_0v + u, z_0)$ is a primitive positive solution such that $x_0u + p_1p_2v \equiv 1 \bmod 4$. □

Remark 2.8 In the above proof, we used twice the following trick: if F is a quadratic field, and ϵ is a unit of norm 1, then $N_{F/\mathbb{Q}}(\eta) = N$ implies that $N_{F/\mathbb{Q}}(\epsilon\eta) = N$. The first time $F = \mathbb{Q}(\sqrt{2})$, $\epsilon = 3 + 2\sqrt{2}$, $\eta = x_i + z_i\sqrt{2}$; and the second $F = \mathbb{Q}(\sqrt{p_1p_2})$, $\epsilon = \epsilon_{p_1p_2}$, and $\eta = x_0 + y_0\sqrt{p_1p_2}$. We shall employ the trick a few times in Lemma 2.9.

Lemma 2.9 *Suppose* p*,* p_1*, and* p_2 *are primes* $\equiv 3 \bmod 4$*, and* N *is a squarefree odd integer.*

(1) *If* $\gcd(N, p) = 1$*, and the equation* $Nz^2 = x^2 - py^2$ *is solvable, then it has a primitive positive integer solution* (x_0, y_0, z_0) *with* $2 \mid y_0$*.*
(2) *If* $\gcd(N, 2p) = 1$ *and* $Nz^2 = x^2 - 2py^2$ *is solvable, then the equation has a primitive positive integer solution* (x_0, y_0, z_0) *with* $x_0 + y_0 \equiv 1 \bmod 4$*.*
(3) *Suppose that* $\gcd(N, p_1p_2) = 1$*, and* $Nz^2 = x^2 - p_1p_2y^2$ *is solvable. Then it has a primitive positive integer solution* (x_0, y_0, z_0) *satisfying either* (i) $2 \nmid z_0$ *and* $x_0 + y_0 \equiv 1 \bmod 4$ *or* (ii) $(x_0, z_0) \equiv (1, 0) \bmod 4$ *if* $p_1p_2 \equiv 1 \bmod 8$ *and* $(3, 2) \bmod 4$ *if* $p_1p_2 \equiv 5 \bmod 8$*.*
(4) *Suppose that* $p_1p_2 \equiv 1 \bmod 8$ *and* $\gcd(N, p_1p_2) = 1$*. If the Diophantine equation* $2Nz^2 = x^2 - p_1p_2y^2$ *is solvable, then it has primitive positive integer solutions* (x_0, y_0, z_0) *and* (x_0', y_0', z_0') *with* $x_0 \equiv 1 \bmod 4$ *and* $x_0' \equiv 3 \bmod 4$*.*

Proof (1) Let $\epsilon_p = u + v\sqrt{p} > 1$ be the fundamental unit of $F = \mathbb{Q}(\sqrt{p})$, then by Proposition 2.6 (1), $2 \mid u$. Let (x_1, y_1, z_1) be a primitive solution of $Nz^2 = x^2 - py^2$. Obviously, $2 \nmid z_1$. Applying the above trick to F, $\epsilon = \epsilon_p$ and

$\eta = x_1 + y_1\sqrt{p}$, we get a solution $(x_0, y_0, z_0 = z_1)$ satisfying $2 \mid y_0$. Since $x_0 + y_0\sqrt{p} = (x_1 + y_1\sqrt{p})\epsilon_p^a$ for $a = 0$ or 1, it is trivial to check that $\gcd(x_0, y_0) = 1$, and the solution is primitive.

(2) Let $\epsilon_{2p} = u + v\sqrt{2p} > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{2p})$, then by Proposition 2.6 (2), $2 \mid v$ and $u + v \equiv 3 \bmod 4$. Let (x_1, y_1, z_1) be a primitive positive solution of $Nz^2 = x^2 - 2py^2$. Now just apply the trick to $F = \mathbb{Q}(\sqrt{2p})$, $\epsilon = \epsilon_{2p}$, and $\eta = x_1 + y_1\sqrt{2p}$, we get the desired solution.

(3) Let $\epsilon_{p_1p_2} = u + v\sqrt{p_1p_2} > 1$ be the fundamental integral unit of $\mathbb{Q}(\sqrt{p_1p_2})$, then by Proposition 2.6 (3), $u \equiv 3 \bmod 4$, $v \equiv 0 \bmod 4$. Let (x_1, y_1, z_1) be a primitive positive solution of $Nz^2 = x^2 - p_1p_2y^2$. Now repeat the trick to the case $F = \mathbb{Q}(\sqrt{p_1p_2})$, $\epsilon = \epsilon_{p_1p_2}$, and $\eta = x_1 + y_1\sqrt{p_1p_2}$.

(4) A primitive solution (x_0, y_0, z_0) and its associated solution (x_1, y_1, z_0) obtained by $x_1 + y_1\sqrt{p_1p_2} = (x_0 + y_0\sqrt{p_1p_2})\epsilon_{p_1p_2}$ for $\epsilon_{p_1p_2}$ as given in (3) must satisfy the condition that one of x_0 and $x_1 \equiv 1 \bmod 4$ and the other $\equiv 3 \bmod 4$.

□

2.4 Decomposition and congruence

Lemma 2.10 *Suppose p_1 and p_2 are distinct primes $\equiv 3 \bmod 4$. Let $F = \mathbb{Q}(\sqrt{p_1p_2})$. Assume $N \equiv 1 \bmod 4$ is a squarefree integer such that $\gcd(N, p_1p_2) = 1$, and the equation $Nz^2 = x^2 - p_1p_2y^2$ has a primitive solution (x_0, y_0, z_0). Take $\alpha = x_0 + \sqrt{p_1p_2}y_0$ if $2 \nmid z_0$ and $\alpha = \frac{x_0+\sqrt{p_1p_2}y_0}{2}$ if $2 \mid z_0$. Let $\overline{\alpha}$ be the conjugate of α in F. Then*

(1) The element $\alpha \in \mathcal{O}_F$, and the ideal $\alpha\mathcal{O}_F$ is relatively prime to $\overline{\alpha}\mathcal{O}_F$.
(2) If $2 \nmid z_0$, then $\alpha \equiv x_0 + y_0 \bmod 4\mathcal{O}_F$.
(3) If $p_1p_2 \equiv 5 \bmod 8$ and $2 \mid z_0$, then in the local field $\mathbb{Q}_2(\sqrt{p_1p_2}) = \mathbb{Q}_2(\sqrt{-3})$, $\alpha \equiv \omega(-x_0)$ or $\omega^2(-x_0) \bmod 4$, where $\omega = \frac{-1+\sqrt{-3}}{2}$.
(4) If $p_1p_2 \equiv 1 \bmod 8$ and $2 \mid z_0$, then $\mathfrak{d}_1 = (2, \alpha) \neq \mathfrak{d}_2 = (2, \overline{\alpha})$ are the two dyadic primes of F, and $\alpha \equiv x_0 \bmod \mathfrak{d}_2^2$ and $\alpha/2^e \equiv x_0 \bmod \mathfrak{d}_1^2\mathcal{O}_{F_{\mathfrak{d}_1}}$ for an even integer e.

Proof The proof of (2)–(4) is similar to that of [1, Lemma 2.6]. Now we prove (1). One can check that $\alpha\overline{\alpha}$ and $\alpha + \overline{\alpha} \in \mathbb{Z}$, so $\alpha \in \mathcal{O}_F$. Assume $\mathfrak{p}$ is a prime of $\mathcal{O}_F$ such that $\mathfrak{p}$ divides both $\alpha\mathcal{O}_F$ and $\overline{\alpha}\mathcal{O}_F$, then $\alpha, \overline{\alpha} \in \mathfrak{p}$, and $\alpha + \overline{\alpha} \in \mathfrak{p}$. If $\mathfrak{p}$ is an odd prime, we have x_0 or $2x_0 = \alpha + \overline{\alpha} \in \mathfrak{p} \cap \mathbb{Z} = (\ell)$, then $\ell \mid x_0$ and $\ell \mid Nz_0^2$. If $\ell \mid p_1p_2$, i.e., if $\ell = p_1$ or p_2, then $\ell \mid z_0$, because $\gcd(N, p_1p_2) = 1$, thus $\ell^2 \mid x_0^2 - Nz_0^2 = p_1p_2y_0^2$, now $\ell \mid y_0$, which contradicts that (x_0, y_0, z_0) is primitive. If $\ell \mid N$, then $\ell \mid y_0$, hence $\ell^2 \mid Nz_0^2 = x_0^2 - p_1p_2y_0^2$, therefore $\ell \mid z_0$, which is also a contradiction. If $\ell \mid z_0$, then $\ell \mid y_0$, which is impossible. $\overline{\alpha}\mathcal{O}_F$ and N is squarefree, $\ell \mid z_0$ and we must have $\ell \mid y_0$, which is impossible. If $\mathfrak{p}$ is a dyadic prime, then $2 \mid z_0$ and $x_0 = \alpha + \overline{\alpha} \in \mathfrak{p} \cap \mathbb{Z} = (2)$, i.e., $2 \mid x_0$, hence $2 \mid y_0$, which is also impossible. □

Lemma 2.11 *Suppose p_1 and p_2 are distinct primes $\equiv 3 \bmod 4$ satisfying $p_1p_2 \equiv 1 \bmod 8$. Let $F = \mathbb{Q}(\sqrt{p_1p_2})$. Suppose N is a squarefree integer such that $2Nz^2 = x^2 - p_1p_2y^2$ has a primitive solution (x_0, y_0, z_0). Let $\alpha = \frac{x_0+y_0\sqrt{p_1p_2}}{2}$ and $\overline{\alpha}$ be its conjugate. Then $\mathfrak{d}_1 = (2, \alpha)$ and $\mathfrak{d}_2 = (2, \overline{\alpha})$ are the two dyadic ideals of F. Moreover,*

(1) *For* $N \equiv 1 \bmod 4$, *if* $2 \| z_0$, *then* $\alpha \equiv x_0 + 2 \bmod \mathfrak{d}_2^2$ *and* $\alpha/2 \equiv x_0 + 2 \bmod \mathfrak{d}_1^2 \mathcal{O}_{F_{\mathfrak{d}_1}}$; *if* $4 \mid z_0$, *then* $\alpha \equiv x_0 \bmod \mathfrak{d}_2^3$ *and* $\alpha/2^e \equiv x_0$ *or* $5x_0 \bmod \mathfrak{d}_1^3 \mathcal{O}_{F_{\mathfrak{d}_1}}$ *for an odd integer* e.

(2) *For* $N \equiv 3 \bmod 4$, *if* $2 \| z_0$, *then* $\alpha \equiv x_0 + 2 \bmod \mathfrak{d}_2^2$ *and* $\alpha/2 \equiv -(x_0 + 2) \bmod \mathfrak{d}_1^2 \mathcal{O}_{F_{\mathfrak{d}_1}}$; *if* $4 \mid z_0$, *then* $\alpha \equiv x_0 \bmod \mathfrak{d}_2^3$ *and* $\alpha/2^e \equiv -x_0$ *or* $3x_0 \bmod \mathfrak{d}_1^3 \mathcal{O}_{F_{\mathfrak{d}_1}}$ *for an odd integer* e.

Proof We prove the case $N \equiv 1 \bmod 4$, the other case is similar.

We have $\alpha\overline{\alpha} = \dfrac{2Nz_0^2}{4} \equiv 0 \bmod 2$ and $\alpha + \overline{\alpha} = x_0 \in \mathbb{Z}$, hence $\alpha \in \mathcal{O}_F$. By the same technique of Lemma 2.10 (1), we can show that $\alpha\mathcal{O}_F$ is relatively prime to $\overline{\alpha}\mathcal{O}_F$. Moreover, by the fact that $\alpha\overline{\alpha} \in 2\mathbb{Z}$, we know $\mathfrak{d}_1 = (2, \alpha)$ and $\mathfrak{d}_2 = (2, \overline{\alpha})$ are the two dyadic ideals of F. If $2 \| z_0$, then $\alpha \in \mathfrak{d}_1$ and $\overline{\alpha} \in \mathfrak{d}_2$. Thus $\alpha = x_0 - \overline{\alpha} \equiv x_0 \bmod \mathfrak{d}_2 \equiv x_0 + 2 \bmod \mathfrak{d}_2^2$ and $\overline{\alpha} \equiv x_0 + 2 \bmod \mathfrak{d}_1^2$. Then $\alpha \cdot \overline{\alpha} \cdot 2^{-1} = \dfrac{Nz_0^2}{2^2} \equiv 1 \bmod \mathfrak{d}_1^2 \mathcal{O}_{F_{\mathfrak{d}_1}}$ and $\dfrac{\alpha}{2} \equiv \overline{\alpha}^{-1} \equiv x_0 + 2 \bmod \mathfrak{d}_1^2 \mathcal{O}_{F_{\mathfrak{d}_1}}$.

If $4 \mid z_0$, then $\alpha\overline{\alpha} \in 8\mathbb{Z}$, thus $\alpha \in \mathfrak{d}_1^3$, $\overline{\alpha} \in \mathfrak{d}_2^3$. Then $\alpha = x_0 - \overline{\alpha} \equiv x_0 \bmod \mathfrak{d}_2^3$ and $\overline{\alpha} \equiv x_0 \bmod \mathfrak{d}_1^3$. If $2^k \| z_0$, $k \geq 2$, then by $\alpha \cdot \overline{\alpha} \cdot 2^{-2(k-1)-1} = \dfrac{Nz_0^2}{2^{2k}} \equiv 1$ or $5 \bmod \mathfrak{d}_1^3 \mathcal{O}_{F_{\mathfrak{d}_1}}$ (because $N \equiv 1$ or $5 \bmod 8$),

$$\frac{\alpha}{2^{2(k-1)+1}} \equiv \overline{\alpha}^{-1} \equiv x_0 \text{ or } 5x_0 \bmod \mathfrak{d}_1^3 \mathcal{O}_{F_{\mathfrak{d}_1}}.$$

□

Lemma 2.12 *Suppose* $p_1 \equiv p_2 \equiv 7 \bmod 8$ *are distinct primes and* $F = \mathbb{Q}(\sqrt{p_1 p_2})$. *Suppose* (x_0, y_0, z_0) *is a solution of* $2z^2 = x^2 - p_1 p_2 y^2$ *as given in Lemma 2.7. Let* $\alpha = \frac{x_0 + \sqrt{p_1 p_2} y_0}{2}$ *and* $\overline{\alpha} = \frac{x_0 - \sqrt{p_1 p_2} y_0}{2}$ *be its conjugate in* F. *Then* $\mathfrak{d}_1 = (2, \alpha)$ *and* $\mathfrak{d}_2 = (2, \overline{\alpha})$ *are the two dyadic primes of* F *and* $\alpha \equiv x_0 \bmod \mathfrak{d}_2^3$ *and* $\alpha/2^e \equiv x_0 \bmod \mathfrak{d}_1^3 \mathcal{O}_{F_{\mathfrak{d}_1}}$ *for an odd integer* e.

Proof The proof is similar to that of Lemma 2.11. □

3 The case $\delta = p$ with prime $p \equiv 3 \bmod 4$

In this section, we assume prime $p \equiv 3 \bmod 4$, $K_0 = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ such that $\gcd(d, p) = 1$. Let $\epsilon_p > 1$ be the fundamental unit of K_0. Note that by Proposition 2.6, $\epsilon_p = 2u_p^2$ for $u_p \in K_0$. Let

$$Q = \{q_1, q_2, \cdots, q_n\} = \text{the set of odd prime divisors of } d, \tag{3}$$

and inside Q, the subsets

$$Q_+ = \left\{q_1, \cdots, q_m \mid q_j \text{ satisfies } \left(\frac{p}{q_j}\right) = 1\right\} \tag{4}$$

$$Q_- = \left\{ q_{m+1}, \cdots, q_n \mid q_j \text{ satisfies } \left(\frac{p}{q_j}\right) = -1 \right\}. \quad (5)$$

We set

$$r_2(Q_+) = \text{the 2-rank of the subgroup of } \mu_2^2 \text{ generated by } \sigma(q) = \left(\left(\frac{-1}{q}\right), \left(\frac{2}{q}\right)\right) \text{ for } q \in Q_+, \quad (6)$$

and if $Q_+ = \emptyset$, we set $r_2(Q_+) = 0$. We denote by the above subgroup $\overline{Q}_+$. If $r_2(Q_+) = 1$, choose $q_1 \in Q_+$ such that $\sigma(q_1)$ is a generator of $\overline{Q}_+$. If $r_2(Q_+) = 2$, choose $q_1, q_2 \in Q_+$ such that $\langle \sigma(q_1), \sigma(q_2) \rangle = \mu_2^2$.

Lemma 3.1 *Suppose conventions on d as above. Then* $s = m + n$ *if* $d \equiv 1$ *or* $3 \bmod 4$ *and* $m + n + 1$ *if* $d \equiv 2 \bmod 4$, *and* $t = r_2(Q_+)$.

Remark 3.2 By Proposition 1.1, we hence know $r_2(\Delta/K^{*2}) = s - 1 - r_2(Q_+)$.

Proof If $q \in Q_+$, then q splits in K_0, if $q \in Q_-$, then q is inert in K_0. All these primes are ramified in K/K_0. If $d \equiv 2 \bmod 4$, 2 is ramified in K_0, and the dyadic prime in K_0 is ramified in K. The above primes are the only primes ramified in K/K_0. We thus get the values of s.

We know that $U_{K_0} = \{\pm 1\} \times \epsilon_p^{\mathbb{Z}}$. Thus

- $t = 0$ if and only if $-1, \pm\epsilon_p \in NK$;
- $t = 1$ if and only if $U_{K_0} \cap NK = \langle 1, -1 \rangle$ or $\langle 1, \epsilon_p \rangle$ or $\langle 1, -\epsilon_p \rangle$;
- $t = 2$ if and only if $-1, \pm\epsilon_p \notin NK$.

To check -1 or $\pm\epsilon_p \in N_{K/K_0}K$, one just needs to check if $(-1, d)_{\mathfrak{p}} = 1$ or $(\pm\epsilon_p, d)_{\mathfrak{p}} = 1$ for every prime $\mathfrak{p}$ of K_0 ramified in K.

For every prime $\mathfrak{q}$ above $q \in Q_+$, we have

$$(-1, d)_{\mathfrak{q}} = (-1)^{\frac{N\mathfrak{q}-1}{2}} = (-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right).$$

For $q \in Q_-$, let $\mathfrak{q}$ be the prime above q. By Lemma 3.3 of [7], we have

$$(-1, d)_{\mathfrak{q}} = (N_{K_0/\mathbb{Q}}(-1), d)_q = (1, d)_q = 1.$$

By $\epsilon_p = 2u_p^2$, for every prime $\mathfrak{q}$ above $q \in Q_+$, we have

$$(\epsilon_p, d)_{\mathfrak{q}} = (2, d)_{\mathfrak{q}} = \left(\frac{2}{q}\right) \quad \text{and} \quad (-\epsilon_p, d)_{\mathfrak{q}} = (-2, d)_{\mathfrak{q}} = \left(\frac{-2}{q}\right).$$

For the prime $\mathfrak{q}$ above $q \in Q_-$, we have

$$(\pm\epsilon_p, d)_{\mathfrak{q}} = (N_{K_0/\mathbb{Q}}(\pm 2), d)_q = (2^2, d)_q = 1.$$

Let $\mathfrak{d}$ be the dyadic prime of K_0 above 2, the product formula gives

$$(-1, d)_{\mathfrak{d}} = (\epsilon_p, d)_{\mathfrak{d}} = (-\epsilon_p, d)_{\mathfrak{d}} = 1.$$

Hence

- $t = 0$ if and only if $q \equiv 1 \bmod 8$ for all $q \in Q_+$, i.e., $r_2(Q_+) = 0$.
- $t = 1$ if and only if $\overline{Q}_+ = \langle(-1, 1)\rangle$ or $\langle(1, -1)\rangle$ or $\langle(-1, -1)\rangle$, i.e., $r_2(Q_+) = 1$.
- $t = 2$ if and only if $\overline{Q}_+ = \{\pm 1\} \times \{\pm 1\}$, i.e., $r_2(Q_+) = 2$.

□

Suppose $Q_+ \neq \emptyset$. For any j such that $r_2(Q_+) + 1 \leq j \leq m$, $\widetilde{q}_j$ is chosen as follows:

- If $r_2(Q_+) = 0$, then for all $1 \leq j \leq m$, let $\widetilde{q}_j = q_j$.
- If $r_2(Q_+) = 1$, then $\sigma(q_j) = \sigma(q_1)^a$ for $a \in \{0, 1\}$. Let $\widetilde{q}_j = q_1^a q_j$ for $2 \leq j \leq m$.
- If $r_2(Q_+) = 2$, then $\sigma(q_j) = \sigma(q_1)^a \sigma(q_2)^b$ with $a, b \in \{0, 1\}$. Let $\widetilde{q}_j = q_1^a q_2^b q_j$ for $3 \leq j \leq m$.

By construction, $\widetilde{q}_j$ is uniquely determined by the condition that the Jacobi symbols

$$\left(\frac{-1}{\widetilde{q}_j}\right) = \left(\frac{2}{\widetilde{q}_j}\right) = 1, \text{ i.e., } \widetilde{q}_j \equiv 1 \bmod 8.$$

Lemma 3.3 *The equation $\widetilde{q}_j z^2 = x^2 - py^2$ is solvable in $\mathbb{Z}$ and has a primitive positive integer solution (x_j, y_j, z_j) such that $2 \mid y_j$.*

Proof The solvability follows by checking the corresponding Hilbert symbols. Then by Lemma 2.9 (1), it has a primitive positive integer solution (x_j, y_j, z_j) such that $2 \mid y_j$. □

Let (x_j, y_j, z_j) be such a solution given in the above Lemma. Then set

$$\alpha_j = x_j + \sqrt{p} y_j. \tag{7}$$

Lemma 3.4 *The elements $q_j \in Q$ (i.e., $1 \leq j \leq n$) and α_j ($r_2(Q_+) + 1 \leq j \leq m$) defined above all belong to D_K^+. If $d \equiv 2 \bmod 4$, $2 \in D_K^+$.*

Proof Since q_j is ramified in K, we see that $q_j \in D_K^+$ for $1 \leq j \leq n$.

For α_j, we know that $\alpha_j \overline{\alpha}_j = q_j z_j^2, q_1 q_j z_j^2, q_2 q_j z_j^2$, or $q_1 q_2 q_j z_j^2$; thus, α_j is totally positive. Since (x_j, y_j, z_j) is a primitive solution, $\alpha_j \mathcal{O}_{K_0}$ is prime to $\overline{\alpha}_j \mathcal{O}_{K_0}$, hence $\alpha_j \mathcal{O}_K$ is relatively prime to $\overline{\alpha}_j \mathcal{O}_K$. Since q_1, q_2, and q_j are ramified in K, we see that $\alpha_j \overline{\alpha}_j \mathcal{O}_K$ is a square of an ideal in $\mathcal{O}_K$, thus $\alpha \in D_K^+$. If $d \equiv 2 \bmod 4$, 2 is ramified in K, thus $2 \in D_K^+$. □

We can now state and prove the main result of this section.

Theorem 3.5 *Assume p and d as above. Then the Hilbert genus field E of $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ is $\mathbb{Q}(\sqrt{p}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$ if $d \equiv 1$ or $3 \bmod 4$ and $\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_{r+1}}, \cdots, \sqrt{\alpha_m})$ if $d \equiv 2 \bmod 4$, where $r = r_2(Q_+)$ is given by (6), α_j is given by (7), and there is no $\sqrt{\alpha_j}$-term in E if $m = r$.*

Proof We note the fact that $K(\sqrt{q_i})/K$ is always unramified.

We first show the case $r_2(Q_+) = 0$ and $d \equiv 1, 3 \bmod 4$ in detail. By Lemma 3.1, we have $r_2(\Delta/K^{*2}) = m + n - 1$. We now show that Δ/K^{*2} is generated by $\{q_1, \ldots, q_{n-1}, \alpha_1, \ldots, \alpha_m\}$. Firstly, we show the set

$$\{q_1, \ldots, q_{n-1}, \alpha_1, \ldots, \alpha_m\} \tag{8}$$

is independent modulo K^{*2}.

Consider $\xi = \prod_i q_i^{a_i} \prod_j \alpha_j^{b_j}$, where $a_i, b_j \in \{0, 1\}$, $q_i \in \{q_1, \ldots, q_{n-1}\}$, $\alpha_j \in \{\alpha_1, \ldots, \alpha_m\}$. Let $K_2 = \mathbb{Q}(\sqrt{pd})$, then

$$N_{K/K_2}(\xi) = \prod_i q_i^{2a_i} \prod_j q_j^{b_j} \cdot \lambda^2, \qquad \lambda \in K_2.$$

Suppose $\xi \in K^{*2}$, then $N_{K/K_2}(\xi) \in K_2^{*2}$, thus $b_j = 0$. Now $\xi = \prod_i q_i^{a_i} \in K^{*2}$, since K has only three quadratic subfields: $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{pd})$, we must have $a_i = 0$. Therefore, the set (8) is independent modulo K^{*2}.

Second, we show that $K(\sqrt{\alpha_j})/K$, $1 \le j \le m$, are unramified extensions. By Proposition 1.1 (1), we only need to show they are unramified at the dyadic primes of K.

Let $\mathfrak{D}$ be a dyadic prime of K and let $\mathfrak{d} = \mathfrak{D} \cap \mathcal{O}_{K_0}$. If $p \equiv 3 \bmod 8$, then $K_{0,\mathfrak{d}} \simeq \mathbb{Q}_2(\sqrt{3})$. Since $\widetilde{q}_j \equiv 1 \bmod 8$, $y_j \equiv 0 \bmod 4$. By the Lemma 2.5 (1), we have

$$\alpha_j = x_j + y_j\sqrt{p} = x_j + y_j + (-1 + \sqrt{p})y_j \equiv x_j + y_j + (-1 + \sqrt{3})y_j \bmod \pi^5,$$

where $\pi = -1 + \sqrt{3}$ is a uniformizer of $\mathbb{Q}_2(\sqrt{3})$. Since $4 \mid y_j$, $\alpha_j \equiv x_j + y_j \bmod \pi^5$. According to Lemma 2.3 (1), $K_{0,\mathfrak{d}}(\sqrt{\alpha_j}) = K_{0,\mathfrak{d}}(\sqrt{x_j + y_j})$. Because $x_j + y_j \equiv \pm 1, \pm 3 \bmod 8$, due to Lemma 2.3 (2), $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified, thus $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is also unramified.

If $p \equiv 7 \bmod 8$, then $K_{0,\mathfrak{d}} \simeq \mathbb{Q}_2(\sqrt{-1})$. Since $\widetilde{q}_j \equiv 1 \bmod 8$, $y_j \equiv 0 \bmod 4$. By the Lemma 2.5 (2), we have

$$\alpha_j = x_j + y_j\sqrt{p} = x_j + y_j + (-1 + \sqrt{p})y_j \equiv x_j + y_j + (-1 + \sqrt{-1})y_j \bmod \pi^5,$$

where $\pi = -1 + \sqrt{-1}$ is a uniformizer of $\mathbb{Q}_2(\sqrt{-1})$. Since $4 \mid y_j$, $\alpha_j \equiv x_j + y_j \bmod \pi^5$. Since $x_j + y_j \equiv \pm 1, \pm 3 \bmod 8$, by Lemma 2.2, $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified, thus $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is also unramified.

For $d \equiv 1, 3 \bmod 4$ and $r = 1$ or 2, the proof is similar to the above situation. We first show that $\left\{q_1, \cdots, q_{n-1}, \alpha_{r_2(Q_+)+1}, \cdots, \alpha_m\right\}$ is a $\mathbb{Z}/2\mathbb{Z}$-basis of Δ/K^{*2}, then use the fact that the construction of α_j $(j > r_2(Q_+))$ implies that $K(\sqrt{\alpha_j})/K$ is unramified.

For $d \equiv 2 \bmod 4$, the proof also follows from the same strategy. We note in this case $K(\sqrt{2})/K$ is an unramified extension. □

4 The case $\delta = 2p$ with prime $p \equiv 3 \bmod 4$

In this section, we assume $p \equiv 3 \bmod 4$ a prime, $d > 0$ squarefree and $\gcd(d, p) = 1$, $K_0 = \mathbb{Q}(\sqrt{2p})$, and $K = \mathbb{Q}(\sqrt{2p}, \sqrt{d})$. Let $\epsilon_{2p} > 1$ be the fundamental unit of K_0. Then $\epsilon_{2p} = 2u_{2p}^2$ where $u_{2p} \in K_0$ by Proposition 2.6. Similar to Sect. 3, set

$$Q = \{q_1, q_2, \cdots, q_n\} = \text{the set of odd prime divisors of } d, \tag{9}$$

and inside Q, the subsets

$$Q_+ = \left\{q_1, \cdots, q_m \mid q_j \text{ satisfies } \left(\frac{2p}{q_j}\right) = 1\right\}, \tag{10}$$

$$Q_- = \left\{q_{m+1}, \cdots, q_n \mid q_j \text{ satisfies } \left(\frac{2p}{q_j}\right) = -1\right\}. \tag{11}$$

We denote by $\overline{Q}_+$ the subgroup of μ_2^2 generated by $\sigma(q) = \left(\left(\frac{-1}{q}\right), \left(\frac{2}{q}\right)\right)$ for $q \in Q_+$ and set

$$r_2(Q_+) = \text{the 2-rank of } \overline{Q}_+, \tag{12}$$

and if $Q_+ = \emptyset$, we set $r_2(Q_+) = 0$. If $r_2(Q_+) = 1$, choose $q_1 \in Q_+$ such that $\sigma(q_1)$ is a generator of $\overline{Q}_+$. If $r_2(Q_+) = 2$, choose $q_1, q_2 \in Q_+$ such that $\langle\sigma(q_1), \sigma(q_2)\rangle = \mu_2^2$.

Lemma 4.1 *Suppose conventions on d as above. Then $s = m + n$ if $d \equiv 1 \bmod 4$ or $6 \bmod 8$ and $m + n + 1$ if $d \equiv 3 \bmod 4$ or $2 \bmod 8$, and $t = r_2(Q_+)$.*

Proof The proof is similar to that of Lemma 3.1. □

Suppose $Q_+ \neq \emptyset$. For any j such that $r_2(Q_+) + 1 \leq j \leq m$, we again get a unique $\widetilde{q}_j = q_1^a q_2^b q_j$ for $a, b \in \{0, 1\}$ satisfying

$$\left(\frac{-1}{\widetilde{q}_j}\right) = \left(\frac{2}{\widetilde{q}_j}\right) = 1, \text{ i.e., } \widetilde{q}_j \equiv 1 \bmod 8..$$

By checking the Hilbert symbol and then Lemma 2.9 (2), we have

Lemma 4.2 *The equation $\widetilde{q}_j z^2 = x^2 - 2py^2$ is solvable in $\mathbb{Z}$ and has a primitive positive integer solution (x_j, y_j, z_j) such that $x_j + y_j \equiv 1 \bmod 4$.*

Let (x_j, y_j, z_j) be such a solution of $\widetilde{q}_j z^2 = x^2 - 2py^2$. Set

$$\alpha_j = x_j + \sqrt{2p}y_j. \tag{13}$$

Lemma 4.3 *The elements q_j $(1 \le j \le n)$ and α_j $(r_2(Q_+)+1 \le j \le m)$ defined above all belong to D_K^+. And if $d \equiv 2 \bmod 4$, $2 \in D_K^+$.*

Proof The proof is similar to that of Lemma 3.4. □

We can now state and prove the main result of this section.

Theorem 4.4 *Assume p and d as above, then the Hilbert genus field E of $K = \mathbb{Q}(\sqrt{2p}, \sqrt{d})$ is $\mathbb{Q}(\sqrt{2p}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$ if $d \equiv 1 \bmod 4$ or $6 \bmod 8$, and $\mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{q_1}, \cdots, \sqrt{q_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$ if $d \equiv 3 \bmod 4$ or $2 \bmod 8$, where $r = r_2(Q_+)$ is given by (12), α_j is given by (13), $\widehat{q}_j = q_j$ if $q_j \equiv 1 \bmod 4$ and $\widehat{q}_j = 2q_j$ if $q_j \equiv 3 \bmod 4$. If $m = r_2(Q_+)$, there is no $\sqrt{\alpha_j}$-term in E.*

Proof We note the fact that if $d \equiv 1 \bmod 4$ or $6 \bmod 8$, $K(\sqrt{\widehat{q}_i})/K$ is always unramified and if $d \equiv 3 \bmod 4$ or $2 \bmod 8$, $K(\sqrt{q_i})/K$ is always unramified.

We first show the case $d \equiv 1 \bmod 4$ or $6 \bmod 8$ and $r = 0$ in detail. By Lemma 4.1, we have $r_2(\Delta/K^{*2}) = m + n - 1$. By the same technique of the proof of Theorem 3.5, we can show that Δ/K^{*2} is generated by $\{q_1, \ldots, q_{n-1}, \alpha_1, \ldots, \alpha_m\}$.

Second, we show that $K(\sqrt{\alpha_j})/K$, $1 \le j \le m$, are unramified extensions. By Proposition 1.1 (1), we only need to show they are unramified at the dyadic primes of K.

Let $\mathfrak{D}$ be a dyadic prime of K and let $\mathfrak{d} = \mathfrak{D} \cap \mathcal{O}_{K_0}$. Then $K_{0,\mathfrak{d}} \simeq \mathbb{Q}_2(\sqrt{2p})$. Let $\pi = \sqrt{2p}$ be a uniformizer of $K_{0,\mathfrak{d}}$. Since (x_j, y_j, z_j) is a primitive positive solution of $\widetilde{q}_j z^2 = x^2 - 2py^2$ and $\widetilde{q}_j \equiv 1 \bmod 8$, we must have x_j, z_j odd and $2 \mid y_j$. Recall that we choose x_j, y_j such that $x_j + y_j \equiv 1 \bmod 4$.

If $x_j \equiv 1 \bmod 4$, $y_j \equiv 0 \bmod 4$, we have

$$\alpha_j = x_j + y_j\sqrt{2p} \equiv 1, 5 \bmod \pi^5.$$

If $x_j \equiv 3 \bmod 4$, $y_j \equiv 2 \bmod 4$, we have

$$\alpha_j = x_j + y_j\sqrt{2p} \equiv 1 + \pi^2 + \pi^3 \text{ or } 1 + \pi^2 + \pi^3 + \pi^4 \bmod \pi^5.$$

By Lemma 2.4, in both cases, $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified. Therefore, $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is also unramified.

The other cases follow the same strategy as above. If $d \equiv 3 \bmod 4$ or $2 \bmod 8$, we need the fact that $K(\sqrt{2})/K$ is an unramified extension. □

5 The case $\delta = p_1 p_2$ with distinct primes $p_1 \equiv p_2 \equiv 3 \bmod 4$

In this section, we assume p_1 and p_2 are distinct primes $\equiv 3 \bmod 4$, $d > 0$ squarefree and prime to $p_1 p_2$, $K_0 = \mathbb{Q}(\sqrt{p_1 p_2})$ and $K = K_0(\sqrt{d}) = \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{d})$ or $K_0(\sqrt{p_1 d}) = \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{p_1 d})$. Let $\epsilon_{p_1 p_2} > 1$ be the fundamental integral unit of K_0. Then $\epsilon_{p_1 p_2} = p_1 u_{p_1 p_2}^2$ where $u_{p_1 p_2} \in K_0$ by Proposition 2.6. Let

$$Q = \{q_1, q_2, \cdots, q_n\} = \text{the set of odd prime divisors of } d, \tag{14}$$

and inside Q, the subsets

$$Q_+ = \left\{q_1, \cdots, q_m \mid q_j \text{ satisfies } \left(\frac{p_1p_2}{q_j}\right) = 1\right\}, \tag{15}$$

$$Q_- = \left\{q_{m+1}, \cdots, q_n \mid q_j \text{ satisfies } \left(\frac{p_1p_2}{q_j}\right) = -1\right\}. \tag{16}$$

Proposition 5.1 *Suppose that p_1, p_2, d, and K_0 as above.*

(1) *If $K = K_0(\sqrt{d})$, then prime $q \in Q_+$ splits in K_0 and every prime $\mathfrak{q}$ of K_0 above q is ramified in K and*

$$(-1, d)_{\mathfrak{q}} = \left(\frac{-1}{q}\right), \qquad (\epsilon_{p_1p_2}, d)_{\mathfrak{q}} = \left(\frac{p_1}{q}\right).$$

Prime $q \in Q_-$ is inert in K_0, and the prime $\mathfrak{q}$ above q in K_0 is ramified in K and

$$(-1, d)_{\mathfrak{q}} = (\epsilon_{p_1p_2}, d)_{\mathfrak{q}} = 1.$$

If $p_1p_2 \equiv 1 \bmod 8$, then 2 splits in K_0 and for $\mathfrak{d}$ a dyadic prime of K_0, we have

$$(-1, d)_{\mathfrak{d}} = \begin{cases} (-1)^{\frac{d-1}{2}} & \text{if } 2 \nmid d \\ (-1)^{\frac{d/2-1}{2}} & \text{if } 2 \mid d, \end{cases} \quad \text{and} \quad (\epsilon_{p_1p_2}, d)_{\mathfrak{d}} = \begin{cases} (-1)^{\frac{d-1}{2}} & \text{if } 2 \nmid d \\ (-1)^{\frac{p_1^2-1}{8}+\frac{d/2-1}{2}} & \text{if } 2 \mid d. \end{cases}$$

If $p_1p_2 \equiv 5 \bmod 8$, then 2 is inert in K_0, the dyadic prime $\mathfrak{d}$ of K_0 is ramified in K if and only if $d \equiv 2$ or $3 \bmod 4$, and

$$(-1, d)_{\mathfrak{d}} = (\epsilon_{p_1p_2}, d)_{\mathfrak{d}} = 1.$$

(2) *If $K = K_0(\sqrt{p_1d})$, then all the assertions in (1) hold if replacing d by p_1d.*

Proof Similar to the calculation in Lemma 3.1. □

5.1 The case $p_1p_2 \equiv 5 \bmod 8$

This situation is similar to the previous two sections. For $q \in Q_+$, let $\sigma(q) = \left(\left(\frac{-1}{q}\right), \left(\frac{p_1}{q}\right)\right) \in \mu_2^2$ and let $\overline{Q}_+ = \langle \sigma(q) \mid q \in Q_+ \rangle$ be the subgroup of μ_2^2 generated by $\{\sigma(q) \mid q \in Q_+\}$. We set

$$r_2(Q_+) = r_2(\overline{Q}_+) = \text{the 2-rank of } \overline{Q}_+ \tag{17}$$

and $r_2(Q_+) = 0$ if $Q_+ = \emptyset$. If $r_2(Q_+) = 1$, choose $q_1 \in Q_+$ such that $\sigma(q_1)$ is a generator of $\overline{Q}_+$. If $r_2(Q_+) = 2$, choose $q_1, q_2 \in Q_+$ such that $\langle \sigma(q_1), \sigma(q_2) \rangle = \mu_2^2$.

Proposition 5.1 tells us that

Lemma 5.2 *If $K = K_0(\sqrt{d})$, then $s = m+n$ if $d \equiv 1 \bmod 4$ and $m+n+1$ if $d \equiv 2$ or $3 \bmod 4$, and $t = r_2(Q_+)$. If $K = K_0(\sqrt{p_1 d})$, then $s = m+n$ if $p_1 d \equiv 1 \bmod 4$ and $m+n+1$ if $p_1 d \equiv 2$ or $3 \bmod 4$, and $t = r_2(Q_+)$.*

Similar to the previous two sections again, if $Q_+ \neq \emptyset$, for any j such that $r_2(Q_+)+1 \leq j \leq m$, we associate to q_j a unique $\widetilde{q}_j = q_1^a q_2^b q_j$ for $a, b \in \{0, 1\}$ such that the Jacobi symbols

$$\left(\frac{-1}{\widetilde{q}_j}\right) = \left(\frac{p_1}{\widetilde{q}_j}\right) = 1.$$

By checking the corresponding Hilbert symbols and then by Lemma 2.9 (3), we have

Lemma 5.3 *The equation $\widetilde{q}_j z^2 = x^2 - p_1 p_2 y^2$ is solvable in $\mathbb{Z}$ and has a primitive positive integer solution (x_j, y_j, z_j) satisfying either (i) $2 \nmid z_j$ and $x_j + y_j \equiv 1 \bmod 4$ or (ii) $(x_j, z_j) \equiv (3, 2) \bmod 4$.*

For such a solution, we set

$$\alpha_j = x_j + \sqrt{p_1 p_2}\, y_j, \ \text{if } 2 \nmid z_j \quad \text{and} \quad \alpha_j = \frac{x_j + \sqrt{p_1 p_2}\, y_j}{2}, \ \text{if } 2 \mid z_j. \tag{18}$$

By the same method of Lemma 3.4, we can show that $\alpha_j \in D_K^+$ for $K = K_0(\sqrt{d})$ or $K_0(\sqrt{p_1 d})$.

Then we have the following theorem.

Theorem 5.4 *Assume $p_1 p_2 \equiv 5 \bmod 8$ and d as above.*

(1) *The Hilbert genus field E of $K = \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{d})$ is given by the following table.*

d	Hilbert genus field E
$1 \bmod 4$	$\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$
$2 \bmod 8$	$\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{2}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$
$6 \bmod 8$	$\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{2p_1}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$
$3 \bmod 4$	$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$

where

- *$r = r_2(Q_+)$ and if $m = r$, there is no $\sqrt{\alpha_j}$-term in E;*
- *the number $\widehat{q}_j = q_j$ if $q_j \equiv 1 \bmod 4$, $\widehat{q}_j = p_1 q_j$ if $q_j \equiv 3 \bmod 4$ and $d \equiv 1 \bmod 4$ or $2 \bmod 8$, and $\widehat{q}_j = 2q_j$ if $q_j \equiv 3 \bmod 4$ and $d \equiv 6 \bmod 8$.*

(2) *The Hilbert genus field E of $K = \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{p_1 d})$ is obtained by replacing d by $p_1 d$ in* (1).

Proof We prove the case that $K = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{d})$, the proof of the case $K = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{p_1d})$ is similar.

We just need to show that the extension $K(\sqrt{\alpha_j})/K$ is unramified.

By Proposition 1.1, it suffices to show that $K(\sqrt{\alpha_j})/K$ is unramified at every dyadic prime $\mathfrak{D}$ of K. Let $\mathfrak{d} = \mathfrak{D} \cap \mathcal{O}_{K_0}$. Then $K_{0,\mathfrak{d}} \simeq \mathbb{Q}_2(\sqrt{-3})$.

If $2 \nmid z_j$, then by Lemma 2.10 (2), $\alpha_j \equiv x_j + y_j \equiv 1 \bmod 4$ in $K_{0,\mathfrak{d}}$. Thus, by Lemma 2.1 (4), $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified. Hence $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is also unramified.

If $2 \mid z_j$, then by Lemma 2.10 (3), $\alpha_j \equiv \omega(-x_j)$ or $\omega^2(-x_j) \bmod 4$. Since now $x_j \equiv 3 \bmod 4$, by Lemma 2.1 (4), $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified. Thus, $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is also unramified. □

5.2 The case $p_1p_2 \equiv 1 \bmod 8$

This is the most complicated situation. We divide this into four cases:

5.2.1 The cases $d \equiv 1 \bmod 4$ and $(d, p_1) \equiv (2, 7) \bmod 8$ for $K_0(\sqrt{d})$ and $p_1d \equiv 1 \bmod 4$ and $(p_1d, p_1) \equiv (2, 7) \bmod 8$ for $K_0(\sqrt{p_1d})$

We note that $p_1d \equiv 1 \bmod 4$ is nothing but $d \equiv 3 \bmod 4$. The form we adopt here is to illustrate the symmetry between d and p_1d.

As in the previous cases, we can again define $\overline{Q}_+$, the 2-rank $r_2(Q_+)$ of Q_+, and choose q_1 and q_2 according to the value of $r_2(Q_+)$. Proposition 5.1 gives the following lemma:

Lemma 5.5 *If $d \equiv 1 \bmod 4$ (resp. $p_1d \equiv 1 \bmod 4$) for $K = K_0(\sqrt{d})$ (resp. $K = K_0(\sqrt{p_1d})$), then $s = m + n$ and $t = r_2(Q_+)$. If $(d, p_1) \equiv (2, 7) \bmod 8$ (resp. $(p_1d, p_1) \equiv (2, 7) \bmod 8$) for $K = K_0(\sqrt{d})$ (resp. $K = K_0(\sqrt{p_1d})$), then $s = m + n + 2$ and $t = r_2(Q_+)$.*

Suppose $Q_+ \neq \emptyset$. For any j such that $r_2(Q) + 1 \leq j \leq m$, we associate to q_j the unique integer $\widetilde{q}_j = q_1^a q_2^b q_j$ for $a, b \in \{0, 1\}$ such that the Jacobi symbols

$$\left(\frac{-1}{\widetilde{q}_j}\right) = \left(\frac{p_1}{\widetilde{q}_j}\right) = 1.$$

By Lemma 2.9 (3),

Lemma 5.6 *The equation $\widetilde{q}_j z^2 = x^2 - p_1p_2y^2$ is solvable in $\mathbb{Z}$ and has a primitive positive integer solution (x_j, y_j, z_j) satisfying either (i) $2 \nmid z_j$ and $x_j + y_j \equiv 1 \bmod 4$ or (ii) $(x_j, z_j) \equiv (1, 0) \bmod 4$.*

For such a solution, we set

$$\alpha_j = x_j + \sqrt{p_1p_2}y_j, \text{ if } 2 \nmid z_j \quad \text{and} \quad \alpha_j = \frac{x_j + \sqrt{p_1p_2}y_j}{2}, \text{ if } 2 \mid z_j. \tag{19}$$

For $(d, p_1) \equiv (2,7) \bmod 8$ (resp. $(p_1 d, p_1) \equiv (2,7) \bmod 8$), set

$$\alpha_0 = \frac{x_0 + \sqrt{p_1 p_2}\, y_0}{2} \text{ with } (x_0, z_0) \equiv (1,0) \bmod 4 \text{ as given in Lemma 2.7.} \quad (20)$$

By the same method of Lemma 3.4, we can show that $\alpha_j \in D_K^+$ for $K = K_0(\sqrt{d})$ or $K_0(\sqrt{p_1 d})$.

Theorem 5.7 (1) *The Hilbert genus field E of $K = K_0(\sqrt{d})$ is $\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$ if $d \equiv 1 \bmod 4$, and $\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{2}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_0}, \sqrt{\alpha_{r+1}}, \ldots, \sqrt{\alpha_m})$ if $(d, p_1) \equiv (2,7) \bmod 8$, where $r = r_2(Q_+)$ is defined as above, α_j is given by (19), $\widehat{q}_j = q_j$ if $q_j \equiv 1 \bmod 4$ and $p_1 q_j$ if $q_j \equiv 3 \bmod 4$. If $m = r$, the terms $\sqrt{\alpha_j}$ $(j > 0)$ are not appearing in E.*

(2) *The Hilbert genus fields E of $K = K_0(\sqrt{p_1 d})$ for the cases $p_1 d \equiv 1 \bmod 4$ and $(p_1 d, p_1) \equiv (2,7) \bmod 8$ are obtained by replacing d by $p_1 d$ in* (1).

Proof We only show the case that $K = K_0(\sqrt{d})$. The case $K = K_0(\sqrt{p_1 d})$ is similar.

In this case, for $d \equiv 1 \bmod 4$ or $(d, p_1) \equiv (2,7) \bmod 8$, we show that $K(\sqrt{\alpha_j})/K$ $(r_2(Q_+) + 1 \le j \le m)$ is unramified. By Proposition 1.1, it suffices to show that they are unramified at every dyadic prime $\mathfrak{D}$ of K. Let $\mathfrak{D} \cap \mathcal{O}_{K_0} = \mathfrak{d}$.

If $2 \nmid z_j$, then by Lemma 2.10 (2), $\alpha_j \equiv x_j + y_j \equiv 1 \bmod 4$ in $K_{0,\mathfrak{d}} = \mathbb{Q}_2$. Thus, $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified, and therefore, $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is unramified.

If $2 \mid z_j$, then by Lemma 2.10 (4), $K_{0,\mathfrak{d}}(\sqrt{\alpha_j}) \simeq \mathbb{Q}_2(\sqrt{x_j})$ or $\mathbb{Q}_2(\sqrt{x_j + 4})$. Since $x_j \equiv 1 \bmod 4$, $K_{0,\mathfrak{d}}(\sqrt{\alpha_j})/K_{0,\mathfrak{d}}$ is unramified; thus, $K_{\mathfrak{D}}(\sqrt{\alpha_j})/K_{\mathfrak{D}}$ is also unramified.

For $(d, p_1) \equiv (2,7) \bmod 8$, we show that $K(\sqrt{\alpha_0})/K$ is unramified at every dyadic prime of K. Since $p_1 p_2 \equiv 1 \bmod 8$, we see that $K_{\mathfrak{D}} \simeq \mathbb{Q}_2(\sqrt{d})$. By Lemma 2.12,

$$\frac{\alpha_0}{2^e} \equiv x_0 \bmod \mathfrak{d}_1^3 \mathcal{O}_{K_{0,\mathfrak{d}_1}} \quad \text{and} \quad \alpha_0 \equiv x_0 \bmod \mathfrak{d}_2^3,$$

where e is an odd integer. Thus, $K_{\mathfrak{D}_1}(\sqrt{\alpha_0}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{2x_0})$ and $K_{\mathfrak{D}_2}(\sqrt{\alpha_0}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{x_0})$. Since $x_0 \equiv 1 \bmod 4$ and $d \equiv 2 \bmod 8$, $K_{\mathfrak{D}_i}(\sqrt{\alpha_0})/K_{\mathfrak{D}_i}$ $(i = 1, 2)$ is unramified. □

5.2.2 The cases $d \equiv 3 \bmod 4$ for $K_0(\sqrt{d})$ and $p_1 d \equiv 3 \bmod 4$ for $K_0(\sqrt{p_1 d})$

By Proposition 5.1

Lemma 5.8 *If $d \equiv 3 \bmod 4$ for $K = K_0(\sqrt{d})$ and $p_1 d \equiv 3 \bmod 4$ for $K = K_0(\sqrt{p_1 d})$, then $s = m + n + 2$ and*

$$t = \begin{cases} 1, & \text{if for all } q \in Q_+, \left(\frac{-p_1}{q}\right) = 1, \\ 2, & \text{if there exists } q \in Q_+, \left(\frac{-p_1}{q}\right) = -1. \end{cases} \quad (21)$$

If $t=2$, choose $q_1 \in Q_+$ such that $\left(\frac{-p_1}{q_1}\right)=-1$. Suppose $Q_+ \neq \emptyset$. For any j such that $t \le j \le m$, we let $\widetilde{q}_j = q_1^a q_j$ for $a=0$ or 1 uniquely determined by $\left(\frac{-p_1}{\widetilde{q}_j}\right)=1$. By computing the Hilbert symbols associated to the equation $\widetilde{q}_j z^2 = x^2 - p_1p_2y^2$, we see that the equation is solvable in $\mathbb{Z}$. Let (x_j, y_j, z_j) be a relatively prime positive integer solution of $\widetilde{q}_j z^2 = x^2 - p_1p_2y^2$ and set

$$\alpha_j = x_j + \sqrt{p_1p_2}y_j, \text{ if } 2 \nmid z_j \quad \text{and} \quad \alpha_j = \frac{x_j+\sqrt{p_1p_2}y_j}{2}, \text{ if } 2 \mid z_j. \tag{22}$$

By the same method of Lemma 3.4, we can show that $\alpha_j \in D_K^+$.

Theorem 5.9 (1) *Assume* $p_1p_2 \equiv 1 \bmod 8$ *and* $d \equiv 3 \bmod 4$ *as above, then Hilbert genus field* E *of* $K = K_0(\sqrt{d})$ *is* $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_t}, \ldots, \sqrt{\alpha_m})$ *where* t *is given by* (21). *If* $m < t$, *there are no* $\sqrt{\alpha_j}$*-terms in* E.

(2) *Assume* $p_1p_2 \equiv 1 \bmod 8$ *and* $p_1d \equiv 3 \bmod 4$ *as above, then Hilbert genus field* E *of* $K = K_0(\sqrt{p_1d})$ *is* $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_t}, \ldots, \sqrt{\alpha_m})$ *where* t *is given by* (21). *If* $m < t$, *there are no* $\sqrt{\alpha_j}$*-terms in* E.

Proof (1) It suffices to show that $K(\sqrt{\alpha_j})/K$ is unramified at every dyadic prime $\mathfrak{D}$ of K.

Since $p_1p_2 \equiv 1 \bmod 8$, $K_{0,\mathfrak{d}} \simeq \mathbb{Q}_2$ and $K_{\mathfrak{D}} \simeq \mathbb{Q}_2(\sqrt{d})$. If $2 \nmid z_j$, then α_j is a 2-adic unit in $\mathbb{Q}_2$. Since $d \equiv 3 \bmod 4$, $K_{\mathfrak{D}}(\sqrt{\alpha_j})$ is unramified over $K_{\mathfrak{D}}$.

If $2 \mid z_j$, then by the same method of Lemma 2.11, one can show that there exist odd integers u_j, v_j such that $K_{\mathfrak{D}_1}(\sqrt{\alpha_j}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{u_j})$ and $K_{\mathfrak{D}_2}(\sqrt{\alpha_j}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{v_j})$. Since $d \equiv 3 \bmod 4$, $K_{\mathfrak{D}_i}(\sqrt{\alpha_j})/K_{\mathfrak{D}_i}$ $(i=1,2)$ is unramified.

The proof of (2) is similar to that of (1). □

5.2.3 The cases $(d, p_1) \equiv (2,3) \bmod 8$ *for* $K_0(\sqrt{d})$ *and* $(p_1d, p_1) \equiv (2,3) \bmod 8$ *for* $K_0(\sqrt{p_1d})$

By Proposition 5.1

Lemma 5.10 *In these cases* $s = m+n+2$ *and*

$$t = \begin{cases} 1, & \text{if for all } q \in Q_+,\ q \equiv 1 \bmod 4, \\ 2, & \text{if there exists } q \in Q_+,\ q \equiv 3 \bmod 4. \end{cases} \tag{23}$$

If $t=2$, choose $q_1 \in Q_+$ such that $q_1 \equiv 3 \bmod 4$. For $t \le j \le m$, let $\widetilde{q}_j = 2^a q_1^b q_j$ $(a, b \in \{0,1\})$ uniquely determined by the following rules: (i) if $q_j \equiv 1 \bmod 4$, then $b=0$; if $q_j \equiv 3 \bmod 4$, then $b=1$; (iii) the equation $\widetilde{q}_j z^2 = x^2 - p_1p_2y^2$ is solvable. By Lemma 2.9 (3) and (4), we have

Lemma 5.11 *There exists a primitive positive solution* (x_j, y_j, z_j) *for* $\widetilde{q}_j z^2 = x^2 - p_1p_2z^2$ *satisfying*

(1) *If* $\widetilde{q}_j$ *is odd, then either* z_j *odd and* $x_j + y_j \equiv 1 \bmod 4$, *or* z_j *even and* $x_j \equiv 1 \bmod 4$.

(2) *If $\widetilde{q}_j$ is even, then either $2\|z_j$ and $x_j \equiv 3 \bmod 4$, or $4 \mid z_j$ and $x_j \equiv 1 \bmod 4$.*

For such a solution, we set

$$\alpha_j = x_j + \sqrt{p_1p_2}y_j, \text{ if } 2 \nmid z_j \quad \text{and} \quad \alpha_j = \frac{x_j + \sqrt{p_1p_2}y_j}{2}, \text{ if } 2 \mid z_j. \tag{24}$$

By the same method of Lemma 3.4, we can show that $\alpha_j \in D_K^+$.

Theorem 5.12 *(1) Assume $p_1p_2 \equiv 1 \bmod 8$ and $(d, p_1) \equiv (2, 3) \bmod 8$ as above, then the Hilbert genus field E of $K = K_0(\sqrt{d})$ is given by*
(i) If for all $q \in Q_+$, $q \equiv 1 \bmod 4$, then $E = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{2}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$,
(ii) If there exists $q \in Q_+$, $q \equiv 3 \bmod 4$, then $E = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{2}, \sqrt{\widehat{q}_1}, \ldots, \sqrt{\widehat{q}_n}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_m})$,
where $\widehat{q}_j = q_j$ if $q_j \equiv 1 \bmod 4$ and $\widehat{q}_j = p_1q_j$ if $q_j \equiv 3 \bmod 4$. If $m < 1$(resp. 2) in (1)(resp. (2)), then there are no $\sqrt{\alpha_j}$-terms.
(2) Assume $p_1p_2 \equiv 1 \bmod 8$ and $(p_1d, p_1) \equiv (2, 3) \bmod 8$ as above, then the Hilbert genus field E of $K = K_0(\sqrt{p_1d})$ has the same description as (1).

Proof In all cases, it suffices to show that $K(\sqrt{\alpha_j})/K$ is unramified at every dyadic prime $\mathfrak{D}$ of K. The proof is similar to that of Theorem 5.7. For the case $\widetilde{q}_j$ even, one needs Lemma 2.11 (1). □

5.2.4 The cases $d \equiv 6 \bmod 8$ for $K_0(\sqrt{d})$ and $p_1d \equiv 6 \bmod 8$ for $K_0(\sqrt{p_1d})$

In these cases, for $q \in Q_+$, we let $\widehat{q} = q$ if $q \equiv 1 \bmod 4$ and $2q$ if $q \equiv 3 \bmod 4$. By Proposition 5.1

Lemma 5.13 *In these cases we have $s = m + n + 2$ and*

$$t = \begin{cases} 1, & \text{if for all } q \in Q,\ \left(\frac{\widehat{q}}{p_1}\right) = 1, \\ 2, & \text{if there exists } q \in Q,\ \left(\frac{\widehat{q}}{p_1}\right) = -1. \end{cases} \tag{25}$$

If $t = 2$, choose q_1 such that $\left(\frac{\widehat{q}_1}{p_1}\right) = -1$. For any j such that $t \leq j \leq m$, we let $\widetilde{q}_j = 2^a q_1^b q_j$ with $a, b \in \{0, 1\}$ uniquely determined by the following rules: (i) $\widetilde{q}_j \equiv 1 \bmod 4$ or $6 \bmod 8$, (ii) the equation $\widetilde{q}_j z^2 = x^2 - q_1q_2y^2$ is solvable. By Lemma 2.9 (3) and (4), we have

Lemma 5.14 *There exists a primitive positive solution (x_j, y_j, z_j) for $\widetilde{q}_j z^2 = x^2 - p_1p_2z^2$ satisfying*

(1) If $\widetilde{q}_j$ is odd, then either z_j odd and $x_j + y_j \equiv 1 \bmod 4$, or z_j even and $x_j \equiv 1 \bmod 4$.
(2) If $\widetilde{q}_j$ is even, then either $2\|z_j$ and $x_j \equiv 3 \bmod 4$, or $4 \mid z_j$ and $x_j \equiv 1 \bmod 4$.

For such a solution, we set

$$\alpha_j = x_j + \sqrt{p_1 p_2}\, y_j, \text{ if } 2 \nmid z_j \quad \text{and} \quad \alpha_j = \frac{x_j + \sqrt{p_1 p_2}\, y_j}{2}, \text{ if } 2 \mid z_j. \tag{26}$$

By the same method of Lemma 3.4, we can show that $\alpha_j \in D_K^+$.

Theorem 5.15 (1) *Assume* $p_1 p_2 \equiv 1 \bmod 8$ *and* $d \equiv 6 \bmod 8$ *as above, then the Hilbert genus field* E *of* $K = \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{d})$ *is* $\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{2p_1}, \sqrt{\widehat{q_1}}, \ldots, \sqrt{\widehat{q_n}}, \sqrt{\alpha_t}, \ldots, \sqrt{\alpha_m})$ *with* t *given by* (25). *If* $m < t$, *there are no* $\sqrt{\alpha_j}$*-terms.*

(2) *Assume* $p_1 p_2 \equiv 1 \bmod 8$ *and* $p_1 d \equiv 6 \bmod 8$ *as above, then the Hilbert genus field* E *of* $K = \mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{p_1 d})$ *is* $\mathbb{Q}(\sqrt{p_1 p_2}, \sqrt{2p_1}, \sqrt{\widehat{q_1}}, \ldots, \sqrt{\widehat{q_n}}, \sqrt{\alpha_t}, \ldots, \sqrt{\alpha_m})$ *with* t *given by* (25). *If* $m < t$, *there are no* $\sqrt{\alpha_j}$*-terms.*

Proof In all cases, it suffices to show that $K(\sqrt{\alpha_j})/K$ is unramified at every dyadic prime $\mathfrak{D}$ of K. The proof is similar to that of Theorem 5.7. For the case $\widetilde{q}_j$ even, one needs Lemma 2.11 (2). □

Acknowledgments The authors would like to thank Prof. Qin Yue for many helpful discussions.

References

1. Bae, S., Yue, Q.: Hilbert genus fields of real biquadratic fields. Ramanujan J. **24**, 161–181 (2011)
2. Conner, P.E., Hurrelbrink, J.: Class Number Parity, Ser. Pure Math., vol. 8. World Scientific, Singapore (1988)
3. Lang, S.: Cyclotomic Fields I and II. GTM 121. Springer-Verlag, New York (1990)
4. McCall, T.M., Parry, C.J., Ranalli, R.R.: On imaginary bicyclic biquadratic fields with cyclic 2-class group. J. Number Theory **53**, 88–99 (1995)
5. Ouyang, Y., Zhang, Z.: Hilbert genus fields of biquadratic fields. Sci. China Math., to appear
6. Sime, P.: Hilbert class fields of real biquadratic fields. J. Number Theory **50**, 154–166 (1995)
7. Yue, Q.: The generalized Rédei matrix. Math. Z. **261**, 23–37 (2009)
8. Yue, Q.: Genus fields of real biquadratic fields. Ramanujan J. **21**, 17–25 (2010)
9. Zhang, Z., Yue, Q.: Fundamental units of real quadratic fields of odd class number. J. Number Theory **137**, 122–129 (2014)