SCIENCE CHINA
Mathematics

• ARTICLES •

October 2014 Vol. 57 No. 10: 2111–2122
doi: 10.1007/s11425-014-4867-2

Hilbert genus fields of biquadratic fields

OUYANG Yi & ZHANG Zhe*

School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026*, China*
Email: yiouyang@ustc.edu.cn, lmlz@mail.ustc.edu.cn

Received June 24, 2013; accepted October 15, 2013; published online July 16, 2014

Abstract The Hilbert genus field of the real biquadratic field $K = \mathbb{Q}(\sqrt{\delta}, \sqrt{d})$ is described by Yue (2010) and Bae and Yue (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 Hilbert genus field of the imaginary biquadratic field $K = \mathbb{Q}(\sqrt{\delta}, \sqrt{d})$, where $\delta = -1, -2$ or $-p$ with $p \equiv 3 \bmod 4$ a prime and d any squarefree integer. This completes the explicit construction of the Hilbert genus field of any biquadratic field which contains an imaginary quadratic subfield of odd class number.

Keywords class group, Hilbert symbol, Hilbert genus field

MSC(2010) 11R65, 11R37

Citation: Ouyang Y, Zhang Z. Hilbert genus fields of biquadratic fields. Sci China Math, 2014, 57: 2111–2122, doi: 10.1007/s11425-014-4867-2

1 Introduction

Let K be a number field and H be the Hilbert class field of K. The Galois group $G = \mathrm{Gal}(H/K)$ is isomorphic to the ideal class group $C(K)$ of K via Artin's reciprocity map (see [5]). The *Hilbert genus field of* K is the invariant field E of G^2. Then by Galois theory

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

and by Kummer theory, there exists a unique multiplicative group Δ, $K^{*2} \subset \Delta \subset K^*$ such that

$$E = H \cap K(\sqrt{K^*}) = K(\sqrt{\Delta}). \tag{1.1}$$

Given K, a natural question 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}.

For δ a squarefree integer, the field $\mathbb{Q}(\sqrt{\delta})$ has odd class number if and only if (i) $\delta = p$ for p a prime or $\delta = 2p$ or p_1p_2 for p, p_1 and p_2 primes 3 mod 4, or (ii) $\delta = -1, -2$ or $-p$ with $p \equiv 3 \bmod 4$ (see [2]). In the real case that $\delta = p$ with $p = 2$ or $p \equiv 1 \bmod 4$, there has been a long history of study on the Hilbert genus field of $K = \mathbb{Q}(\sqrt{p}, \sqrt{d})$ where d is a squarefree positive integer prime to p. When $p \equiv 1 \bmod 8$ and $d \equiv 3 \bmod 4$, Sime [6] used Herglotz's results [3] to give the Hilbert genus field of K, under the condition that 2-Sylow subgroups of the class groups of $K_0 = \mathbb{Q}(\sqrt{p})$, $K_1 = \mathbb{Q}(\sqrt{d})$ and $K_2 = \mathbb{Q}(\sqrt{pd})$ are elementary. Later, Yue [8] improved Sime's result to $p \equiv 1 \bmod 4$, $d \equiv 3 \bmod 4$, and without the

*Corresponding author

condition on the class groups. Recently, Bae and Yue [1] worked out the case $p \equiv 1 \bmod 4$ or $p = 2$ and d a squarefree positive integer.

In this paper, we shall work out the imaginary case (i.e., the second case). We give a complete explicit construction of the Hilbert genus field of $K = \mathbb{Q}(\sqrt{\delta}, \sqrt{d})$ where $\delta = -1, -2$ or $-p$ with $p \equiv 3 \bmod 4$ and d a squarefree integer. Our results are stated in Theorem 3.4 ($\delta = -p$), Theorem 4.2 ($\delta = -1$) and Theorem 5.2 ($\delta = -2$).

Our strategy to explicitly construct E is based on the following theoretical results. For a number field K, set

$$D_K = \{x \in K^* \mid v_{\mathfrak{p}}(x) \equiv 0 \bmod 2 \text{ for all finite primes } \mathfrak{p} \text{ of } K\}. \tag{1.2}$$

Then we have

Proposition 1.1. *Let K be a number field. Suppose $\mathcal{O}_K$ and U_K are the ring of integers and the group of units of K respectively.*

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

(2) *The sequence*

$$1 \longrightarrow U_K/U_K^2 \longrightarrow D_K/K^{*2} \xrightarrow{\phi} C(K)[2] \longrightarrow 1$$

is exact, where $\phi([x]) = [I]$ if $x\mathcal{O}_K = I^2$. Hence we have

$$r_2(\Delta/K^{*2}) = r_2(C(K)) = r_2(D_K/K^{*2}) - r_2(U_K/U_K^2), \tag{1.3}$$

where for a finite Abelian group A, $r_2(A)$ is the 2-rank of A.

Proof. (1) The proof is similar to that of [8, Lemma 2.1].

(2) Since D_K is the set $\{x \in K^* \mid (x) = I^2 \text{ for some fractional ideal } I \text{ of } K\}$, the sequence is exact. $\square$

From now on, we suppose

(1) $K = \mathbb{Q}(\sqrt{\delta}, \sqrt{d})$, where $\delta = -1, -2$ or $-p$ with $p \equiv 3 \bmod 4$ and d a squarefree integer;

(2) $K_0 = \mathbb{Q}(\sqrt{\delta})$ has odd class number in our case;

(3) $E = K(\sqrt{\Delta})$ is the Hilbert genus field of K, where $K^{*2} \subset \Delta \subset K^*$;

(4) NK is the image of K under the norm map N_{K/K_0};

(5) s is the number of finite primes of K_0 ramified in K.

Then we have

Proposition 1.2. *Assume K as above, then*

$$r_2(C(K)) = r_2(\Delta/K^{*2}) = r_2(D_K/K^{*2}) - 2 = s - 1 - r_2(U_{K_0}/U_{K_0} \cap NK). \tag{1.4}$$

Proof. The second equality follows from Proposition 1.1. In this case, $r_2(U_K/U_K^2) = 2$. It suffices to show the third equality.

We show that the 2-Sylow subgroup $C(K)^{\mathrm{Gal}(K/K_0)}[2^\infty]$ of the group of ambiguous ideal classes $C(K)^{\mathrm{Gal}(K/K_0)}$ is nothing but $C(K)[2]$, the 2-torsion subgroup of $C(K)$. As a consequence $r_2(C(K)) = r_2(C(K)^{\mathrm{Gal}(K/K_0)})$ and $C(K)^{\mathrm{Gal}(K/K_0)}$ has no 4-torsion. Indeed, suppose σ is the nontrivial element of $\mathrm{Gal}(K/K_0)$. For $\mathfrak{c}$ an element of $C(K)^{\mathrm{Gal}(K/K_0)}[2^\infty]$, then $\mathfrak{c} = \sigma(\mathfrak{c})$. Suppose 2^k is the order of $\mathfrak{c}$, then $(\mathfrak{c}\sigma(\mathfrak{c}))^{2^{k-1}} = 1$. We regard $\mathfrak{c}\sigma(\mathfrak{c})$ as an ideal class of $C(K_0)$. Then $(\mathfrak{c}\sigma(\mathfrak{c}))^{\#C(K_0)} = 1$. Since K_0 has odd ideal class number, we must have $\mathfrak{c}\sigma(\mathfrak{c}) = 1$. Thus $\sigma(\mathfrak{c}) = \mathfrak{c}^{-1}$ and $\mathfrak{c}^2 = 1$. Conversely, for $\mathfrak{c} \in C(K)[2]$, $\mathfrak{c}^2 = 1$, we have $\mathfrak{c} = \mathfrak{c}^{-1}$. Since $(\mathfrak{c}\sigma(\mathfrak{c}))^2 = (\mathfrak{c}\sigma(\mathfrak{c}))^{\#C(K_0)} = 1$ and $\#C(K_0)$ is an odd integer, we deduce that $\mathfrak{c}\sigma(\mathfrak{c}) = 1$. Hence $\sigma(\mathfrak{c}) = \mathfrak{c}^{-1} = \mathfrak{c}$ and thus $\mathfrak{c} \in C(K)^{\mathrm{Gal}(K/K_0)}$.

Now the third equality follows from the class number formula [4, Lemma 4.1, p. 307] for cyclic extensions,

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

By Proposition 1.2 we first study the group $U_{K_0}/U_{K_0} \cap NK$ to obtain the 2-ranks of Δ/K^{*2} and D_K/K^{*2}. Then we find a set of representatives of D_K/K^{*2}. From this set we get a set of representatives of Δ/K^{*2} and hence our results follow.

2 Local and global computation

In this section, we compile several results for later usage. First we fix the following notation.

For a number field or local field F, we let $\mathcal{O}_F$ be the ring of integers of F and U_F be the unit group of $\mathcal{O}_F$. If F is a number field and $\mathfrak{p}$ is 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. An integer solution of a Diophantine equation is called *primitive* if the components are relatively prime to each other.

2.1 Ramification

Lemma 2.1 (See [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) $U_F^{(5)} = (U_F^{(2)})^2$, $U_F^2 = U_F^{(5)} \bigsqcup (-1) \cdot U_F^{(5)}$.

(2) $F(\sqrt{3}) = F(\sqrt{-3})$ *is unramified over* F.

Proof. (1) We can see that π is a uniformizer because it is a root of Eisenstein polynomial x^2+2x+2. By $U_F = U_F^{(1)}$, $[U_F : U_F^{(5)}] = 16$. That $U_F^{(5)} = (U_F^{(2)})^2$ is easy. Now one just has to check $-1 = (1+\pi)^2 \notin U_F^{(5)}$.

(2) It is clear that $F(\sqrt{3}) = F(\sqrt{-3})$ is the unique unramified extension of degree two over F. $\square$

Lemma 2.3. *Suppose* $F = \mathbb{Q}_2(\sqrt{-2})$. *Then* $\pi = \sqrt{-2}$ *is a uniformizer of* F, *and*

(1) $U_F^{(5)} = (U_F^{(3)})^2$ *and* $U_F^2 = U_F^{(5)} \bigsqcup (1+\pi^2+\pi^3) U_F^{(5)}$.

(2) $F(\sqrt{1+\pi^2+\pi^3+\pi^4}) = F(\sqrt{1+\pi^4})$ *is unramified over* F.

Proof. The proof is similar to that of Lemma 2.2. $\square$

2.2 Decomposition and congruence

Lemma 2.4. *Suppose* $p \equiv 3 \bmod 4$ *is a prime.*

(1) *If* q *is an odd prime such that* $(\frac{-p}{q}) = 1$, *then the equation* $x^2 + py^2 = qz^2$ *has a solution in* $\mathbb{Z}$.

(2) *If furthermore* $p \equiv 7 \bmod 8$, *then there exists a primitive solution* (x_0, z_0) *of* $x^2 + p = 2z^2$ *such that* $4 \mid z_0$.

(3) *Furthermore, if* $q \equiv 3 \bmod 4$, *then* $2qz^2 = x^2 + py^2$ *has a primitive solution* $(x, y, z) = (u_0, v_0, w_0)$ *such that* $4 \mid w_0$.

Proof. (1) It suffices to compute the Hilbert symbols associated to the equation, which is clear.

(2) Any integer solution is clearly primitive, and moreover, x_0 is odd and z_0 is even. Replace (x_0, z_0) by $(3x_0 + 4z_0, 2x_0 + 3z_0)$ if necessary, we can get z_0 such that $4 \mid z_0$.

(3) Let (x_0, z_0) be as given in (2) and (x_1, y_1, z_1) be a primitive solution of $qz^2 = x^2 + py^2$ such that $(x_1, y_1) \equiv (1, 1) \bmod 4$ if $2 \mid z_1$. Then $(x, y, z) = (x_0x_1 - py_1, x_0y_1 + x_1, z_0z_1)$ is a solution of $2qz^2 = x^2 + py^2$. We will complete the proof by the following two cases:

If $2 \nmid z_1$, then $(x_1, y_1) \equiv (0, 1) \bmod 2$, thus $x_0x_1 - py_1$ and $x_0y_1 + x_1$ are odd integers. Since $4 \mid z_0z_1$, $(x_0x_1 - py_1, x_0y_1 + x_1, z_0z_1)$ gives a primitive solution (u_0, v_0, w_0) with $4 \mid w_0$.

If $2 \mid z_1$, we can choose $x_0 \equiv 1 \bmod 4$, then

$$(x_0x_1 - py_1, x_0y_1 + x_1) \equiv (x_1 + y_1, x_1 + y_1) \equiv (2, 2) \bmod 4.$$

Since $8 \mid z_0z_1$, $(x_0x_1 - py_1, x_0y_1 + x_1, z_0z_1)$ gives a primitive solution (u_0, v_0, w_0) with $4 \mid w_0$. $\square$

Lemma 2.5. *Assume that $p \equiv 3 \bmod 4$ is a prime and $F = \mathbb{Q}(\sqrt{-p})$, $N \equiv 1 \bmod 4$, $N = q$ or q_1q_2, where q, q_1, q_2 are primes satisfying Lemma 2.4(1). Let (x_0, y_0, z_0) be a primitive solution of $Nz^2 = x^2 + py^2$. Take $\alpha = x_0 + \sqrt{-p}y_0$ if $2 \nmid z_0$ and $\alpha = \frac{x_0+\sqrt{-p}y_0}{2}$ 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 $-p \equiv 5 \bmod 8$ and $2 \mid z_0$, then in the local field $\mathbb{Q}_2(\sqrt{-p}) = \mathbb{Q}_2(\sqrt{-3})$, $\alpha \equiv \omega(-x_0)$ or $\omega^2(-x_0) \bmod 4$, where $\omega = \frac{-1+\sqrt{-3}}{2}$.*

(4) *If $-p \equiv 1 \bmod 8$ and $2 \mid z_0$, then $D_1 = (2, \alpha) \neq D_2 = (2, \overline{\alpha})$ are the two dyadic primes of F, and $\alpha \equiv x_0 \bmod D_2^2$ and $\alpha/2^e \equiv x_0 \bmod D_1^2\mathcal{O}_{F_{D_1}}$ for an even integer e.*

Proof. The proofs of (2)–(4) are similar to those of [1, Lemma 2.6], so we only need to prove (1). One can check that $\alpha\overline{\alpha}$ and $\alpha + \overline{\alpha} \in \mathbb{Z}$, so $\alpha \in \mathcal{O}_F$. If $\mathfrak{p}$ is a prime of $\mathcal{O}_F$ which divides both $\alpha\mathcal{O}_F$ and $\overline{\alpha}\mathcal{O}_F$, then $\alpha + \overline{\alpha} \in \mathfrak{p}$. 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 $\ell \mid x_0$. Since $\ell \mid z_0$, we have $\ell \mid y_0$, which is absurd. 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 2.6. *Suppose p is a prime congruence to 7 modulo 8, $F = \mathbb{Q}(\sqrt{-p})$.*

(1) *Suppose (x_0, z_0) is a solution of $x^2 + p = 2z^2$ as given in Lemma 2.4(2). Let $\alpha = \frac{x_0+\sqrt{-p}}{2}$ and $\overline{\alpha} = \frac{x_0-\sqrt{-p}}{2}$ be its conjugate in F. Then $D_1 = (2, \alpha)$ and $D_2 = (2, \overline{\alpha})$ are the two dyadic primes of F, $\alpha \equiv x_0 \bmod D_2^3$ and $\alpha/2^{e_1} \equiv x_0 \bmod D_1^3\mathcal{O}_{F_{D_1}}$ for an odd integer e_1.*

(2) *Suppose $q \equiv 3 \bmod 4$ satisfies the assumption in Lemma 2.4(1) and let (a_0, b_0, c_0) be a primitive solution of $qz^2 = x^2 + py^2$. If $2 \mid c_0$ and $(a_0, b_0) \equiv (x_0, 1) \bmod 4$, let $\beta = \frac{a_0+b_0\sqrt{-p}}{2}$, $\overline{\beta}$ be the conjugate of β in F. Then $(2, \beta) = D_1$, $(2, \overline{\beta}) = D_2$, $\beta \equiv a_0 \bmod D_2^2$ and $\beta/2^{e_2} \equiv -a_0 \bmod D_1^2\mathcal{O}_{F_{D_1}}$ for an even integer e_2.*

(3) *Suppose $q \equiv 3 \bmod 4$ satisfies the assumption in Lemma 2.4(3) and let (u_0, v_0, w_0) be a primitive solution of $2qz^2 = x^2+py^2$ such that $(u_0, v_0, w_0) \equiv (x_0, 1, 0) \bmod 4$. Let $\gamma = \frac{u_0+v_0\sqrt{-p}}{2}$, $\overline{\gamma}$ be the conjugate of γ in F. Then $(2, \gamma) = D_1$, $(2, \overline{\gamma}) = D_2$, $\gamma \equiv u_0 \bmod D_2^3$ and $\gamma/2^{e_3} \equiv -u_0$ or $3u_0 \bmod D_1^3\mathcal{O}_{F_{D_1}}$ for an odd integer e_3.*

Proof. (1) We have $\alpha\overline{\alpha} = \frac{2z_0^2}{4} \equiv 0 \bmod 8$ and $\alpha + \overline{\alpha} = x_0 \in \mathbb{Z}$, hence $\alpha \in \mathcal{O}_F$. By the same argument as Lemma 2.5(1), we can show that $\alpha\mathcal{O}_F$ is prime to $\overline{\alpha}\mathcal{O}_F$. Moreover, by the fact that $\alpha\overline{\alpha} \in 8\mathbb{Z}$, we know $D_1 = (2, \alpha)$ and $D_2 = (2, \overline{\alpha})$ are the two dyadic primes of F, and $\alpha \in D_1^3$ and $\overline{\alpha} \in D_2^3$. Then $\alpha = x_0 - \overline{\alpha} \equiv x_0 \bmod D_2^3$ and $\overline{\alpha} \equiv x_0 \bmod D_1^3$. If $2^k \| z_0$, $k \geqslant 2$, then by

$$\alpha \cdot \overline{\alpha} \cdot 2^{-2(k-1)-1} = \frac{z_0^2}{2^{2k}} \equiv 1 \bmod D_1^3\mathcal{O}_{F_{D_1}}$$

(since the square of an odd integer $\equiv 1 \bmod 8$),

$$\frac{\alpha}{2^{2(k-1)+1}} \equiv \overline{\alpha}^{-1} \equiv x_0 \bmod D_1^3\mathcal{O}_{F_{D_1}}.$$

(2) Since $a_0 \equiv x_0 \bmod 4$ and $b_0 \equiv 1 \bmod 4$, $(2, \beta) = (2, \alpha) = D_1$ and $(2, \overline{\beta}) = (2, \overline{\alpha}) = D_2$. The rest of (2) follows from the same argument in the proof of (1).

(3) Since $u_0 \equiv x_0 \bmod 4$ and $v_0 \equiv 1 \bmod 4$, $(2, \gamma) = (2, \alpha) = D_1$ and $(2, \overline{\gamma}) = (2, \overline{\alpha}) = D_2$. The rest of (3) follows from the same argument in the proof of (1), just recall that $q \equiv -1$ or $3 \bmod 8$. □

3 The case $K = \mathbb{Q}(\sqrt{-p}, \sqrt{d})$ with $p \equiv 3 \bmod 4$

In this section, $p \equiv 3 \bmod 4$, $K_0 = \mathbb{Q}(\sqrt{-p})$ and $K = \mathbb{Q}(\sqrt{-p}, \sqrt{d})$. We always write

$$d = \pm \prod_{j=1}^{n} q_j \quad \text{or} \quad d = \pm 2 \prod_{j=1}^{n} q_j \tag{3.1}$$

with $p, q_1, \ldots, q_n$ distinct odd primes such that the Legendre symbol

$$\left(\frac{-p}{q_j}\right) = \begin{cases} 1, & \text{if } 1 \leqslant j \leqslant m, \\ -1, & \text{if } m+1 \leqslant j \leqslant n, \end{cases} \tag{3.2}$$

and we assume that

$$q_1 \equiv 3 \bmod 4 \text{ if there exists } j \text{ for } 1 \leqslant j \leqslant m \text{ such that } q_j \equiv 3 \bmod 4. \tag{3.3}$$

Note that (3.3) means

$$\text{If } m \geqslant 1, \text{ then } q_1 \equiv 1 \bmod 4 \text{ if and only if } q_j \equiv 1 \bmod 4 \text{ for all } 1 \leqslant j \leqslant m. \tag{3.4}$$

Suppose $m \geqslant 1$. We now choose the elements α_j, β_j and γ_j for $1 \leqslant j \leqslant m$ and α_0. By Lemma 2.4, for any $1 \leqslant j \leqslant m$, the equation $q_j z^2 = x^2 + py^2$ has an integer solution, so do the equations $q_1 q_j z^2 = x^2 + py^2$ for $2 \leqslant j \leqslant m$. For each j, choose a primitive solution (x_j, y_j, z_j) of $q_j z^2 = x^2 + py^2$ (resp. $q_1 q_j z^2 = x^2 + py^2$) if $q_j \equiv 1 \bmod 4$ (resp. $j > 1$ and $q_j \equiv 3 \bmod 4$) by the following rules:
- if there exists odd z_j, then choose x_j and y_j such that $x_j + y_j \equiv 1 \bmod 4$;
- if every primitive solution z_j is even, then choose $x_j \equiv 3 \bmod 4$ if $p \equiv 3 \bmod 8$ and $x_j \equiv 1 \bmod 4$ if $p \equiv 7 \bmod 8$.

Then set

$$\alpha_j = x_j + \sqrt{-p}y_j, \quad \text{if } 2 \nmid z_j \quad \text{and} \quad \alpha_j = \frac{x_j + \sqrt{-p}y_j}{2}, \quad \text{if } 2 \mid z_j. \tag{3.5}$$

Now we assume $p \equiv 7 \bmod 8$. Set

$$\alpha_0 = \frac{x_0 + \sqrt{-p}}{2}, \quad \text{with } (x_0, z_0) \equiv (1, 0) \bmod 4 \text{ a primitive solution of } x^2 + p = 2z^2. \tag{3.6}$$

Let (x_j, y_j, z_j) be any primitive solution of $q_j z^2 = x^2 + py^2$, then set

$$\beta_j = x_j + \sqrt{-p}y_j, \quad \text{if } 2 \nmid z_j \quad \text{and} \quad \beta_j = \frac{x_j + \sqrt{-p}y_j}{2}, \quad \text{if } 2 \mid z_j. \tag{3.7}$$

If $q_j \equiv 3 \bmod 4$, let (x_j, y_j, z_j) be a primitive solution of $2q_j z^2 = x^2 + py^2$ such that $4 \mid z_j$ and $x_j \equiv 1 \bmod 4$. Set

$$\gamma_j = \alpha_j, \quad \text{if } q_j \equiv 1 \bmod 4 \quad \text{and} \quad \gamma_j = \frac{x_j + \sqrt{-p}y_j}{2}, \quad \text{if } q_j \equiv 3 \bmod 4. \tag{3.8}$$

Lemma 3.1. *The elements -1, $\pm q_i$ $(1 \leqslant i \leqslant n)$, α_j, β_j and γ_j $(1 \leqslant j \leqslant m)$ defined above all belong to D_K. If $d \equiv 2$ or $3 \bmod 4$, $\pm 2 \in D_K$.*

Proof. $-1 \in D_K$ is trivial. Since q_i is ramified in K, we see that $\pm q_i \in D_K$ for $1 \leqslant i \leqslant n$.

For α_j, we know that $\alpha_j \overline{\alpha}_j = q_j z_j^2$, $\frac{q_j z_j^2}{4}$, $q_1 q_j z_j^2$ or $\frac{q_1 q_j z_j^2}{4}$ and that q_1, q_j are ramified in K. By Lemma 2.5, $\alpha_j \mathcal{O}_{K_0}$ is prime to $\overline{\alpha}_j \mathcal{O}_{K_0}$, hence $\alpha_j \mathcal{O}_K$ is prime to $\overline{\alpha}_j \mathcal{O}_K$ in $\mathcal{O}_K$. We see that in $\mathcal{O}_K$, $\alpha_j \overline{\alpha}_j \mathcal{O}_K$ is a square of an ideal, thus $\alpha_j \in D_K$. The proofs of β_j and γ_j are similar.

If $d \equiv 2$ or $3 \bmod 4$, 2 is ramified in K, thus $\pm 2 \in D_K$. □

Lemma 3.2. *Suppose that p is a prime $\equiv 7 \bmod 8$. Then*

(1) *$\alpha_0 \in D_K$.*

(2) *If $d \equiv 3 \bmod 4$, both $K(\sqrt{2})/K$ and $K(\sqrt{\alpha_0})/K$ are ramified at some dyadic prime of K for every choice of α_0.*

(3) *If $d \equiv 2 \bmod 8$, then $K(\sqrt{2})/K$ is unramified at the dyadic primes and so is $K(\sqrt{\alpha_0})/K$. If $d \equiv 6 \bmod 8$, $K(\sqrt{-2})/K$ is unramified at the dyadic primes and $K(\sqrt{\alpha_0})/K$ is ramified at some dyadic prime of K.*

Proof. (1) Since $\alpha_0\bar{\alpha}_0 = \frac{z_0^2}{2}$ and $(\alpha_0\mathcal{O}_{K_0}, \overline{\alpha}_0\mathcal{O}_{K_0}) = 1$, $\alpha_0 \in D_K$.

In both (2) and (3), $d \equiv 2$ or $3 \bmod 4$, 2 is ramified in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, so $2\mathcal{O}_K = \mathcal{D}_1^2\mathcal{D}_2^2$, where

$$D_1 = \mathcal{D}_1 \cap \mathcal{O}_{K_0}, \quad D_2 = \mathcal{D}_2 \cap \mathcal{O}_{K_0}$$

are the dyadic primes of K_0 as given in Lemma 2.6. For any dyadic prime $\mathcal{D}$ of K, let $D = \mathcal{D} \cap \mathcal{O}_{K_0}$, then $K_{0,D} = \mathbb{Q}(\sqrt{-p})_D \simeq \mathbb{Q}_2$. Hence $K_{\mathcal{D}} \simeq \mathbb{Q}_2(\sqrt{d})$.

If $d \equiv 3 \bmod 4$, then $K_{\mathcal{D}} \simeq \mathbb{Q}_2(\sqrt{3})$ or $\mathbb{Q}_2(\sqrt{-1})$, hence $K(\sqrt{2})/K$ is ramified at the dyadic primes of K. By Lemma 2.6(1), $K_{\mathcal{D}_1}(\sqrt{\alpha_0}) = K_{\mathcal{D}_1}(\sqrt{\frac{\alpha_0}{2^{e_1-1}}}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{2x_0})$ is totally ramified over $\mathbb{Q}_2$, hence $K(\sqrt{\alpha_0})/K$ is ramified at $\mathcal{D}_1$.

If $d \equiv 2 \bmod 8$, then $K_{\mathcal{D}_1} \simeq K_{\mathcal{D}_2} \simeq \mathbb{Q}_2(\sqrt{2})$ or $\mathbb{Q}_2(\sqrt{10})$. Thus $K(\sqrt{2})/K$ is unramified at the dyadic primes of K. By Lemma 2.6(1), $K_{\mathcal{D}_1}(\sqrt{\alpha_0}) \simeq \mathbb{Q}_2(\sqrt{2}, \sqrt{2x_0})$ or $\mathbb{Q}_2(\sqrt{10}, \sqrt{2x_0})$. Since $x_0 \equiv 1 \bmod 4$, $K_{\mathcal{D}_1}(\sqrt{\alpha_0})/K_{\mathcal{D}_1}$ is unramified. Similarly, $K_{\mathcal{D}_2}(\sqrt{\alpha_0})/K_{\mathcal{D}_2}$ is also unramified. Therefore, $K(\sqrt{\alpha_0})/K$ is unramified at the dyadic primes of K.

If $d \equiv 6 \bmod 8$, then $K_{\mathcal{D}_1} \simeq K_{\mathcal{D}_2} \simeq \mathbb{Q}_2(\sqrt{6})$ or $\mathbb{Q}_2(\sqrt{-2})$. Hence $K(\sqrt{-2})/K$ is unramified at the dyadic primes of K and one of the extensions $K_{\mathcal{D}_1}(\sqrt{\alpha_0})/K_{\mathcal{D}_1}$ and $K_{\mathcal{D}_2}(\sqrt{\alpha_0})/K_{\mathcal{D}_2}$ must be ramified. $\square$

Lemma 3.3. *Suppose conventions on d are as above. Then we have the following table*:

p	d	q_1	s	$r_2(\Delta/K^{*2})$
3 mod 4	1 mod 4	1 mod 4	$m+n$	$m+n-1$
		3 mod 4	$m+n$	$m+n-2$
3 mod 8	2, 3 mod 4	1 mod 4	$m+n+1$	$m+n$
		3 mod 4	$m+n+1$	$m+n-1$
7 mod 8	3 mod 4, 6 mod 8		$m+n+2$	$m+n$
7 mod 8	2 mod 8	1 mod 4	$m+n+2$	$m+n+1$
		3 mod 4	$m+n+2$	$m+n$

Proof. For $d \equiv 1 \bmod 4$, there are $m+n$ finite primes ramified in K/K_0, and for $d \equiv 2, 3 \bmod 4$, there are $m+n+1$ (resp. $m+n+2$) finite primes ramified in K/K_0 if 2 is inert (resp. split) in K_0, i.e., $p \equiv 3 \bmod 8$ (resp. $7 \bmod 8$). We thus get the values of s in the table.

To know $r_2(\Delta/K^{*2})$, by Proposition 1.2, it suffices to know $U_{K_0}/U_{K_0} \cap NK$. If $p \neq 3$, then $U_{K_0} = \{\pm 1\}$, thus we just have to check if $-1 \in NK$, equivalently, if $(-1, d)_{\mathfrak{p}} = 1$ for every prime $\mathfrak{p}$ of K_0 which ramified in K. For $1 \leqslant j \leqslant m$, q_j splits in K_0. For every prime $\mathfrak{q}_j$ above q_j, we have

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

For $m+1 \leqslant j \leqslant n$, q_j is inert in K_0. Let $\mathfrak{q}_j$ be the prime above q_j. By Lemma 3.3 of [7], we have

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

For $p \equiv 7 \bmod 8$, 2 splits in K_0. Let D be a dyadic prime above 2. We have $(-1, d)_D = (-1)^{\frac{d-1}{2}}$ or $(-1)^{\frac{d/2-1}{2}}$ depending on d being odd or even. For $p \equiv 3 \bmod 8$, 2 is inert in K_0, the product formula gives $(-1, d)_D = 1$. We thus get the values of $r_2(\Delta/K^{*2})$ in the table.

If $p = 3$, then $K_0 = \mathbb{Q}(\sqrt{-3})$ and $U_{K_0} = \{\pm 1, \pm\omega, \pm\omega^2\}$, where ω is a primitive 3-rd root unity. Since $\omega = (\omega^2)^2$, $\{1, \omega, \omega^2\} \subset NK$ and the same result holds. $\square$

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

Theorem 3.4. *Assume p and d as above, then the Hilbert genus field E of* $K = \mathbb{Q}(\sqrt{-p}, \sqrt{d})$ *is given by the following table*:

Case	p	d	q_1	*Hilbert genus field* E
I	3 (mod 4)	1 (mod 4)	1 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_m})$
			3 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_m})$
II	3 (mod 8)	3 (mod 4)	1 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{-1}, \sqrt{q_1}, \dots, \sqrt{q_n}, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_m})$
			3 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{-1}, \sqrt{q_1}, \dots, \sqrt{q_n}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_m})$
III	3 (mod 8)	2 (mod 8)	1 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_m})$
			3 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_m})$
IV	3 (mod 8)	6 (mod 8)	1 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{-2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_m})$
			3 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{-2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_m})$
V	7 (mod 8)	3 (mod 4)		$\mathbb{Q}(\sqrt{-p}, \sqrt{-1}, \sqrt{q_1}, \dots, \sqrt{q_n}, \sqrt{\beta_1}, \dots, \sqrt{\beta_m})$
VI	7 (mod 8)	2 (mod 8)	1 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_0}, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_m})$
			3 (mod 4)	$\mathbb{Q}(\sqrt{-p}, \sqrt{2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\alpha_0}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_m})$
VII	7 (mod 8)	6 (mod 8)		$\mathbb{Q}(\sqrt{-p}, \sqrt{-2}, \sqrt{q_1^*}, \dots, \sqrt{q_n^*}, \sqrt{\gamma_1}, \dots, \sqrt{\gamma_m})$

Here $q^* = (-1)^{\frac{q-1}{2}} q$, $\alpha_j, \alpha_0, \beta_j, \gamma_j$ *are given by* (3.5)–(3.8).

Example 3.5 (Case I and Case VII)**.** Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{5005})$. It is clear that $5005 = 7 \times 13 \times 5 \times 11 \equiv 1 \bmod 4$, $\left(\frac{-3}{7}\right) = \left(\frac{-3}{13}\right) = 1$, $\left(\frac{-3}{5}\right) = \left(\frac{-3}{11}\right) = -1$. Then $n = 4$, $m = 2$. Since $q_1 = 7 \equiv 3 \bmod 4$, $r_2(\Delta/K^{*2}) = m + n - 2 = 4$. Since $q_2 = 13 \equiv 1 \bmod 4$ and $13 = 1^2 + 3 \cdot 2^2$, we have $\alpha_2 = -1 + 2\sqrt{-3}$, and

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

Let $K = \mathbb{Q}(\sqrt{-7}, \sqrt{110})$. It is clear that $110 = 2 \times 11 \times 5 \equiv 6 \bmod 8$, $\left(\frac{-7}{11}\right) = 1$, $\left(\frac{-7}{5}\right) = -1$. Then $n = 2$, $m = 1$, $r_2(\Delta/K^{*2}) = m + n = 3$. Since $q_1 = 11 \equiv 3 \bmod 4$ and $2 \cdot 11 \cdot 4^2 = 3^2 + 7 \cdot 7^2$, we have $\gamma_1 = \frac{-3+7\sqrt{-7}}{2}$ and

$$E = \mathbb{Q}(\sqrt{-7}, \sqrt{-2}, \sqrt{5}, \sqrt{-11}, \sqrt{\gamma_1}).$$

We shall prove the theorem case by case. We note the fact that $K(\sqrt{q_i^*})/K$ is always unramified.

Proof of Case I. (1) If $q_1 \equiv 1 \bmod 4$, by Lemma 3.3, we have $r_2(\Delta/K^{*2}) = m+n-1$ and $r_2(D_K/K^{*2}) = m + n + 1$. We first show the set

$$\{-1, q_1^*, \dots, q_{n-1}^*, \alpha_1, \dots, \alpha_m, \eta\}, \tag{3.9}$$

where $\eta = x + y\sqrt{d} \in K$, $N_{K/K_0}(\eta) = -1$, is a set of representatives of D_K/K^{*2}. It suffices to show that its elements are independent modulo K^{*2}.

Consider $\xi = \eta^a \cdot \prod_i q_i^{*b_i} \prod_j \alpha_j^{c_j}$, where $a, b_i, c_j \in \{0, 1\}$, $q_i^* \in \{-1, q_1^*, \dots, q_{n-1}^*\}$, $\alpha_j \in \{\alpha_1, \dots, \alpha_m\}$. Let $K_2 = \mathbb{Q}(\sqrt{-pd})$, then

$$N_{K/K_2}(\xi) = (-1)^a \cdot \prod_i q_i^{2b_i} \prod_j q_j^{c_j} \cdot \lambda^2, \quad \lambda \in K_2.$$

Suppose $\xi \in K^{*2}$, then $N_{K/K_2}(\xi) \in K_2^{*2}$, thus $a = c_j = 0$. Now $\xi = \prod_i q_i^{*b_i} \in K^{*2}$, since K has only three quadratic subfields: $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{-pd})$, we must have $b_i = 0$. Therefore the set (3.9) is a representative set of D_K/K^{*2}.

We now show Δ/K^{*2} is generated by $\{q_1^*, \dots, q_{n-1}^*, \alpha_1, \dots, \alpha_m\}$. It suffices to show that $K(\sqrt{\alpha_j})/K$, $1 \leqslant j \leqslant m$, are unramified extensions. By Proposition 1.1(1), we only need to show that they are unramified at the dyadic primes of K.

Let $\mathcal{D}$ be a dyadic prime of K. If $p \equiv 3 \bmod 8$, $K_{\mathcal{D}} \simeq \mathbb{Q}_2(\sqrt{-3})$. For $1 \leqslant j \leqslant m$, if $2 \nmid z_j$, $\alpha_j \equiv x_j + y_j \equiv 1 \bmod 4$. Hence $K_{\mathcal{D}}(\sqrt{\alpha_j})/K_{\mathcal{D}}$ is unramified. If $2 \mid z_j$, then $\alpha_j \equiv \omega(-x_j)$ or $\equiv \omega^2(-x_j) \bmod 4$. Then by Lemma 2.1(4), $K_{\mathcal{D}}(\sqrt{\alpha_j})/K_{\mathcal{D}}$ is also unramified.

If $p \equiv 7 \bmod 8$, we have $K_{\mathcal{D}} \simeq \mathbb{Q}_2$ if $d \equiv 1 \bmod 8$ and $K_{\mathcal{D}} \simeq \mathbb{Q}_2(\sqrt{-3})$ if $d \equiv 5 \bmod 8$. According to Lemma 2.5, if $2 \nmid z_j$, $\alpha_j \equiv x_j + y_j \equiv 1 \bmod 4$. Hence $K_{\mathcal{D}}(\sqrt{\alpha_j})/K_{\mathcal{D}}$ is unramified. If $2 \mid z_j$, then by Lemma 2.5, $K_{\mathcal{D}}(\sqrt{\alpha_j}) \simeq K_{\mathcal{D}}(\sqrt{x_j})$ or $K_{\mathcal{D}}(\sqrt{x_j + 4}) \simeq K_{\mathcal{D}}$ or $K_{\mathcal{D}}(\sqrt{-3})$. Thus $K_{\mathcal{D}}(\sqrt{\alpha_j})/K_{\mathcal{D}}$ is also unramified.

(2) If $q_1 \equiv 3 \bmod 4$, then by Lemma 3.3, we have $r_2(\Delta/K^{*2}) = m+n-2$. By the construction of α_j, $2 \leqslant j \leqslant m$ and similar to the proof of (1), we see that $\{q_1^*, \dots, q_{n-1}^*, \alpha_2, \dots, \alpha_m\}$ is a set of representatives of Δ/K^{*2} and $E = K(\sqrt{q_1^*}, \dots, \sqrt{q_{n-1}^*}, \sqrt{\alpha_2}, \dots, \sqrt{\alpha_m})$ is the Hilbert genus field of K. Note that if $q_j \equiv 3 \bmod 4$, we are using the solution of $q_1 q_j z^2 = x^2 + py^2$ instead of $q_j z^2 = x^2 + py^2$, because the latter one produces a ramified extension. □

Proof of Case II. (1) If $q_1 \equiv 1 \bmod 4$, then by Lemma 3.3, $r_2(\Delta/K^{*2}) = m+n$ and $r_2(D_K/K^{*2}) = m+n+2$. Let $\eta = x + y\sqrt{d} \in K$ such that $N_{K/K_0}(\eta) = -1$. Similar to the proof of Case I, we see that $\{-1, 2, q_1, \dots, q_{n-1}, \alpha_1, \dots, \alpha_m, \eta\}$ is a set of representatives of D_K/K^{*2}.

It is easy to verify that $K(\sqrt{-1})/K$ is unramified at the dyadic primes. For $1 \leqslant j \leqslant m$, by Lemma 2.5, we have $\alpha_j \equiv 1 \bmod 4$ if $2 \nmid z_j$ and $\alpha_j \equiv \omega(-x_j)$ or $\omega^2(-x_j) \bmod 4$ if $2 \mid z_j$. Then by Lemma 2.1(4), $K(\sqrt{\alpha_j})/K$ is unramified at the dyadic primes of K. Thus $\{-1, q_1, \dots, q_{n-1}, \alpha_1, \dots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}.

(2) Similarly, if $q_1 \equiv 3 \bmod 4$, we know that $r_2(\Delta/K^{*2}) = m+n-1$. By the construction, $\alpha_j \equiv 1$, $\omega(-x_j)$ or $\omega^2(-x_j) \bmod 4$, then by Lemma 2.1(4), $K(\sqrt{\alpha_j})/K$ is unramified and

$$\{-1, q_1, \dots, q_{n-1}, \alpha_2, \dots, \alpha_m\}$$

is a set of representatives of Δ/K^{*2}. □

Proof of Case III. If $q_1 \equiv 1 \bmod 4$, then by Lemma 3.3, $r_2(\Delta/K^{*2}) = m+n$. By Proposition 1.1(1) and Lemma 3.2, $K(\sqrt{2})/K$ is unramified. Similar to Case I, $K(\sqrt{\alpha_j})/K$ is unramified and the set

$$\{2, q_1^*, \dots, q_{n-1}^*, \alpha_1, \dots, \alpha_m\}$$

is independent modulo K^{*2}, so it is a set of representatives of Δ/K^{*2}.

If $q_1 \equiv 3 \bmod 4$, $r_2(\Delta/K^{*2}) = m+n-1$. By construction, for $2 \leqslant j \leqslant m$, $K(\sqrt{\alpha_j})/K$ is unramified and $\{2, q_1^*, \dots, q_{n-1}^*, \alpha_2, \dots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}. □

Proof of Case IV. If $q_1 \equiv 1 \bmod 4$, we know that $r_2(\Delta/K^{*2}) = m+n$. By Proposition 1.1(1) and Lemma 3.2, $K(\sqrt{-2})/K$ is an unramified extension. Similar to Case I, $K(\sqrt{\alpha_j})/K$ is unramified and $\{-2, q_1^*, \dots, q_{n-1}^*, \alpha_1, \dots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}.

If $q_1 \equiv 3 \bmod 4$, $r_2(\Delta/K^{*2}) = m+n-1$. By the same method, $\{-2, q_1^*, \dots, q_{n-1}^*, \alpha_2, \dots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}. □

Proof of Case V. By Lemma 3.3, $r_2(\Delta/K^{*2}) = m+n$ and thus $r_2(D_K/K^{*2}) = m+n+2$. By similar process to that in Case I, we know that $\{-1, 2, q_1, \dots, q_{n-1}, \alpha_0, \beta_1, \dots, \beta_m\}$ is a set of representatives of D_K/K^{*2}. We claim that $\{-1, q_1, \dots, q_{n-1}, \beta_1, \dots, \beta_m\}$ is a set of representatives of Δ/K^{*2}. It suffices to show that $K(\sqrt{\beta_j})/K$ is unramified at the dyadic primes.

Let $\mathcal{D}_1, \mathcal{D}_2$ be the two dyadic primes of K and $\mathcal{D}_1 \cap \mathcal{O}_{K_0} = D_1, \mathcal{D}_2 \cap \mathcal{O}_{K_0} = D_2$. Then $K_{0,D_1} \simeq K_{0,D_2} \simeq \mathbb{Q}_2$ and $K_{\mathcal{D}_1} \simeq K_{\mathcal{D}_2} \simeq \mathbb{Q}_2(\sqrt{d})$. If $2 \nmid z_j$, then β_j is a unit in $\mathbb{Z}_2$, since $d \equiv 3 \bmod 4$, $K_{\mathcal{D}_i}(\sqrt{\beta_j})/K_{\mathcal{D}_i}$ $(i = 1, 2)$ is unramified. If $2 \mid z_j$, then by Lemmas 2.5(4) and 2.6(2),

$$\frac{\beta_j}{2^e} \equiv x_j \text{ or } -x_j \bmod D_1^2 \mathcal{O}_{F_{D_1}} \text{ according to } q_j \equiv 1 \text{ or } -1 \bmod 4 \quad \text{and} \quad \beta_j \equiv x_j \bmod D_2^2,$$

where e is an even integer. Hence there exist odd integers u_j, v_j such that $K_{\mathcal{D}_1}(\sqrt{\beta_j}) \simeq \mathbb{Q}_2(\sqrt{u_j}, \sqrt{d})$ and $K_{\mathcal{D}_2}(\sqrt{\beta_j}) \simeq \mathbb{Q}_2(\sqrt{v_j}, \sqrt{d})$. Since $d \equiv 3 \bmod 4$, both $K_{\mathcal{D}_1}(\sqrt{\beta_j})/K_{\mathcal{D}_1}$ and $K_{\mathcal{D}_2}(\sqrt{\beta_j})/K_{\mathcal{D}_2}$ are unramified. Therefore, $K(\sqrt{\beta_j})/K$ is an unramified extension. □

Proof of Case VI. If $q_1 \equiv 1 \bmod 4$, then by Lemma 3.3, $r_2(\Delta/K^{*2}) = m+n+1$ and $r_2(D_K/K^{*2}) = m+n+3$. Let $\eta = x + y\sqrt{d}$ such that $N_{K/K_0}(\eta) = -1$. It is easy to verify that

$$\{-1, 2, q_1^*, \dots, q_{n-1}^*, \alpha_0, \alpha_1, \dots, \alpha_m, \eta\}$$

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

We now find a set of representatives of Δ/K^{*2}. We know by Lemma 3.2 that both $K(\sqrt{2})/K$ and $K(\sqrt{\alpha_0})/K$ are unramified at the dyadic primes. By the construction of α_j, we know that $K(\sqrt{\alpha_j})/K$ is also unramified at the dyadic primes. Hence $\{2, q_1^*, \dots, q_{n-1}^*, \alpha_0, \alpha_1, \dots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}.

If $q_1 \equiv 3 \bmod 4$, then $r_2(\Delta/K^{*2}) = m + n$. By the construction of α_j $(2 \leqslant j \leqslant m)$, we see that

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

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

Proof of Case VII. From Lemma 3.3, we know that $r_2(\Delta/K^{*2}) = m+n$ and $r_2(D_K/K^{*2}) = m+n+2$. We see that $\{-1, 2, q_1^*, \dots, q_{n-1}^*, \alpha_0, \gamma_1, \dots, \gamma_m\}$ is a set of representatives of D_K/K^{*2}.

For $1 \leqslant j \leqslant m$, if $q_j \equiv 1 \bmod 4$, $\gamma_j = \alpha_j$ and hence $K(\sqrt{\gamma_j})/K$ is unramified. If $q_j \equiv 3 \bmod 4$, then by Lemma 2.6(3), we have $\frac{\gamma_j}{2^e} \equiv -x_j$ or $3x_j \bmod D_1^3\mathcal{O}_{F_{D_1}}$ and $\gamma_j \equiv x_j \bmod D_2^3$, where e is an odd integer and D_1, D_2 are the dyadic primes of K_0. Let $\mathcal{D}_1, \mathcal{D}_2$ be the two dyadic primes of K above D_1 and D_2 respectively. Then $K_{\mathcal{D}_1} \simeq K_{\mathcal{D}_2} \simeq \mathbb{Q}_2(\sqrt{d})$ and $K_{\mathcal{D}_1}(\sqrt{\gamma_j}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{-2x_j})$ or $\mathbb{Q}_2(\sqrt{d}, \sqrt{6x_j})$, $K_{\mathcal{D}_2}(\sqrt{\gamma_j}) \simeq \mathbb{Q}_2(\sqrt{d}, \sqrt{x_j})$. Since $x_j \equiv 1 \bmod 4$ and $d \equiv 6 \bmod 8$, $\mathbb{Q}_2(\sqrt{d}, \sqrt{-2x_j})/\mathbb{Q}_2(\sqrt{d})$, $\mathbb{Q}_2(\sqrt{d}, \sqrt{6x_j})/\mathbb{Q}_2(\sqrt{d})$ and $\mathbb{Q}_2(\sqrt{d}, \sqrt{x_j})/\mathbb{Q}_2(\sqrt{d})$ are all unramified. Hence $K(\sqrt{\gamma_j})/K$ is unramified. Therefore, $\{-2, q_1^*, \dots, q_{n-1}^*, \gamma_1, \dots, \gamma_m\}$ is a set of representatives of Δ/K^{*2}. $\square$

4 The case $K = \mathbb{Q}(\sqrt{-1}, \sqrt{d})$

In this section $K = \mathbb{Q}(\sqrt{-1}, \sqrt{d})$, $K_0 = \mathbb{Q}(\sqrt{-1})$. We write

$$d = \pm \prod_{j=1}^{n} q_j \quad \text{or} \quad d = \pm 2 \prod_{j=1}^{n} q_j \tag{4.1}$$

with $q_1, \dots, q_n$ being distinct odd primes such that $q_j \equiv 1 \bmod 4$ if $1 \leqslant j \leqslant m$ (i.e., $(\frac{-1}{q_j}) = 1$) and $q_j \equiv 3 \bmod 4$ if $m+1 \leqslant j \leqslant n$. We assume $q_1 \equiv 5 \bmod 8$ if there exists j $(1 \leqslant j \leqslant m)$ such that $q_j \equiv 5 \bmod 8$. Therefore $q_1 \equiv 1 \bmod 8$ if and only if $q_j \equiv 1 \bmod 8$ for all $1 \leqslant j \leqslant m$. For $1 \leqslant j \leqslant m$, choose $(x_j, y_j) \equiv (1, 0) \bmod 2$ to be a primitive solution of $q_j = x^2 + y^2$ (resp. $q_1 q_j = x^2 + y^2$) if $q_j \equiv 1 \bmod 8$ (resp. $j > 1$ and $q_j \equiv 5 \bmod 8$). Then in both cases, $y_j \equiv 0 \bmod 4$. Set

$$\alpha_j = x_j + y_j\sqrt{-1}. \tag{4.2}$$

Lemma 4.1. *Assume notation as above, then we have the following table*:

d	q_1	s	$r_2(\Delta/K^{*2})$
$\pm 1 \bmod 4$	$1 \bmod 8$	$m+n$	$m+n-1$
	$5 \bmod 8$	$m+n$	$m+n-2$
$2 \bmod 4$	$1 \bmod 8$	$m+n+1$	$m+n$
	$5 \bmod 8$	$m+n+1$	$m+n-1$

Proof. For $d \equiv \pm 1 \bmod 4$, there are $m+n$ finite primes ramified in K/K_0, and for $d \equiv 2 \bmod 4$, there are $m+n+1$ finite primes ramified in K/K_0. We thus get the values of s in the table.

To know $r_2(\Delta/K^{*2})$, by Proposition 1.2, it suffices to know $U_{K_0}/U_{K_0} \cap NK$. Since $U_{K_0} = \{\pm 1, \pm\sqrt{-1}\}$ and $-1 = N_{K/K_0}(\sqrt{-1}) \in NK$, we just have to check if $\sqrt{-1} \in NK$ or not, equivalently, if $(\sqrt{-1}, d)_{\mathfrak{p}} = 1$ for every prime $\mathfrak{p}$ of K_0 which ramified in K. For $1 \leqslant j \leqslant m$, q_j splits in K_0. For every prime $\mathfrak{q}_j$ above q_j, we have

$$(\sqrt{-1}, d)_{\mathfrak{q}_j} = (\sqrt{-1})^{\frac{q_j - 1}{2}} = \begin{cases} 1, & \text{if } q_j \equiv 1 \bmod 8, \\ -1, & \text{if } q_j \equiv 5 \bmod 8. \end{cases}$$

For $m+1 \leqslant j \leqslant n$, q_j is inert in K_0. Let $\mathfrak{q}_j$ be the prime above q_j. By Lemma 3.3 of [7], we have

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

We know that 2 is ramified in K_0. Let $\mathfrak{p}$ be the prime above 2 in K_0, then the product formula gives $(\sqrt{-1}, d)_{\mathfrak{p}} = 1$. We thus get the values of $r_2(\Delta/K^{*2})$ in the table. □

Theorem 4.2. *Assume d as above, then the Hilbert genus field of $K = \mathbb{Q}(\sqrt{-1}, \sqrt{d})$ is given by the following table*:

Case	d	q_1	*Hilbert genus field E*
I	$\pm 1 \bmod 4$	$1 \bmod 8$	$\mathbb{Q}(\sqrt{-1}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$
		$5 \bmod 8$	$\mathbb{Q}(\sqrt{-1}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_m})$
II	$2 \bmod 4$	$1 \bmod 8$	$\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$
		$5 \bmod 8$	$\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_m})$

Proof of Case I. (1) If $q_1 \equiv 1 \bmod 8$, then by Lemma 4.1, $r_2(\Delta/K^{*2}) = m+n-1$, and so $r_2(D_K/K^{*2}) = m+n+1$. Similar to the proof of Theorem 3.4, Case I, we see that

$$\{2, q_1, \ldots, q_{n-1}, \alpha_1, \ldots, \alpha_m, \eta\} \tag{4.3}$$

is a set of representatives of D_K/K^{*2}, where $\eta = x + y\sqrt{d} \in K$ with $N_{K/K_0}(\eta) = -1$.

We now show Δ/K^{*2} is generated by $\{q_1, \ldots, q_{n-1}, \alpha_1, \ldots, \alpha_m\}$. It suffices to show that $K(\sqrt{\alpha_j})/K$, $1 \leqslant j \leqslant m$, are unramified extensions. By Proposition 1.1(1), we only need to show that they are unramified at the dyadic prime of K.

Let $\mathcal{D}$ be a dyadic prime of K and $\mathcal{D} \cap \mathcal{O}_{K_0} = D$. Since $q_j \equiv 1 \bmod 8$, $4 \mid y_j$, in the local field $K_{0,D} = \mathbb{Q}_2(\sqrt{-1})$, $\alpha_j = x_j + y_j\sqrt{-1} = x_j + y_j + (-1+\sqrt{-1})y_j \equiv x_j + y_j \bmod \pi^5$, where $\pi = -1+\sqrt{-1}$ is a uniformizer of $\mathbb{Q}_2(\sqrt{-1})$. Since $x_j + y_j \equiv \pm 1, \pm 3 \bmod \pi^5$, by Lemma 2.2, $K_{0,D}(\sqrt{\alpha_j})/K_{0,D}$ is unramified. Thus $K_{\mathcal{D}}(\sqrt{\alpha_j})/K_{\mathcal{D}}$ is also unramified.

(2) If $q_1 \equiv 5 \bmod 8$, similarly, we see that $\{q_1, \ldots, q_{n-1}, \alpha_2, \ldots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}. □

Proof of Case II. (1) If $q_1 \equiv 1 \bmod 8$, then by Lemma 4.1, $r_2(\Delta/K^{*2}) = m+n$. Since $K(\sqrt{2})/K$ is unramified at the dyadic primes, we see that $\{2, q_1, \ldots, q_{n-1}, \alpha_1, \ldots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}.

(2) If $q_1 \equiv 5 \bmod 8$, then $r_2(\Delta/K^{*2}) = m+n-2$. It is clear that $\{2, q_1, \ldots, q_{n-1}, \alpha_2, \ldots, \alpha_m\}$ is a set of representatives of Δ/K^{*2}. □

5 The case $K = \mathbb{Q}(\sqrt{-2}, \sqrt{d})$

In this section, $K_0 = \mathbb{Q}(\sqrt{-2})$, $K = \mathbb{Q}(\sqrt{-2}, \sqrt{d})$. Since $\mathbb{Q}(\sqrt{-2}, \sqrt{d}) = \mathbb{Q}(\sqrt{-2}, \sqrt{-2d})$, without loss of generality, we can assume $d \equiv 1$ or $3 \bmod 4$. We write

$$d = \pm \prod_{j=1}^{n} q_j \tag{5.1}$$

with $q_1, \ldots, q_n$ being distinct odd primes such that $q_j \equiv 1,\ 3 \bmod 8$ if $1 \leqslant j \leqslant m$ (i.e., $(\frac{-2}{q_j}) = 1$) and $q_j \equiv 5, 7 \bmod 8$ if $m+1 \leqslant j \leqslant n$. We assume $q_1 \equiv 3 \bmod 8$ if there exists j $(1 \leqslant j \leqslant m)$ such that $q_j \equiv 3 \bmod 8$. Therefore $q_1 \equiv 1 \bmod 8$ if and only if $q_j \equiv 1 \bmod 8$ for all $1 \leqslant j \leqslant m$. For $1 \leqslant j \leqslant m$, choose (x_j, y_j) to be a primitive solution of $q_j = x^2 + 2y^2$ (resp. $q_1 q_j = x^2 + 2y^2$) such that $x_j + y_j \equiv 1 \bmod 4$ if $q_j \equiv 1 \bmod 8$ (resp. $j > 1$ and $q_j \equiv 3 \bmod 8$). Set

$$\alpha_j = x_j + y_j\sqrt{-2}. \tag{5.2}$$

Lemma 5.1. *Assume notation as above, then we have the following table*:

d	q_1	s	$r_2(\Delta/K^{*2})$
1 mod 4	1 mod 8	$m+n$	$m+n-1$
	3 mod 8	$m+n$	$m+n-2$
3 mod 4	1 mod 8	$m+n+1$	$m+n$
	3 mod 8	$m+n+1$	$m+n-1$

Proof. For $d \equiv 1 \bmod 4$, there are $m+n$ finite primes ramified in K/K_0, and for $d \equiv 3 \bmod 4$, there are $m+n+1$ finite primes ramified in K/K_0. We thus get the values of s in the table.

To know $r_2(\Delta/K^{*2})$, by Proposition 1.2, it suffices to know $U_{K_0}/U_{K_0} \cap NK$. Since $U_{K_0} = \{\pm 1\}$, we just have to check if $-1 \in NK$, equivalently, if $(-1, d)_{\mathfrak{p}} = 1$ for every prime $\mathfrak{p}$ of K_0 which ramified in K.

For $1 \leqslant j \leqslant m$, q_j splits in K_0. For every prime $\mathfrak{q}_j$ above q_j, we have

$$(\sqrt{-1}, d)_{\mathfrak{q}_j} = (\sqrt{-1})^{\frac{q_j-1}{2}} = \begin{cases} 1, & \text{if } q_j \equiv 1 \bmod 8, \\ -1, & \text{if } q_j \equiv 3 \bmod 8. \end{cases}$$

For $m+1 \leqslant j \leqslant n$, q_j is inert in K_0. Let $\mathfrak{q}_j$ be the prime above q_j. By Lemma 3.3 of [7], we have

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

We know that 2 is ramified in K_0. Let $\mathfrak{p}$ be the prime above 2 in K_0, then the product formula gives

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

We thus get the values of $r_2(\Delta/K^{*2})$ in the table. □

Theorem 5.2. *Assume d as above, then the Hilbert genus field of $K = \mathbb{Q}(\sqrt{-2}, \sqrt{d})$ is given by the following table*:

Case	d	q_1	*Hilbert genus field E*
I	1 mod 4	1 mod 8	$\mathbb{Q}(\sqrt{-2}, \sqrt{q_1^*}, \ldots, \sqrt{q_n^*}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$
		3 mod 8	$\mathbb{Q}(\sqrt{-2}, \sqrt{q_1^*}, \ldots, \sqrt{q_n^*}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_m})$
II	3 mod 4	1 mod 8	$\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$
		3 mod 8	$\mathbb{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{q_1}, \ldots, \sqrt{q_n}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_m})$

Proof of Case I. (1) If $q_1 \equiv 1 \bmod 8$, then by Lemma 5.1, $r_2(\Delta/K^{*2}) = m+n-1$, and so $r_2(D_K/K^{*2}) = m+n+1$. Similar to the proof of Case I of Theorem 3.4, we see that

$$\{-1, q_1^*, \ldots, q_{n-1}^*, \alpha_1, \ldots, \alpha_m, \eta\} \tag{5.3}$$

is a set of representatives of D_K/K^{*2}, where $\eta = x + y\sqrt{d} \in K$ with $N_{K/K_0}(\eta) = -1$.

We now show Δ/K^{*2} is generated by $\{q_1^*, \ldots, q_{n-1}^*, \alpha_1, \ldots, \alpha_m\}$. It suffices to show that $K(\sqrt{\alpha_j})/K$, $1 \leqslant j \leqslant m$, are unramified extensions. By Proposition 1.1(1), we only need to show that they are unramified at the dyadic prime of K.

Let $\mathcal{D}$ be a dyadic prime of K and $\mathcal{D} \cap \mathcal{O}_{K_0} = D$. Let $\pi = \sqrt{-2}$ be a uniformizer of the local field $K_{0,D} = \mathbb{Q}_2(\sqrt{-2})$. Since $q_j \equiv 1 \bmod 8$, $x_j \equiv 1 \bmod 2$, $y_j \equiv 0 \bmod 2$ and recall that we choose x_j, y_j such that $x_j + y_j \equiv 1 \bmod 4$.

If $x_j \equiv 1 \bmod 4$, $y_j \equiv 0 \bmod 4$, then $\alpha_j = x_j + y_j\sqrt{-2} \equiv 1, 5 \bmod \pi^5$. Thus $K_{0,D}(\sqrt{\alpha_j})/K_{0,D}$ is unramified.

If $x_j \equiv 3 \bmod 4$, $y_j \equiv 2 \bmod 4$, then $\alpha_j = x_j + y_j\sqrt{-2} \equiv 1 + \pi^2 + \pi^3$ or $1 + \pi^2 + \pi^3 + \pi^4 \bmod \pi^5$. By Lemma 2.3, if $\alpha_j \equiv 1+\pi^2+\pi^3 \bmod \pi^5$, then $K_{0,D}(\sqrt{1+\pi^2+\pi^3}) = K_{0,D}$. If $\alpha_j \equiv 1+\pi^2+\pi^3+\pi^4 \bmod \pi^5$, then $K_{0,D}(\sqrt{1+\pi^2+\pi^3+\pi^4})/K_{0,D}$ is also unramified. Hence $K_{\mathcal{D}}(\sqrt{\alpha_j})/K_{\mathcal{D}}$ is unramified.

(2) If $q_1 \equiv 3 \bmod 8$, then $r_2(\Delta/K^{*2}) = m+n-2$. Similar to the proof of (1), we see that

$$\{q_1, \ldots, q_{n-1}, \alpha_2, \ldots, \alpha_m\}$$

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

Proof of Case II. The proof of Case II is similar to that of Case I, just recall that $K(\sqrt{-1})/K$ is an unramified extension. $\square$

Acknowledgements This work was supported by National Key Basic Research Program of China (Grant No. 2013CB834202) and National Natural Science Foundation of China (Grant No. 11171317). The authors thank Prof. Qin Yue for suggesting this problem to the second author and for his many helpful comments. The authors are grateful to the anonymous referees for useful comments and suggestions.

References

1 Bae S, Yue Q. Hilbert genus fields of real biquadratic fields. Ramanujan J, 2011, 24: 161–181
2 Conner P E, Hurrelbrink J. Class Number Parity, Ser Pure Math 8. Singapore: World Scientific, 1988
3 Herglotz G. Über einen Dirichletschen Satz. Math Z, 1922, 12: 225–261
4 Lang S. Cyclotomic Fields I and II. GTM 121. New York: Springer-Verlag, 1990
5 Neukirch J. Class Field Theory. Berlin-Heidelberg-New York-Tokyo: Springer-Verlag, 1986
6 Sime P. Hilbert class fields of real biquadratic fields. J Number Theory, 1995, 50: 154–166
7 Yue Q. The generalized Rédei matrix. Math Z, 2009, 261: 23–37
8 Yue Q. Genus fields of real biquadratic fields. Ramanujan J, 2010, 21: 17–25