ACTA ARITHMETICA
150.4 (2011)

Class groups under relative quadratic extensions

by

Qin Yue (Nanjing)

1. Introduction. Let A be a finite abelian group. We will denote by $r_{2^k}(A)$ the 2^k-rank of A. The beginning of the genus theory of quadratic extensions can be traced back to the work of C. F. Gauss (see [2, Chapter 3, Section 8]). Namely, in our current language, C. F. Gauss computed the 2-rank of the narrow class group $C_+(E)$ of a quadratic number field $E = \mathbb{Q}(\sqrt{d})$. He showed that $r_2(C_+(E)) = t - 1$, where t is the number of primes that ramify in E (see [7, p. 159]). Moreover, Gauss also obtained the following result: an ideal class $[I]$ is in $C_+(E)^2$ if and only if $|N_{E/\mathbb{Q}}(I)| \in N_{E/\mathbb{Q}}(E^*)$, where I is a fractional ideal of E and $|N_{E/\mathbb{Q}}(I)|$ is the norm of I (see [7, Theorem 145]). Then L. Rédei found a method to compute the 4-rank of $C_+(E)$, namely $r_4(C_+(E)) = t - 1 - \operatorname{rank} R_E$, where R_E is the Rédei matrix of E (see [13]). Throughout, the rank is computed over $\mathbb{F}_2$.

For a relative quadratic extension E/F, class groups have been studied by several authors (see [1, 3, 4, 8, 9, 11, 14, 15]). In particular, Gras gave a method to compute the 2-Sylow subgroup of the class group $C(E)$ (see [5, 6]).

This paper is mainly devoted to generalizing the Rédei formula to a relative quadratic extension E/F. Let $E = F(\sqrt{d})$ be a relative quadratic extension of F and $\mathrm{Gal}(E/F) = \{1, \sigma\}$ the Galois group. Then $\mathrm{Gal}(E/F)$ acts on the class group $C(E)$ of E and there is an exact sequence

$$1 \to \mathrm{Am}(E/F) \to C(E) \xrightarrow{1-\sigma} C(E)^{1-\sigma} \to 0,$$

where $\mathrm{Am}(E/F)$ is the subgroup generated by all ambiguous ideal classes of $C(E)$. There is the well-known formula

$$\#\mathrm{Am}(E/F) = h(F)\frac{2^{m-1}}{[U_F : U_F \cap N_{E/F}(E^*)]},$$

where m is the number of primes of F ramifying in E, $h(F)$ is the class number of F and U_F is the unit group of the integral ring O_F (see [1] or [10,

2010 *Mathematics Subject Classification*: Primary 11R65; Secondary 11R37.
Key words and phrases: Galois cohomology, Hilbert symbol, genus theory.

DOI: 10.4064/aa150-4-5

p. 307]). If $h(F)$ is odd, we have the well-known result

$$r_2(C(E)) = r_2(\mathrm{Am}(E/F)) = m - 1 - r_2(U_F/U_F \cap N_{E/F}(E^*)).$$

Moreover, in [15] we get a formula

$$r_4(C(E)) = m - 1 - \operatorname{rank} R_{E/F},$$

where $R_{E/F}$ is a matrix of local Hilbert symbols with coefficients in $\mathbb{F}_2$.

In this paper, we mainly generalize the above formulas provided that $C(F)$ has even order. We make the following standing assumptions: $E = F(\sqrt{d})$ is a relative quadratic extension of F, the 2-Sylow subgroup of the class group $C(F)$ is elementary, i.e. $r_2(C(F)) = s$ and $r_4(C(F)) = 0$, S is a set consisting of all infinite primes of F and some finite primes $P_1, \ldots, P_s$ of F, which ramify in E, such that the S-ideal class group $C^S(F)$ has odd order. We give two formulas for the 2-rank and the 4-rank of the class group $C(E)$:

$$r_2(C(E)) = m - 1 - r_2(U_F^S/U_F^S \cap N_{E/F}(E^*)),$$

where U_F^S is the S-unit group of F, and

$$\begin{aligned} r_4(C(E)) = m - 1 &- \operatorname{rank} R_{E/F} \\ &+ r_2(U_F^S/U_F^S \cap N_{E/F}(E^*)) - r_2(U_F/U_F \cap N_{E/F}(E^*)), \end{aligned}$$

where $R_{E/F}$ is a matrix of local Hilbert symbols with coefficients in $\mathbb{F}_2$. We call $R_{E/F}$ the *generalized Rédei matrix*. We also give algorithms to compute the values of $r_2(C(E))$ and $r_4(C(E))$.

A key step in the proofs of the formulas for the 2-rank and 4-rank of $C(E)$ is the use of the exact hexagon of Conner and Hurrelbrink. We recall this hexagon in Section 2. For convenience, we introduce the following *notation*:

E/F	relative quadratic extension,
O_F, O_E	ring of integers of F, ring of integers of E,
U_F, U_E	unit group of O_F, unit group of O_E,
U_F^S, U_E^S	S-unit group of F, S-unit group of E,
$C(F)$, $C(E)$	ideal class group of F, ideal class group of E,
$h(F)$, $h(E)$	class number of F, class number of E,
$[P]$, $[\mathcal{P}]$	class of an ideal P in $C(F)$, class of an ideal $\mathcal{P}$ in $C(E)$,
N	field norm map from E to F,
$N(x)$, NE	norm of $x \in E$ to F, set of norms from E to F,
A_2	2-Sylow subgroup of an abelian group A,
${}_2A$	subgroup of elements of order ≤ 2 of a finite abelian group A,
$r_{2^k}(A)$	2^k-rank of a finite abelian group A,
m	number of primes of F ramifying in E,
n	number of finite primes of F ramifying in E.

2. An exact hexagon. In [4, Theorem 2.3], Conner and Hurrelbrink introduced the exact hexagon which is analogous to Herbrand's theorem. Now we describe it. Let $C_2 = \mathrm{Gal}(E/F) = \{1, \sigma\}$ be the Galois group of E/F. As the class group $C(E)$ and the unit group U_E are C_2-modules, we define $H^0(C_2, C(E)) = \mathrm{Am}(E/F)/NC(E)$ and $H^0(C_2, U_E) = U_F/NU_E$. There is a homomorphism

$$d_0 : H^0(C_2, C(E)) \to H^0(C_2, U_E), \quad \mathrm{cl}(\mathcal{A}) \mapsto \mathrm{cl}(u),$$

where $\mathcal{A}$ is a fractional ideal of E, $\sigma\mathcal{A} = y\mathcal{A}$, $y \in E^*, N(y) = u \in U_F$. Moreover, there is a homomorphism between first cohomology groups:

$$d_1 : H^1(C_2, C(E)) \to H^1(C_2, O_E^*), \quad \mathrm{cl}(\mathcal{A}) \mapsto \mathrm{cl}(w),$$

where $\sigma\mathcal{A} \cdot \mathcal{A} = yO_E, y \in E^*, w = \sigma(y) \cdot y^{-1} \in U_E$ (for details, see [4, p. 2]).

Let $I(E)$ be the multiplicative group of fractional ideals of E. We now define two groups. Let

$$R^0 = \{(x, \mathcal{A}) \in F^* \times I(E) \mid x\mathcal{A}\sigma(\mathcal{A}) = O_E\},$$

a subgroup of the direct product $F^* \times I(E)$ of the multiplicative groups F^* and $I(E)$. Let

$$N^0 = \{(N(y), y^{-1}\sigma(\mathcal{B})\mathcal{B}^{-1}) \in R^0 \mid y \in E^*,\ \mathcal{B} \in I(E)\},$$

a subgroup of R^0. We define the quotient group

$$R^0(E/F) = R^0/N^0$$

and denote the class of $(x, \mathcal{A})$ by $\langle x, \mathcal{A}\rangle$.

Let

$$R^1 = \{(w, \mathcal{A}) \in U_E \times I(E) \mid N(w) = 1,\ \sigma\mathcal{A} = \mathcal{A}\},$$

a subgroup of the direct product $U_E \times I(E)$ of the multiplicative groups U_E and $I(E)$. Let

$$N^1 = \{(\sigma(y)y^{-1}, y\sigma(\mathcal{B})\mathcal{B}) \in R^1 \mid y \in E^*,\ \mathcal{B} \in I(E)\},$$

a subgroup of R^1. We define the quotient group

$$R^1(E/F) = R^1/N^1$$

and denote the class of $(w, \mathcal{A})$ by $|w, \mathcal{A}|$.

By [4, Theorem 2.3] we have

LEMMA 2.1. *There is an exact hexagon*

$$\begin{array}{ccccc} & H^1(C_2, C(E)) & \xrightarrow{d_1} & H^1(C_2, U_E) & \\ {}^{j_1}\nearrow & & & & \searrow^{i_1} \\ R^0(E/F) & & & & R^1(E/F), \\ {}^{i_0}\nwarrow & & & & \swarrow^{j_0} \\ & H^0(C_2, U_E) & \xleftarrow{d_0} & H^0(C_2, C(E)) & \end{array}$$

where $i_1 : \mathrm{cl}(w) \mapsto |w, O_E|$, $j_0 : |w, \mathcal{A}| \mapsto \mathrm{cl}(\mathcal{A})$, $i_0 : \mathrm{cl}(u) \mapsto \langle u, O_E \rangle$, $j_1 : \langle x, \mathcal{A} \rangle \mapsto \mathrm{cl}(\mathcal{A})$.

Since $C(E)$ is finite and E/F is a cyclic extension, by Herbrand's theorem (see [12, p. 13, Proposition 4.3])

$$h(C_2, C(E)) = |H^0(C_2, C(E))/H^1(C_2, C(E))| = 1.$$

By the exact hexagon,

$$r_2(H^1(C_2, U_E)) - r_2(H^0(C_2, U_E)) = r_2(R^1(E/F)) - r_2(R^0(E/F)).$$

If E/F is ramified, then, by [4, Theorems 4.2 and 5.1], $r_2(R^0(E/F)) = m - 1$ and $r_2(R^1(E/F)) = n$. Hence

$$r_2(H^1(C_2, U_E)) - r_2(H^0(C_2, U_E)) = 1 - (m - n).$$

If $P_1, \ldots, P_n$ are all finite prime ideals of F that ramify in E/F and $\mathcal{P}_1, \ldots, \mathcal{P}_n$ are finite prime ideals of E with $\mathcal{P}_i^2 = P_i O_E$, $i = 1, \ldots, n$, then, by [4, Theorem 5.1], $R^1(E/F)$ has generators

$$|1, \mathcal{P}_1|, \ldots, |1, \mathcal{P}_n|. \tag{2.1}$$

3. 2-rank. For convenience, "primes of F" will be prime ideals of F. In this paper, we always assume that $r_2(C(F)) = s$, $r_4(C(F)) = 0$, $S_f = \{P_1, \ldots, P_s\}$ is a set of some finite primes of F that ramify in E/F, S is the set consisting of all infinite primes of F and all primes in S_f, and the S-ideal class group $C^S(F)$ has odd order. Note that if $r_2(C(F)) = s$, $r_4(C(F)) = 0$, and S' is the set consisting of all infinite primes of F and all finite primes of F ramifying in E such that the S'-ideal class group $C^{S'}(E)$ has odd order, then there must exist a subset S of S' as above such that the S-ideal class group $C^S(E)$ has odd order.

Let H be the subgroup of $C(F)$ generated by the ideal classes $[P_1], \ldots, [P_s]$. Then the S-ideal class group $C^S(F) = C(F)/H$ has odd order. Without loss of generality, we always assume that $[P_1], \ldots, [P_s]$ are elements of order 2, i.e.

$$P_i^2 = x_i O_F, \quad x_i \in F^*, \ i = 1, \ldots, s, \tag{3.2}$$

and

$$C(F)_2 = H = ([P_1]) \times \cdots \times ([P_s]).$$

If necessary we replace $[P_i]$ with $[P_i]^h$, where $h = h(F)/2^s$ is odd.

In the following, we decompose H into three direct summands. For each ideal class $[P] \in H$,

$$PO_E = \mathcal{P}^2, \quad P^2 = xO_F.$$

Let H' be the subgroup of H generated by all $[P] \in H$ with $xU_F \cap NE \neq \emptyset$. Hence we can decompose H as

$$H = H' \times H_3.$$

Note that H' is unique but H_3 is not. We have two facts: $1 \neq [P] \in H'$ if and only if $xU_F \cap NE \neq \emptyset$; if $1 \neq [P] \in H_3$, then $xU_F \cap NE = \emptyset$. Moreover we can decompose H' as

$$H' = H_1 \times H_2,$$

where H_1 is the subgroup generated by all $[P] \in H'$ with $xU_F \cap NO_E \neq \emptyset$, NO_E being the set of norms from O_E to F. Note that H_1 is unique but H_2 is not. In fact, $1 \neq [P] \in H_1$ if and only if $xU_F \cap NO_E \neq \emptyset$; if $1 \neq [P] \in H_2$, then $xU_F \cap NE \neq \emptyset$ and $xU_F \cap NO_E = \emptyset$. Hence we get the following result.

LEMMA 3.1. *Let $1 \neq [P] \in H = C(F)_2$ with $P^2 = xO_F$. Then there is a decomposition of subgroups:*

$$C(F)_2 = H = H_1 \times H_2 \times H_3,$$

where $[P] \in H_1$ if and only if $xU_F \cap NO_E \neq \emptyset$; $[P] \in H_1 \times H_2$ if and only if $xU_F \cap NE \neq \emptyset$; moreover, $r_2(H_1) = s_1$, $r_2(H_2) = s_2$, $r_2(H_3) = s_3$, $r_2(C(F)) = s = s_1 + s_2 + s_3$ are determined uniquely by E/F. ■

Now we lift direct summands of H into $C(E)$. Suppose E/F is a ramified extension. Then there is a well-known exact sequence of 2-Sylow subgroups

$$0 \to \ker N \to C(E)_2 \xrightarrow{N} C(F)_2 \to 0, \tag{3.3}$$

where $N : [\mathcal{A}] \mapsto [A]$ and $N(\mathcal{A}) = A$ is an ideal of F. Let $1 \neq [P] \in H$, $P^2 = xO_F$ and $PO_E = \mathcal{P}^2$. Then $[\mathcal{P}]^4 = 1$ in $C(E)$ and $N : [\mathcal{P}] \mapsto [P]$, so the order of $[\mathcal{P}]$ is either 2 or 4 in $C(E)$.

LEMMA 3.2. *Suppose $1 \neq [P] \in H = C(F)_2$, $P^2 = xO_F$ and $PO_E = \mathcal{P}^2$. Then*

(1) *$[P] \in H_1$ if and only if $[\mathcal{P}]$ is of order 2 in $C(E)$.*
(2) *$[P] \in H_1 \times H_2$ if and only if there is an element $[\mathcal{B}] \in C(E)$ of order 2 such that $N : [\mathcal{B}] \mapsto [P]$. Moreover, $[P] \in H_2$ if and only if $[\mathcal{P}]$ is of order 4 in $C(E)$ and there is an element $[\mathcal{B}] \in C(E)$ of order 2 such that $N : [\mathcal{B}] \mapsto [P]$.*
(3) *$[P] \in H_3$ if and only if $[\mathcal{P}]$ is of order 4 in $C(E)$ and there is no $[\mathcal{B}] \in C(E)$ of order 2 such that $N : [\mathcal{B}] \mapsto [P]$.*

Proof. (1) If $[\mathcal{P}]$ is of order 2 in $C(E)$, i.e. $\mathcal{P}^2 = yO_E$, $y \in O_E$, then $xO_F = P^2 = N(\mathcal{P})^2 = N(y)O_F$ and there is $u \in U_F$ such that $N(y) = xu, y \in O_E$, i.e. $xU_F \cap NO_E \neq \emptyset$. Hence $[P] \in H_1$ by Lemma 3.1. Conversely, if $[P] \in H_1$, then $xU_F \cap NO_E \neq \emptyset$ by Lemma 3.1, i.e. there is a $y \in O_E$ such that $N(y) = xu, u \in U_F$; then $yO_E = \mathcal{P}^2 = PO_E$ as each prime ideal divisor of P ramifies in E, so $N : [\mathcal{P}] \mapsto [P]$. Hence $[\mathcal{P}]$ is of order 2 in $C(E)$.

(2) Suppose that $[P] \in H_1 \times H_2$, i.e. $xU_F \cap NE \neq \emptyset$ by Lemma 3.1, so there is $y \in E^*$ such that $N(y) = xu, u \in U_F$. For all finite primes $\mathcal{Q}$ of E, we have $v_{\mathcal{Q}}(y) + v_{\mathcal{Q}}(\sigma(y)) = v_{\mathcal{Q}}(x)$, where $v_{\mathcal{Q}}$ is the normalized exponential

valuation belonging to $\mathcal{Q}$. Hence

$$yO_E = \mathcal{P}^2 \frac{\mathcal{B}_1}{\sigma\mathcal{B}_1}, \quad \sigma(y)O_E = \mathcal{P}^2 \frac{\sigma\mathcal{B}_1}{\mathcal{B}_1}, \quad [\mathcal{P}^2] = \frac{[\mathcal{B}_1]}{\sigma[\mathcal{B}_1]},$$

where $\mathcal{B}_1$ is an integral ideal of O_E. Let $\mathcal{B}_1\sigma\mathcal{B}_1 = B_1 O_E$, where B_1 is an integral ideal of O_F. In $C(F)$, there is $[P_1] \in H$ such that $[P_1][B_1] = [B_2]^2 \in C(F)^2$, i.e. $[B_1] = [B_2]^2[P_1]$. Hence in $C(E)$, $[\mathcal{B}_1]\sigma[\mathcal{B}_1] = [B_1 O_E] = [B_2\mathcal{P}_1]^2$, where $\mathcal{P}_1^2 = P_1 O_E$. Set

$$\mathcal{B} = \mathcal{P}\frac{\mathcal{B}_1}{B_2\mathcal{P}_1}.$$

Then $[\mathcal{B}]^2 = [\mathcal{P}]^2 \frac{[\mathcal{B}_1]^2}{[B_2\mathcal{P}_1]^2} = 1$ in $C(E)$ and $N([\mathcal{B}]) = N([\mathcal{P}]) = [P]$, so $[\mathcal{B}]$ is of order 2 in $C(E)$. Conversely, if there is a $[\mathcal{B}] \in C(E)$ of order 2 such that $N([\mathcal{B}]) = [P]$, then $\mathcal{B}^2 = yO_E$, $y \in E^*$, and $N(y)O_F = (N\mathcal{B})^2 = (kP)^2 = k^2 x O_F$, $k \in F^*$. Hence there is a $u \in U_F$ such that $N(y/k) = xu$, i.e. $xU_F \cap NE \neq \emptyset$. Hence $[P] \in H_1 \times H_2$ by Lemma 3.1. The second part of (2) is clear from (1) and the first part of (2).

(3) This is straightforward from (1) and (2). ∎

By Lemmas 3.1 and 3.2, we have a natural lift of $C(F)_2$ to $C(E)$.

Corollary 3.1. *Let* $K_i = \{[\mathcal{P}] \in C(E) \mid \mathcal{P}^2 = PO_E, [P] \in H_i\}$, $i = 1, 2, 3$. *Then*

$$K = K_1 \times K_2 \times K_3, \quad K_1 \cong H_1, \quad K_2/K_2^2 \cong H_2, \quad K_3/K_3^2 \cong H_3,$$

where K_1 *is* 2*-elementary abelian and* $r_4(K_i) = r_2(K_i) = r_2(H_i)$, $i = 2, 3$. ∎

We know that $i : C(F)_2 \to C(E)_2, [P] \mapsto [PO_E]$, is a homomorphism of groups.

Lemma 3.3.

(1) *There is an exact sequence*

$$0 \to H_1 \to C(F)_2 \xrightarrow{i} C(E)_2.$$

(2) *There is a decomposition into subgroups*

$$C(E)_2 = K_1 \times K_2' \times K_3 \cdot \ker N,$$

where $K_2' \cong H_2$ *and* $K_2^2, K_3^2 \subset \ker N$.

Proof. (1) This is clear from Lemma 3.2.

(2) We consider the exact sequence of (3.3). By Lemma 3.2(1), there is an isomorphism of groups $j_1 : H_1 \to K_1$, $[P] \mapsto [\mathcal{P}]$, where $PO_E = \mathcal{P}^2$. By Lemma 3.2(2), for each $1 \neq [P] \in H_2$, there is a $[\mathcal{B}] \in C(E)$ of order 2 such that $N : [\mathcal{B}] \mapsto [P]$; let K_2' be the subgroup of $C(E)$ generated by all such $[\mathcal{B}]$. Then $j_2 : H_2 \to K_2', [P] \mapsto [\mathcal{B}]$, is an isomorphism. Hence there are subgroups K_1 and K_2' such that $C(E)_2 = K_1 \times K_2' \times N^{-1}(H_3)$, where $K_1 \cong H_1$, $K_2' \cong H_2$, $N^{-1}(H_3) = K_3 \cdot \ker N$ and $K_2^2, K_3^2 \subset \ker N$. ∎

LEMMA 3.4. *Let $C^S(E) = C(E)/K$ be the S-ideal class group of E. Suppose that the S-ideal class group $C^S(F)$ of F has odd order. Then $r_2(C^S(E)) = m-1-r_2(U_F^S/U_F^S\cap NE)$, where U_F^S is the S-unit group of F.*

Proof. In the exact hexagon, if we replace $C(E)$ and U_E with $C^S(E)$ and U_E^S, respectively, we also obtain an exact hexagon (see [4]). Suppose $C^S(F)$ has odd order. Then $\operatorname{im} d_1 = 1$ and there is an exact sequence (see [4, Lemma 9.1])

$$\to H^0(C_2, U_E^S) \xrightarrow{i_0} R^{0S}(E/F) \xrightarrow{j_1} H^1(C_2, C^S(E)) \to 1.$$

We know (see [4, p. 24]) that $\operatorname{im} i_0 \cong U_F^S/U_F^S\cap NE)$, $r_2(R^{0S}(E/F)) = m-1$, and $r_2(C^S(E)) = r_2(H^1(C_2, C^S(E)))$ since the order of $C^S(F)$ is odd. Hence

$$r_2(C^S(E)) = m-1-r_2(U_F^S/U_F^S\cap NE). \ \blacksquare$$

THEOREM 3.1.

(1) $r_2(C(E)) = s+m-1-r_2(U_F^S/U_F^S\cap NE)$, *where U_F^S is the S-ideal class group of F.*

(2) $r_2(K_3) = s_3 = r_2(U_F^S/U_F^S\cap NE) - r_2(U_F/U_F\cap NE)$.

Proof. Let $\operatorname{Am}(E/F) = \{[\mathcal{P}] \in C(E) \mid \sigma[\mathcal{P}] = [\mathcal{P}]\}$ be the subgroup generated by all ambiguous ideal classes of $C(E)$. By [10], we have the well-known formula

$$\#\operatorname{Am}(E/F) = h(F)\frac{2^{m-1}}{[U_F : U_F\cap NE]}.$$

Since $K = K_1\times K_2\times K_3 \subset \operatorname{Am}(E/F)_2$, there is an exact sequence

$$0\to \operatorname{Am}\to \operatorname{Am}(E/F)_2 \xrightarrow{N} H\to 0,$$

where Am is a 2-elementary subgroup. Hence

$$\operatorname{Am}(E/F)_2 = K_1\times K_2\times K_3\times \operatorname{Am}_1, \quad \operatorname{Am}_1\subset \operatorname{Am}, \tag{3.4}$$

and

$$r_2(\operatorname{Am}(E/F)) = m-1+s_1-r_2(U_F/U_F\cap NE).$$

On the other hand, by Lemma 3.3(2) it is clear that

$${}_2\operatorname{Am}(E/F) = K_1\times {}_2\ker N = K_1\times {}_2(K_3\cdot \ker N)$$

and ${}_2(C(E)) = K_2'\times {}_2\operatorname{Am}(E/F)$. Hence

$$\begin{aligned} r_2(C(E)) &= r_2(K_2') + r_2(\operatorname{Am}(E/F)) \\ &= s_1+s_2+m-1-r_2(U_F/U_F\cap NE), \\ r_2(\ker N) &= m-1-r_2(U_F/U_F\cap NE). \end{aligned} \tag{3.5}$$

Now we investigate the S-ideal class group $C^S(E) = C(E)/K$, where $K = K_1\times K_2\times K_3$. There is an exact sequence

$$0\to K_1\times K_2\times K_3\to C(E)\to C^S(E)\to 0.$$

By tensoring the above exact sequence with $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, we obtain the exact sequence

$$0 \to (K_1 \times K_2 \times K_3) \otimes \mathbb{F}_2 \xrightarrow{i\otimes 1} C(E) \otimes \mathbb{F}_2 \to C^S(E) \otimes \mathbb{F}_2 \to 0.$$

In fact, $C(E) \otimes \mathbb{F}_2 \cong C(E)/C(E)^2$ and $K_i \otimes \mathbb{F}_2 \cong K_i/K_i^2$, $i = 2, 3$. For each $[\mathcal{P}] \in K_i$ of order 4, $i = 2, 3$, we have $[\mathcal{P}] \notin C(E)^2$ by (3.3), hence $i \otimes 1$ is injective. Then

$$r_2(C(E)) = r_2(C^S(E)) + r_2(K). \tag{3.6}$$

By Lemma 3.4 and (3.6),

$$r_2(C(E)) = s + m - 1 - r_2(U_F^S/U_F^S \cap NE). \tag{3.7}$$

This proves (1). By (3.5), (3.7), Corollary 3.1 and $s = s_1 + s_2 + s_3$, we have

$$r_2(K_3) = s_3 = r_2(U_F^S/U_F^S \cap NE) - r_2(U_F/U_F \cap NE).$$

This proves (2). ∎

We now give an algorithm to compute $r_2(U_F/U_F \cap NE)$ and $r_2(K_3) = s_3$. Let $r_2(U_F/U_F^2) = l$, $U_F/U_F^2 = (\{\overline{u}_1, \ldots, \overline{u}_l\})$. For each prime Q of F which splits or is inert in E, the local Hilbert symbol $(u_i, d)_Q$ is 1. Thus, by Hasse's norm theorem, we only need to investigate the local Hilbert symbols $(u_i, d)_P$ for all primes of F which ramify in E. Let $P_1, \ldots, P_m$ be all primes (finite or infinite) of F which ramify in E. For convenience, we construct a matrix of local Hilbert symbols over $\mathbb{F}_2$:

$$M_U = \begin{pmatrix} (u_1, d)_{P_1} & \cdots & (u_1, d)_{P_m} \\ \cdots & \cdots & \cdots \\ (u_l, d)_{P_1} & \cdots & (u_l, d)_{P_m} \end{pmatrix}.$$

We replace the 1's with 0's, and the -1's with 1's. Then

$$r_2(U_F/U_F \cap NE) = \operatorname{rank} M_U.$$

In order to compute $r_2(K_3)$, as above we also construct a matrix of local Hilbert symbols over $\mathbb{F}_2$:

$$M_S = \begin{pmatrix} (x_1, d)_{P_1} & \cdots & (x_1, d)_{P_m} \\ \cdots & \cdots & \cdots \\ (x_s, d)_{P_1} & \cdots & (x_s, d)_{P_m} \\ (u_1, d)_{P_1} & \cdots & (u_1, d)_{P_m} \\ \cdots & \cdots & \cdots \\ (u_l, d)_{P_1} & \cdots & (u_l, d)_{P_m} \end{pmatrix},$$

where $x_1, \ldots, x_s$ are defined in (3.2). If the first row of M_S cannot be linearly represented by the last l rows of M_S, then $x_1U_F \cap NE = \emptyset$. Hence

$$r_2(K_3) = \operatorname{rank} M_S - \operatorname{rank} M_U.$$

4. 4-rank. In this section, we investigate the 4-rank of $C(E)$. By (3.3) we have

$$r_4(C(E)) = r_2({}_2C(E) \cap C(E)^2) = r_2({}_2\ker N \cap C(E)^2).$$

We will construct all elements of ${}_2\ker N$ to compute $r_2({}_2\ker N \cap C(E)^2)$.

First we investigate $H^0(C_2, C(E)) = \mathrm{Am}(E/F)/N(C(E))$. It is clear that $H^0(C_2, C(E)) = \mathrm{Am}(E/F)_2/N(C(E))_2$. By (3.4), we have

$$\mathrm{Am}(E/F)_2 = K_1 \times K_2 \times K_3 \times \mathrm{Am}_1, \quad {}_2\ker N = K_2^2 \times K_3^2 \times \mathrm{Am}_1,$$

where Am_1 is a 2-elementary subgroup of $\mathrm{Am}(E/F)_2$. Since $N(C(E))_2 = K_2^2 \times K_3^2$,

$$H^0(C_2, C(E)) = K_1 \times K_2/K_2^2 \times K_3/K_3^2 \times \mathrm{Am}_1\,.$$

By the exact hexagon, there is an exact sequence

(4.8)
$$H^1(C_2, U_E) \xrightarrow{i_1} R^1(E/F) \xrightarrow{j_0} H^0(C_2, C(E)) \xrightarrow{d_0} H^0(C_2, U_E) \xrightarrow{i_0} R^0(E/F),$$

where $r_2(R^1(E/F)) = n$.

For convenience, we assume that $\{P_1, \ldots, P_s, P_{s+1}, \ldots, P_n\}$ is the set of all finite prime ideals of F which ramify in E, $H_1 = ([P_1], \ldots, [P_{s_1}])$, $H_2 \times H_3 = ([P_{s_1+1}], \ldots, [P_s])$. For each $[P_j] \in C(F)$ $(s+1 \le j \le n)$, without loss of generality, we assume that there is a $[P_j'] \in H$ such that $[P_j][P_j'] = 1$. If necessary we can replace $[P_j]$ with $[P_j^h]$, $h = h(F)/2^s$ odd. Let

$$P_iO_E = \mathcal{P}_i^2, \quad i = 1, \ldots, n,$$

$$\text{(4.9)} \qquad P_jP_j' = x_jO_F, \quad (\mathcal{P}_j\mathcal{P}_j')^2 = P_jP_j'O_E, \quad j = 1, \ldots, n,$$

where we take $\mathcal{P}_j = \mathcal{P}_j'$ if $j = 1, \ldots, s$. By [2], we know that

$$R^1(E/F) = (|1, \mathcal{P}_1|, \ldots, |1, \mathcal{P}_s|, |1, \mathcal{P}_{s+1}\mathcal{P}_{s+1}'|, \ldots, |1, \mathcal{P}_n\mathcal{P}_n'|).$$

We investigate the inverse image of d_0 in (4.8). We know that $d_0 : H^0(C_2, C(E)) \to H^0(C_2, U_E)$, $\mathrm{cl}(\mathcal{A}) \mapsto \mathrm{cl}(u)$, where $\sigma\mathcal{A} = y\mathcal{A}$ and $N(y) = u \in U_F \cap NE$. Conversely, let $r_2(U_F/U_F^2) = l$ and $r_2((U_F \cap NE)/U_F^2) = t$, i.e.

$$\text{(4.10)} \qquad U_F/U_F^2 = (\overline{u}_1) \times \cdots \times (\overline{u}_t) \times (\overline{u}_{t+1}) \times \cdots \times (\overline{u}_l)$$

and

$$(U_F \cap NE)/U_F^2 = (\overline{u}_1) \times \cdots \times (\overline{u}_t).$$

If $N(y_i) = u_i \in U_F \cap NE$, then $y_iO_E = \frac{\sigma\mathcal{B}_i}{\mathcal{B}_i}$ by the Hilbert–Noether theorem, i.e. $H^1(C_1, I(E)) = 1$. Since $N(\mathcal{B}_i) = B_i$ is an ideal of F, there is an ideal class $[P_i''] \in C(F)_2$ such that $[B_i][P_i''] \in C(F)^2$. Hence, without loss of generality, we assume that $[B_i][P_i''] = 1$; if necessary we replace y_i with y_i^h, $h = h(F)/2^s$, so there are $v_i \in F^*$ such that $B_i P_i'' = v_i O_F$, $i = 1, \ldots, t$. Let $\mathcal{P}_i''^2 = P_i'' O_E$. Then

$$(4.11) \qquad y_i O_E = \frac{\sigma(\mathcal{B}_i \mathcal{P}_i'')}{\mathcal{B}_i \mathcal{P}_i''}, \quad \mathcal{B}_i \mathcal{P}_i'' \sigma(\mathcal{B}_i \mathcal{P}_i'') = v_i O_E, \quad i = 1, \ldots, t,$$

and $d_0 : \mathrm{cl}(\mathcal{B}_i \mathcal{P}_i'') \mapsto \mathrm{cl}(u_i)$. Hence by (4.8),

$$\mathrm{Am}(E/F)_2 = ([\mathcal{P}_1], \ldots, [\mathcal{P}_s], [\mathcal{P}_{s+1}\mathcal{P}_{s+1}'], \ldots, [\mathcal{P}_n \mathcal{P}_n'], [\mathcal{B}_1 \mathcal{P}_1''], \ldots, [\mathcal{B}_t \mathcal{P}_t''])$$

and

$${}_2\ker N = ([\mathcal{P}_{s_1+1}^2], \ldots, [\mathcal{P}_s^2], [\mathcal{P}_{s+1}\mathcal{P}_{s+1}'], \ldots, [\mathcal{P}_n \mathcal{P}_n'], [\mathcal{B}_1 \mathcal{P}_1''], \ldots, [\mathcal{B}_t \mathcal{P}_t'']).$$

We define $\mathrm{Ker}\, N = \{[\mathcal{A}] \in C(E) \mid [\mathcal{A}]\sigma[\mathcal{A}] = 1\}$, $I_{C_2}(C(E)) = \{\sigma[\mathcal{A}]/[\mathcal{A}] \mid [\mathcal{A}] \in C(E)\}$ and $H^1(C_2, C(E)) = \mathrm{Ker}\, N / I_{C_2}(C(E))$.

LEMMA 4.1.

(1) $(\mathrm{Ker}\, N)_2 = \ker N \times K_1$, *where* $\ker N$ *is defined as* (3.3).
(2) ${}_2C(E) \cap C(E)^2 = {}_2\ker N \cap C(E)^2 = ({}_2\ker N \cap I_{C_2}(C(E))) \times K_3^2$ *and* $K_3^2 \cap I_{C_2}(C(E)) = 1$. *Moreover* ${}_2\ker N / ({}_2\ker N \cap I_{C_2}(C(E))) \cong {}_2\ker N / ({}_2\ker N \cap C(E)^2) \times K_3^2$.

Proof. (1) By Lemma 3.3, it is clear that $K_1 \times \ker N \subset (\mathrm{Ker}\, N)_2$. Conversely, if $[\mathcal{A}] \in (\mathrm{Ker}\, N)_2$, then $[\mathcal{A}]\sigma[\mathcal{A}] = 1$ in $C(E)$. On the other hand, $N(\mathcal{A}) = A$ is an ideal of F, so there is a $[P] \in H$ such that $[A][P] = 1$ in $C(F)$. Then for $\mathcal{P}^2 = PO_E$, $[\mathcal{A}]\sigma[\mathcal{A}][\mathcal{P}^2] = 1$ and $[\mathcal{P}^2] = 1$ in $C(E)$. Hence $[\mathcal{A}][\mathcal{P}] \in \ker N$ and $[\mathcal{P}] \in K_1 \times K_2^2 \times K_3^2 \subset K_1 \times \ker N$, so $[\mathcal{A}] \in K_1 \times \ker N$.

(2) By Lemma 3.3(2), we have ${}_2C(E) \cap C(E)^2 = {}_2\ker N \cap C(E)^2$. Let

$$\frac{\sigma[\mathcal{A}]}{[\mathcal{A}]} = \frac{(\sigma[\mathcal{A}])^2}{[AO_E]} \in I_{C_2}(C(E)),$$

where $N(\mathcal{A}) = A$ is an ideal of O_F. Then since $C(F)_2$ is 2-elementary there is a $[P] \in H$ such that $[PA] \in C(F)^2$, $[PAO_E] \in C(E)^2$ and $[AO_E] \in C(E)^2$, where $[PO_E] = [\mathcal{P}^2] \in C(E)^2$. Hence $I_{C_2}(C(E)) \subset C(E)^2$ and ${}_2\ker N \cap I_{C_2}(C(E)) \subset {}_2\ker N \cap C(E)^2$. Conversely, let $[\mathcal{A}] = [\mathcal{B}]^2 \in {}_2\ker N \cap C(E)^2$ and $N(\mathcal{B}) = B$, an ideal of F. Then there is an ideal class $[P] \in H$ such that $[BP]$ has odd order. On the other hand, since $[\mathcal{A}] = [\mathcal{B}]^2 \in {}_2\ker N$, we have $1 = N([\mathcal{A}]) = N([\mathcal{B}])^2 = [B]^2$ and $N([\mathcal{B}][\mathcal{P}]) = [B][P]$ has even order, where $PO_E = \mathcal{P}^2$. Hence $N([\mathcal{B}P]) = [BP] = 1$ in $C(F)$ and

$$[\mathcal{A}] = [\mathcal{B}\mathcal{P}^2]^2 = \frac{[\mathcal{B}P]}{\sigma[\mathcal{B}P]}[\mathcal{P}^2].$$

By the proof of Lemma 3.2, we know that $[\mathcal{P}^2] \in K_2^2$ if and only if $[\mathcal{P}^2] \in I_{C_2}(C(E))$. Therefore ${}_2\ker N \cap C(E)^2 = ({}_2\ker N \cap I_{C_2}(C(E))) \times K_3^2$. We have proved the first part of (2).

Moreover, there is an exact sequence

$$0 \to K_3^2 \to {}_2\ker N/{}_2\ker N \cap I_{C_2}(C(E)) \to {}_2\ker N/{}_2\ker N \cap C(E)^2 \to 0,$$

so we have proved the second part. ∎

Now we calculate $r_4(C(E))$. By the exact hexagon, we have

$$\to H^0(C_2, U_E) \xrightarrow{i_0} R^0(E/F) \xrightarrow{j_1} H^1(C_2, C(E)) \to . \tag{4.12}$$

Let R be the subgroup of $R^0(E/F)$ generated by $\{\langle x_{s_1+s_2+1}, \mathcal{P}_{s_1+s_2+1}^2\rangle, \ldots, \langle x_n, \mathcal{P}_n\mathcal{P}_n'\rangle, \langle v_1, \mathcal{B}_1\mathcal{P}_1''\rangle, \ldots, \langle v_t, \mathcal{B}_t''\mathcal{P}_t''\rangle, \langle u_{t+1}, O_E\rangle, \ldots, \langle u_l, O_E\rangle\}$, where x_i, u_j, v_k are given in (4.9)–(4.11). By (4.12), there is an exact sequence

$$0 \to \frac{U_F}{U_F \cap NE} \to R \to \frac{{}_2\ker N}{{}_2\ker N \cap I_{C_2}(C(E))} \to 0. \tag{4.13}$$

Hence by Lemma 4.1(2),

$$\begin{aligned} r_2({}_2\ker N/{}_2\ker N \cap C(E)^2) &= r_2({}_2\ker N/{}_2\ker N \cap I_{C_2}(C(E))) - r_2(K_3) \\ &= r_2(R) - r_2(U_F/U_F \cap NE) - r_2(K_3). \end{aligned}$$

Now we give an algorithm to compute $r_2(R)$. Let $P_1, \ldots, P_n, \ldots, P_m$ be all finite and infinite primes of F which ramify in E. We construct a matrix of local Hilbert symbols

$$R_{E/F} = \begin{pmatrix} (x_{s_1+s_2+1}, d)_{P_1} & \cdots & (x_{s_1+s_2+1}, d)_{P_n} & \cdots & (x_{s_1+s_1+1}, d)_{P_m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (x_n, d)_{P_1} & \cdots & (x_n, d)_{P_n} & \cdots & (x_n, d)_{P_m} \\ (v_1, d)_{P_1} & \cdots & (v_1, d)_{P_n} & \cdots & (v_1, d)_{P_m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (v_t, d)_{P_1} & \cdots & (v_t, d)_{P_n} & \cdots & (v_t, d)_{P_m} \\ (u_{t+1}, d)_{P_1} & \cdots & (u_{t+1}, d)_{P_n} & \cdots & (u_{t+1}, d)_{P_m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (u_l, d)_{P_1} & \cdots & (u_l, d)_{P_n} & \cdots & (u_l, d)_{P_m} \end{pmatrix}.$$

We consider the above matrix with coefficients in $\mathbb{F}_2$ by replacing the 1's by 0's and the -1's by 1's. With this notation,

$$r_2(R) = \operatorname{rank} R_{E/F}.$$

Hence by (3.5),

$$\begin{aligned} r_4(C(E)) = r_2({}_2\ker N \cap C(E)^2) &= r_2(\ker N) - r_2({}_2\ker N/{}_2\ker N \cap C(E)^2) \\ &= m - 1 - r_2(U_F/U_F \cap NE) \\ &\quad - [r_2(R) - r_2(U_F/U_F \cap NE) - r_2(K_3)] \\ &= m - 1 - \operatorname{rank} R_{E/F} + r_2(K_3). \end{aligned}$$

By Theorem 3.1, we have

THEOREM 4.1.
$r_4(C(E)) = m - 1 - \operatorname{rank} R_{E/F} + r_2(U_F^S/U_F^S \cap NE) - r_2(U_F/U_F \cap NE)$. ∎

5. Some examples. Let $F = \mathbb{Q}(\sqrt{-d_1})$ be an imaginary quadratic number field and $D = p_1^* \ldots p_{s+1}^*$ the discriminant of F, where $p_i^* = (-1)^{(p_i-1)/2} p_i$ if p_i is an odd prime and $p_{s+1}^* = -4, 8$, or -8 if $2 \mid D$. We have the $(s+1) \times (s+1)$ Rédei matrix of Legendre or Kronecker symbols over $\mathbb{F}_2$,

$$R_F = \begin{pmatrix} \left(\frac{D/p_1^*}{p_1}\right) & \left(\frac{p_2}{p_1}\right) & \cdots & \left(\frac{p_{s+1}}{p_1}\right) \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ \left(\frac{p_1}{p_s}\right) & \left(\frac{p_2}{p_s}\right) & \cdots & \left(\frac{p_{s+1}}{p_s}\right) \\ \left(\frac{p_{s+1}^*}{p_1}\right) & \left(\frac{p_{s+1}^*}{p_2}\right) & \cdots & \left(\frac{D/p_{s+1}^*}{p_{s+1}}\right) \end{pmatrix}.$$

Note that we replace the 1's with 0's and the -1's with 1's. Then

$$r_4(C(F)) = s - \operatorname{rank} R_F.$$

Let R_F' be the $s \times (s+1)$ matrix obtained by deleting the $(s+1)$th row of R_F. It is clear that $r_4(C(F)) = 0$ if and only if $\operatorname{rank} R_F = \operatorname{rank} R_F' = s$.

Let $E = F(\sqrt{d}), d \in \mathbb{Z}$, be a relative quadratic extension of F. Let $F_0 = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Suppose $S_f' = \{q_1, \ldots, q_r, q_{r+1}, \ldots, q_{r+r'}\}$ is the set of all prime numbers of $\mathbb{Q}$ which ramify in F_0, $q_1, \ldots, q_r$ split in F, and $q_{r+1}, \ldots, q_{r+r'}$ are inert in F. Consider the following matrix of Legendre symbols over $\mathbb{F}_2$:

$$M_E = \begin{pmatrix} \left(\frac{q_1}{p_1}\right) & \cdots & \left(\frac{q_r}{p_1}\right) \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots} \\ \left(\frac{q_1}{p_s}\right) & \cdots & \left(\frac{q_r}{p_s}\right) \end{pmatrix}.$$

Suppose S' is the set consisting of all infinite primes of F and all finite primes of F ramifying in E. Then $\#S' = n + 1 = 2r + r' + 1$. By [14, Proposition 2.2], we have

LEMMA 5.1. *If $r_4(C(F)) = 0$, then the S'-ideal class group $C^{S'}(F)$ has odd order if and only if* $\operatorname{rank} M_E = s$. ∎

In fact, if $\operatorname{rank} M_E = s$, then $s \le r$. Without loss of generality, consider the submatrix of M_E:

$$M_E' = \begin{pmatrix} \left(\frac{q_1}{p_1}\right) & \cdots & \left(\frac{q_s}{p_1}\right) \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots} \\ \left(\frac{q_1}{p_s}\right) & \cdots & \left(\frac{q_s}{p_s}\right) \end{pmatrix}$$

with $\operatorname{rank} M_E' = s$. Let

$$q_i O_F = Q_i Q_i', \quad i = 1, \ldots, s,$$

$S_f = \{Q_1, \ldots, Q_s\}$, and S the set including the infinite prime and all primes in S_f. Then $C^S(F)$ has odd order (for details, see [14]). Hence we use the method to compute the 2-rank and 4-rank of $C(E)$ for all such biquadratic fields E.

EXAMPLE 5.1. Let

$$F = \mathbb{Q}(\sqrt{-21}), \qquad E = F(\sqrt{5 \cdot 11 \cdot 13}).$$

Set $p_1 = 3$, $p_2 = 7$, $p_3 = 2$. We have the Rédei matrix over $\mathbb{F}_2$

$$R'_F = \begin{pmatrix} \left(\frac{D/p_1^*}{p_1}\right) & \left(\frac{p_2}{p_1}\right) & \left(\frac{p_3}{p_1}\right) \\ \left(\frac{p_1}{p_2}\right) & \left(\frac{D/p_2^*}{p_2}\right) & \left(\frac{p_3}{p_2}\right) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

It is clear that $5, 11$ split in F and 13 is inert in F. Set $q_1 = 5$, $q_2 = 11$, $q_3 = 13$ and there is a matrix over $\mathbb{F}_2$

$$M_E = \begin{pmatrix} \left(\frac{q_1}{p_1}\right) & \left(\frac{q_2}{p_1}\right) \\ \left(\frac{q_1}{p_2}\right) & \left(\frac{q_2}{p_2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

We have $\operatorname{rank} M_E = s = 2$. In fact, since $2 \cdot 11 = 1^2 + 21$, we have $[Q_2][Q_{11}] = 1$ and $Q_{11}^2 = (10 - \sqrt{-21})O_F$, where $Q_2^2 = 2O_F$ and $Q_{11}Q'_{11} = 11O_F$; since $5 \cdot 2 \cdot 7 = 7^2 + 21$, we have $[Q_5][Q_2Q_7] = 1$ and $Q_5^2 = (2 - \sqrt{-21})O_F$, where $Q_7^2 = 7O_F, Q_5Q'_5 = 5O_F$. Let $S_f = \{Q_5, Q_{11}\}$ and $S = \{\infty, Q_5, Q_{11}\}$. Then $C^S(F)$ has odd order. It is clear that $m = n = 5$ and $U_F/U_F^2 = (\overline{-1})$. Let $P_1 = (5, 2 - \sqrt{-21}) = Q_5$, $P_2 = (11, 10 - \sqrt{-21}) = Q_{11}$, $P_3 = (5, 2 + \sqrt{-21})$, $P_4 = (11, 10 + \sqrt{-21})$, $P_5 = 13O_F$ be all finite prime ideals of F ramifying in E and $x_1 = 2 - \sqrt{-21}$, $x_2 = 10 - \sqrt{-21}$, $x_3 = 5$, $x_4 = 11$, $x_5 = 13$, i.e.

$$P_1^2 = x_1O_F, \quad P_2^2 = x_2O_F, \quad P_1P_3 = x_3O_F, \quad P_2P_4 = x_4O_F, \quad P_5 = x_5O_F.$$

Let $d = 5 \cdot 11 \cdot 13$. Then

$$M_S = \begin{pmatrix} (x_1, d)_{P_1} & (x_1, d)_{P_2} & (x_1, d)_{P_3} & (x_1, d)_{P_4} & (x_1, d)_{P_5} \\ (x_2, d)_{P_1} & (x_2, d)_{P_2} & (x_2, d)_{P_3} & (x_2, d)_{P_4} & (x_2, d)_{P_5} \\ (-1, d)_{P_1} & (-1, d)_{P_2} & (-1, d)_{P_3} & (-1, d)_{P_4} & (-1, d)_{P_5} \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Hence $r_2(K_3) = s_3 = 1$, i.e. $x_1 = 2 - \sqrt{-21} \in NE$, and $-1 \notin NE$, so $r_2(C(E)) = s + m - 1 - r_2(U_F/U_F \cap NE) - s_3 = 2 + 5 - 1 - 1 - 1 = 4$. Moreover, if $d = 5 \cdot 11 \cdot 13$,

$$R_{E/F} = \begin{pmatrix} (x_2,d)_{P_1} & (x_2,d)_{P_2} & (x_2,d)_{P_3} & (x_2,d)_{P_4} & (x_2,d)_{P_5} \\ (x_3,d)_{P_1} & (x_3,d)_{P_2} & (x_3,d)_{P_3} & (x_3,d)_{P_4} & (x_3,d)_{P_5} \\ (x_4,d)_{P_1} & (x_4,d)_{P_2} & (x_4,d)_{P_3} & (x_4,d)_{P_4} & (x_4,d)_{P_5} \\ (x_5,d)_{P_1} & (x_5,d)_{P_2} & (x_5,d)_{P_3} & (x_5,d)_{P_4} & (x_5,d)_{P_5} \\ (-1,d)_{P_1} & (-1,d)_{P_2} & (-1,d)_{P_3} & (-1,d)_{P_4} & (-1,d)_{P_5} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Since $\operatorname{rank} R_{E/F} = 2$, we have $r_4(C(E)) = m - 1 - \operatorname{rank} R_{E/F} + s_3 = 5 - 1 - 2 + 1 = 3$.

REMARK 5.1. If E is a biquadratic number field with $\mathrm{Gal}(E/\mathbb{Q}) \cong K_4$ (Klein's four group), then $E/\mathbb{Q}$ has three intermediate fields, say F_1, F_2, F_3; let U_1, U_2, U_3, U_E be the unit groups of F_1, F_2, F_3, E, respectively. Kuroda gave a formula for the class number (see [11]):

$$h(E) = \begin{cases} \frac{1}{4}[U_E : U_1U_2U_3]h(F_1)h(F_2)h(F_3) & \text{if } E \text{ is real,} \\ \frac{1}{2}[U_E : U_1U_2U_3]h(F_1)h(F_2)h(F_3) & \text{if } E \text{ is imaginary.} \end{cases}$$

In Example 5.1, we get the structure of the 2-Sylow subgroup of $C(E)$.

In the following, we give an example where E is a relative quadratic extension of $F = \mathbb{Q}(\sqrt{d_1})$, $d_1 \in \mathbb{Z}$, and $E/\mathbb{Q}$ is not a Galois extension.

EXAMPLE 5.2. Let

$$F = \mathbb{Q}(\sqrt{-21}), \qquad E = F\Big(\sqrt{11(8+\sqrt{-21})}\Big).$$

Since $N_{E/F}(8+\sqrt{-21}) = 5 \cdot 17$, we know that the prime ideals $Q_5 = (5, 8 + \sqrt{-21}) = (5, 2 - \sqrt{-21})$, $Q_{11} = (11, 10 - \sqrt{-21})$, $Q'_{11} = (11, 10 + \sqrt{-21})$, $Q_{17} = (17, 8 + \sqrt{-21})$ of F ramify in E and the dyadic ideal $D = (2, 1 + \sqrt{-21})$ of F ramifies in E. In fact, let F_D be the complete field of F at D. Then $F_D \cong \mathbb{Q}_2(\sqrt{3})$. Since $11(8+\sqrt{-21}) \equiv 3\sqrt{3} \bmod 8$, it follows that

$$f(x+\sqrt{3}) = (x+\sqrt{3})^2 - 3\sqrt{3} = x^2 + 2\sqrt{3}x + 3(1-\sqrt{3})$$

is an Eisenstein polynomial in $\mathbb{Q}_2(\sqrt{3})$. Hence the dyadic prime D of F ramifies in E, so $m = n = 5$. Let $S_f = \{Q_5, Q_{11}\}$ and $S = \{\infty, Q_5, Q_{11}\}$. Then $C^S(F)$ has odd order by Example 5.1. Let $P_1 = Q_5 = (5, 2 - \sqrt{-21})$, $P_2 = (11, 10 - \sqrt{-21})$, $P_3 = (11, 10 + \sqrt{-21})$, $P_4 = (17, 8 + \sqrt{-21}) = Q_{17}$, $P_5 = (2, 1 + \sqrt{-21})$ be all finite prime ideals of F ramifying in E and

$x_1 = 2-\sqrt{-21}$, $x_2 = 10-\sqrt{-21}$, $x_3 = 11$, $x_4 = 8+\sqrt{-21}$, $x_5 = 1+\sqrt{-21}$, i.e. $P_1^2 = x_1 O_F$, $P_2^2 = x_2 O_F$, $P_3P_2 = x_3 O_F$, $P_4P_1 = x_4 O_F$, $P_5P_2 = x_5 O_F$. Let $d = 11(8+\sqrt{-21})$. Then

$$M_S = \begin{pmatrix} (x_1,d)_{P_1} & (x_1,d)_{P_2} & (x_1,d)_{P_3} & (x_1,d)_{P_4} & (x_1,d)_{P_5} \\ (x_2,d)_{P_1} & (x_2,d)_{P_2} & (x_2,d)_{P_3} & (x_2,d)_{P_4} & (x_2,d)_{P_5} \\ (-1,d)_{P_1} & (-1,d)_{P_2} & (-1,d)_{P_3} & (-1,d)_{P_4} & (-1,d)_{P_5} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Hence $r_2(K_3) = s_3 = 2$ and $r_2(C(E)) = s+m-1-r_2(U_F/U_F \cap NE) - s_3 = 2+5-1-1-2 = 3$. Moreover,

$$R_{E/F} = \begin{pmatrix} (x_1,d)_{P_1} & (x_1,d)_{P_2} & (x_1,d)_{P_3} & (x_1,d)_{P_4} & (x_1,d)_{P_5} \\ (x_2,d)_{P_1} & (x_2,d)_{P_2} & (x_2,d)_{P_3} & (x_2,d)_{P_4} & (x_2,d)_{P_5} \\ (x_3,d)_{P_1} & (x_3,d)_{P_2} & (x_3,d)_{P_3} & (x_3,d)_{P_4} & (x_3,d)_{P_5} \\ (x_4,d)_{P_1} & (x_4,d)_{P_2} & (x_4,d)_{P_3} & (x_4,d)_{P_4} & (x_4,d)_{P_5} \\ (x_5,d)_{P_1} & (x_5,d)_{P_2} & (x_5,d)_{P_3} & (x_5,d)_{P_4} & (x_5,d)_{P_5} \\ (-1,d)_{P_1} & (-1,d)_{P_2} & (-1,d)_{P_3} & (-1,d)_{P_4} & (-1,d)_{P_5} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Hence $\operatorname{rank} R_{E/F} = 4$, so $r_4(C(E)) = m - 1 - \operatorname{rank} R_{E/F} + s_3 = 2$.

Acknowledgements. The paper is partly supported by NNSF of China (No. 10771100, No. 10971250, No. 11171150) and the Morningside Center of Mathematics in Beijing (MCM). The author thanks the referees for their valuable comments and suggestions.

References

[1] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields with* $Cl_2(K) \cong (2,2,2)$, J. Number Theory 103 (2003), 38–70.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, Orlando, FL, 1966.

[3] C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Tokyo 2 (1933), 365–476.
[4] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. 8, World Sci., Singapore, 1988.
[5] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, I*, Ann. Inst. Fourier (Grenoble) 23 (1973), no. 3, 1–48.
[6] —, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, II*, ibid. 23 (1973), no. 4, 1–44.
[7] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, New York, 1981.
[8] J. Hurrelbrink and M. Kolster, *Tame kernels under relative quadratic extensions and Hilbert symbols*, J. Reine Angew. Math. 499 (1998), 145–188.
[9] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
[10] S. Lang, *Cyclotomic Fields, I, II*, Grad. Texts in Math. 121, Springer, New York, 1990.
[11] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. 66 (1994), 245–260.
[12] J. Neukirch, *Class Field Theory,* Springer, New York, 1980.
[13] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69–74.
[14] Q. Yue, *Tame kernels for biquadratic number fields*, K-Theory 35 (2005), 69–91.
[15] —, *The generalized Rédei-matrix*, Math. Z. 261 (2009), 23–37.

Qin Yue
Department of Mathematics
College of Science
Nanjing University of Aeronautics and Astronautics
Nanjing 210016, People's Republic of China
E-mail: yueqin@nuaa.edu.cn

Received on 2.2.2010
and in revised form on 27.5.2011 (6295)