The Ramanujan Journal (2021) 54:463–473
https://doi.org/10.1007/s11139-020-00251-4

The 2-Sylow subgroup of K_2O_F for certain quadratic number fields

Xia Wu[1]

Received: 13 April 2019 / Accepted: 17 January 2020 / Published online: 17 July 2020

Abstract
In this paper, we apply Qin's theorem for the 4-rank of K_2O_F to establish the relation between the 4-rank of the ideal class group of $F = \mathbb{Q}(\sqrt{d})$ and the 4-rank of K_2O_F provided that all odd prime factors of d are congruent to 1 mod 8. As an application, we give a concise and unified proof of two conjectures proposed by Conner and Hurrelbrink (Acta Arith 73:59–65, 1995).

Keywords Tame kernel · Ideal class group · Quadratic number field

Mathematics Subject Classification 11R70 · 19F15 · 11R29 · 11R11

1 Introduction

Let F be a number field, O_F the ring of integers in F. Let K_2O_F denote the Milnor group of O_F, which coincides with the tame kernel of F. As a finite abelian group, K_2O_F contains rich arithmetical information. In particular, the Birch–Tate conjecture and the Lichtenbaum conjecture establish a relation between the order of K_2O_F and the value $\zeta_F^*(-1)$, where $\zeta_F(\cdot)$ is the Dedekind zeta-function of F. To understand K_2O_F, we need to know the p^n-rank of K_2O_F for any prime p and any positive integer n. If F contains a primitive p^n-th root of unity, the p^n-rank of K_2O_F formula is given by Tate [13], in particular, the 2-rank of K_2O_F formula is given for any number field. See also Keune [6].

When $F = \mathbb{Q}(\sqrt{d})$ is a quadratic field, Browkin and Schinzel [3] give an explicit formula for the 2-rank of K_2O_F. Qin [9–11] obtains formulas for the 4-rank of K_2O_F and the 8-rank of K_2O_F. See also [8,12]. In this paper, we apply Qin's theorem for

This work was supported by the National Natural Science Foundation of China (Grant No. 11971102).

✉ Xia Wu
wuxia80@seu.edu.cn

1 School of Mathematics, Southeast University, Nanjing 210096, China

the 4-rank of $K_2 O_F$ to establish a relation between the 4-rank of ideal class group and the 4-rank of $K_2 O_F$ provided that all odd prime factors of d are congruent to 1 mod 8. As an application, we give a concise and unified proof of two conjectures proposed by Conner and Hurrelbrink in [4]. Both conjectures are proved by Vazzana [14,15], but the proofs, which use graph theory, are somewhat involved.

2 Statement of main theorems

We first state main theorems of this paper. For any abelian group A, let $r_4(A)$ denote the 4-rank of A.

Theorem 2.1 *Let $E = \mathbb{Q}(\sqrt{d})$, where $d = p_1 \dots p_k$ with $p_i \equiv 1 \pmod 8$ and let $C(E)$ be the class group of E. Assume that*

(i) *the norm of the fundamental unit of E is -1, and*
(ii) *an odd number of the primes $p_1, \dots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$. Then*

$$r_4(K_2 O_E) = r_4(C(E)).$$

Theorem 2.2 *Let $F = \mathbb{Q}(\sqrt{2d})$ and $E = \mathbb{Q}(\sqrt{d})$, where $d = p_1 \dots p_k$ with $p_i \equiv 1 \pmod 8$ and let $C(E)$ be the class group of E. Assume that*

(i) *the norm of the fundamental unit of E is -1, and*
(ii) *an odd number of the primes $p_1, \dots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 64y^2$. Then*

$$r_4(K_2 O_F) = r_4(C(E)).$$

Theorem 2.3 *Let $F = \mathbb{Q}(\sqrt{2d})$, where $d = p_1 \dots p_k$ with $p_i \equiv 1 \pmod 8$ and let $C(F)$ be the class group of F. Assume that*

(i) *the norm of the fundamental unit of F is -1, and*
(ii) *an odd number of the primes $p_1, \dots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 64y^2$. Then*

$$r_4(K_2 O_F) = r_4(C(F)) - 1.$$

As corollaries of Theorems 2.1 and 2.2, we have the following two theorems.

Theorem 2.4 *The 2-primary part of $K_2(\mathcal{O}_E)$ is elementary abelian if and only if*

(i) *the 2-primary part of the ideal class group $C(E)$ is elementary abelian and the norm of the fundamental unit of E is -1, and*
(ii) *an odd number of the primes $p_1, \dots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

Theorem 2.4 gives an explicit set of conditions under which the 2-primary part of $K_2(\mathcal{O}_E)$ is elementary abelian. A similar theorem for the field $F = \mathbb{Q}(\sqrt{2d})$ is as follows.

Theorem 2.5 *The 2-primary part of $K_2(\mathcal{O}_F)$ is elementary abelian if and only if*

(i) *the 2-primary part of the ideal class group $C(E)$ is elementary abelian and the norm of the fundamental unit of E is -1, and*
(ii) *an odd number of the primes $p_1, \ldots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 64y^2$.*

Both of these two theorems were conjectured by Conner and Hurrelbrink in [4]. Vazzana proved the two theorems in [14] and [15], respectively. In particular, his proof for Theorem 2.5 is complicated. He made use of a graph associated with the primes $p_1, \ldots, p_k$ and studied its relationship to a new graph associated with the primes lying over $p_1, \ldots, p_k$ in $\mathbb{Q}(\sqrt{-2})$. Our alternative proof is not only unified but also very concise.

3 Prelimilary results

In this section, we review some known results which are useful in this paper. The following result is classical. One can find a proof in [5].

Lemma 3.1 (Legendre's Theorem) *Suppose that a, b, c are square-free,*

$$(a,\ b) = (a,\ c) = (b,\ c) = 1$$

and a, b, c do not have the same sign. Then the Diophantine equation

$$aX^2 + bY^2 + cZ^2 = 0$$

has nontrivial solutions if and only if for every odd prime $p|abc$, say, $p|a$, $\left(\frac{-bc}{p}\right) = 1$.

We adopt the notation from [11]. Let $d \neq 0$ be an integer. Put

$$S(d) = \begin{cases} \{\pm 1, \pm 2\} & \text{if } d > 0, \\ \{1, 2\} & \text{if } d < 0. \end{cases} \tag{1}$$

For any abelian group A, set

$${}_2A = \{x \in A | x^2 = 1\}.$$

For a number field F, we use NF for the set of norms from F over $\mathbb{Q}$.

Let F be a number field with r_2 complex places. By Tate [13], every element of order two in K_2F is of the form $\{-1,\ a\}$, where $a \in F^*$. Let Δ denote the Tate kernel of F, i.e., the group of elements $x \in F^*$ such that $\{-1, \ x\} = 1$. If $\sqrt{2} \notin F$, then by [13],

$$(\Delta : (F^*)^2) = 2^{r_2+1}.$$

In particular, if $F \neq \mathbb{Q}(\sqrt{2})$ is a real quadratic field, then $\Delta = F^* \cup 2F^*$.

Theorem 3.2 (Browkin and Schinzel) *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free. Then ${}_2K_2(O_F)$ can be generated by*

$$\{-1, m\}, \quad m|d,$$

together with

$$\{-1, u_i + \sqrt{d}\},$$

if $\{-1, \pm 2\} \cap NF \neq \emptyset$, where $u_i \in \mathbb{Z}$ is such that $u_i^2 - d = c_i w_i^2$ for some $w_i \in \mathbb{Z}$ and $c_i \in \{-1, \pm 2\} \cap NF$.

Remark The general $r_2(K_2 O_F)$ formula for an arbitrary number field F is given by Tate [13].

For any integer n, put $\nabla^n = \{\alpha \in K_2 O_F | \alpha = \beta^n$ for some $\beta \in K_2 O_F\}$.

Our main tool is the following theorem of Qin, which completely determines the 4-rank of $K_2 O_F$ for any quadratic field (see [9,10]).

Theorem 3.3 (Qin) *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free. Suppose that $m|d$ ($m > 0$ if $d > 0$, ,but m also takes on negative values if $d < 0$) and write $d = u^2 - 2w^2$ with $u, w \in \mathbb{Z}$ if $2 \in NF$. Then $\{-1, m\} \in \nabla^2$ if and only if one can find an $\epsilon \in S(d)$ such that*

(i) $\left(\frac{\frac{d}{m}}{p}\right) = \left(\frac{\epsilon}{p}\right)$ *for every odd prime $p|m$;*

(ii) $\left(\frac{m}{p}\right) = \left(\frac{\epsilon}{p}\right)$ *for every odd prime $p|\frac{d}{m}$;*

and $\{-1, m(u + \sqrt{d})\} \in \nabla^2$ if and only if one can find an $\epsilon \in S(d)$ such that

(iii) $\left(\frac{\frac{d}{m}}{p}\right) = \left(\frac{\epsilon(u+w)}{p}\right)$ *for every odd prime $p|m$;*

(iv) $\left(\frac{m}{p}\right) = \left(\frac{\epsilon(u+w)}{p}\right)$ *for every odd prime $p|\frac{d}{m}$.*

Corollary 3.4 *Let $d = p_1 \dots p_k$ be a product of different primes congruent to 1 mod 8, and let $F = \mathbb{Q}(\sqrt{d})$ or $F = \mathbb{Q}(\sqrt{2d})$. If $m \mid d$, then $\{-1, m\} \in \nabla^2$ if and only if*

$$Z^2 = mX^2 + \frac{d}{m}Y^2$$

is solvable in $\mathbb{Z}$; $\{-1, m(u + \sqrt{d})\} \in \nabla^2$ if and only if

$$(u + w)Z^2 = mX^2 + \frac{d}{m}Y^2$$

is solvable in $\mathbb{Z}$.

Proof Since for every odd prime p dividing d, $\left(\frac{\pm 1}{p}\right) = \left(\frac{\pm 2}{p}\right) = 1$, the result follows from Theorem 3.3 and Lemma 3.1. □

4 Proofs of main results

Lemma 4.1 *Let $d = p_1 \dots p_k$ be a product of rational primes congruent to* 1 *mod* 8. *Assume that $d = u^2 - 2w^2$, $v = u + w (u > 0)$. Then $v \equiv 3 \pmod 4$ if and only if an odd number of the primes $p_1, \dots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

Proof First we assume that $k = 1$. There exist two integers u, w such that $p = u^2 - 2w^2$. Assume that $u > 0$ and write $v = u + w$. Since $u^2 - 2w^2 = (3u + 4w)^2 - 2(2u + 3w)^2$ and $p \equiv 1 \pmod 8$, by a suitable choice of u, w, we can write $p = u^2 - 2(4w')^2$. Hence $v = u + 4w' \equiv u \pmod 4$. By [1], we have that $v \equiv 1 \pmod 4$ if and only if $p = x^2 + 32y^2$, equivalently, $v \equiv 3 \pmod 4$ if and only if $p \neq x^2 + 32y^2$.

We consider now the general case. Assume that $d_1 = u_1^2 - 2w_1^2$, $d_2 = u_2^2 - 2w_2^2$ and $d_1 d_2 = u^2 - 2w^2$. Then $d_1 d_2 = (u_1 u_2 + 2w_1 w_2)^2 - 2(u_1 w_2 + u_2 w_1)^2$. If we assume further that $d_1 \equiv d_2 \equiv 1 \pmod 4$, then both w_1 and w_2 are even. We have

$$(u_1 u_2 + 2w_1 w_2) + (u_1 w_2 + u_2 w_1) \equiv (u_1 + w_1)(u_2 + w_2) \pmod 4, \tag{2}$$

i.e., $v = u + w \equiv v_1 v_2 \pmod 4$, where $v_1 = u_1 + w_1$, $v_2 = u_2 + w_2$. Now suppose that $p_1 \dots p_k = u^2 - 2w^2$, $v = u + w (u > 0)$. For any $1 \leq i \leq k$, assume that $p_i = u_i^2 - 2w_i^2$ $(u_i > 0)$ and write $v_i = u_i + w_i$. By induction,

$$v \equiv v_1 \dots v_k \pmod 4.$$

Note that $v_i \equiv 1$ or $3 \pmod 4$ and $v_i \equiv 1 \pmod 4$ if and only if $p_i = x^2 + 32y^2$. Therefore, $v \equiv 3 \pmod 4$ if and only if an odd number of the primes $p_1, \dots, p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$. □

Lemma 4.2 *Let $p_1, \dots, p_k$ be rational primes congruent to* 1 *mod* 8. *Let $d = p_1 \dots p_k$ or $2p_1 \dots p_k$, let $E = \mathbb{Q}(\sqrt{d})$, and let $C(E)$ be the class group of E. Write ε for the fundamental unit of $E = \mathbb{Q}(\sqrt{d})$. Then*

(i) *$N\varepsilon = 1$ if and only if the following Diophantine equation is solvable for some $m \mid d$, $m \neq \pm 1$ or $\pm d$,*

$$mX^2 - \frac{d}{m}Y^2 = \pm 1. \tag{3}$$

(ii) *if $N\varepsilon = -1$ then ${}_2C(E)$ can be generated by the ideals $\wp_1, \dots, \wp_k$, where for any i, $\wp_i^2 = p_i$.*

Proof

(i) We apply the result on the Tate kernel of real quadratic fields to show that the norm of the fundamental unit of $E = \mathbb{Q}(\sqrt{d})$ is 1 if and only if

$$mX^2 - \frac{d}{m}Y^2 = \pm 1$$

is solvable for some $m \mid d$, $m \neq \pm 1, \pm d$. In fact, since $\{-1, \varepsilon\} \in {}_2K_2(O_E)$, by Theorem 3.2, there exists some $m \mid d$, $m \neq \pm 1, \pm d$ such that $\{-1, \varepsilon\} = \{-1, m\}$ or $\{-1, \varepsilon\} = \{-1, m(u + \sqrt{d})\}$. It is straightforward to see that

$$\varepsilon m(u + \sqrt{d}) \notin E^{*2} \cup 2E^{*2}.$$

Clearly, we have $\varepsilon m \notin 2E^{*2}$. Hence, $\varepsilon m \in E^{*2}$. Therefore, $m^2 = \varepsilon m \bar{\varepsilon} m = (X^2 - dY^2)^2$ for some integers X, Y, so we obtain $\pm m = X^2 - dY^2$, i.e., (3) holds.
Conversely, if $\pm m = X^2 - dY^2$, $m \neq \pm 1, \pm d$, we put

$$\varepsilon = \frac{X + \sqrt{d}Y}{X - \sqrt{d}Y}.$$

It is obvious that $(m, Y) = 1$. Hence, for any finite prime P of E, if $P \mid m$, then $v_P(X + \sqrt{d}Y) = v_P(X - \sqrt{d}Y) = 1$; if $P \nmid m$, then $v_P(X + \sqrt{d}Y) = v_P(X - \sqrt{d}Y) = 0$. Therefore, ε is an algebraic integer. Moreover, ε is not a square, since $\varepsilon(X - \sqrt{d}Y)^2 = X^2 - dY^2 = \pm m,\ m \neq \pm 1, \pm d$, is not a square.

(ii) By genus theory, the 2-rank of $C(E)$ is $k - 1$ if $E = \mathbb{Q}(\sqrt{p_1 \dots p_k})$, and k if $E = \mathbb{Q}(\sqrt{2p_1 \dots p_k})$. For any $m \mid d$, the ideal $(m, \sqrt{d})$ satisfies that $(m, \sqrt{d})^2 = (m)$. Moreover, $(m, \sqrt{d})$ is principal in $C(E)$ if and only if

$$\pm m = X^2 - dY^2 \tag{4}$$

is solvable over $\mathbb{Z}$.
But the assumption that $N\varepsilon = -1$ implies that for any $m \mid d$, $m \neq \pm 1, \pm d$, (4) has no integer solution. Therefore, the ideals $\wp_1, \dots, \wp_k$ generate ${}_2C(E)$.

□

Proof of Theorem 2.1 We apply Theorem 3.3 to compute $r_4(K_2O_E)$.
We first show that the assumption (ii) implies $\{-1, m(u + \sqrt{d})\} \notin \nabla^2$.
Recall that in our case, all prime factors are congruent to 1 mod 8. By Corollary 3.4 to theorem of Qin, the condition that $\{-1, m(u + \sqrt{d}\} \in \nabla^2$ is equivalent to the fact that there exists a positive factor m of d, so that

$$vmZ^2 = X^2 + dY^2 \tag{5}$$

is solvable in $\mathbb{Z}$. Since $d \equiv 1 \pmod 8$, $m \mid d$, $X^2 + dY^2 \equiv 0, 1, 2 \pmod 4$. Now the assumption (ii) and Lemma 4.1 imply that $v \equiv 3 \pmod 4$. Hence, $vmZ^2 \equiv 0, 3 \pmod 4$ and so (5) has no solution with $(X, Y, Z) = 1$.

Therefore, in ${}_2K_2O_E$ only $\{-1, m\}$ could belong to ∇^2. By sending $\{-1, m\}$ to the ideal $\mathfrak{M}(\mathfrak{M}^2 = m)$, we obtain a bijection from the set $\{\{-1, m\}, m \mid d\} \subseteq {}_2K_2O_E$ to ${}_2C(E)$.

By [7], we see that $\mathfrak{M}$ is a square in $C(E)$ if and only if

$$mZ^2 = X^2 - dY^2 \tag{6}$$

is solvable in $\mathbb{Z}$. Furthermore, $\{-1, m\}$ is a square in K_2O_E, i.e., $\{-1, m\} \in \nabla^2$ if and only if

$$mZ^2 = X^2 + dY^2 \tag{7}$$

is solvable in $\mathbb{Z}$. As (6) and (7) have the same solvability,

$$r_4(K_2O_F) = r_4(C(F))$$

holds. □

To prove Theorem 2.2, we need the following Lemma 4.5, which is an analog of Lemma 4.1. First we have

Lemma 4.3 *Let $\alpha = 2^{\frac{1}{4}}$ and $L = \mathbb{Q}(\alpha)$. Then $\mathbb{Z}[\alpha]$ is the ring of algebraic integers of L. The class number of L is* 1.

Proof This can be done by the GP calculator. □

Lemma 4.4 *Let $p \equiv 1 \pmod 8$ be a prime. Assume that $p = u^2 - 2w^2$ with $u > 0$. Then $p = x^2 + 64y^2$ if and only if $u \equiv 1, 3 \pmod 8$.*

Proof We need the following result: Let $p \equiv 1 \pmod 8$ be a prime. Then $\gamma^4 \equiv 2 \pmod p$ is solvable if and only if $p = x^2 + 64y^2$. See, for example, Theorem 7.5.2 in [2]. Hence, for a prime $p = x^2 + 64y^2$, $\gamma^4 \equiv 2 \pmod p$ has four distinct solutions. It follows that p splits completely in L. Hence, there are integers a, b, c, d such that

$$p = N_{L/\mathbb{Q}}(a + b\alpha + c\alpha^2 + d\alpha^3) = (a^2 + 2c^2 - 4bd)^2 - 2(b^2 + 2d^2 - 2ac)^2.$$

Since $p \equiv 1 \pmod 8$, we see that a is odd and $2 \mid b$. Hence we have $u = a^2 + 2c^2 - 4bd \equiv 1, 3 \pmod 8$.

Conversely, if $p = u^2 - 2w^2$ with $|u| \equiv 1, 3 \pmod 8$ and w even, then $p = x^2 + 64y^2$. In fact, we may write $u = t^2u'$, $w = 2^e s^2 w'$, where u', w' are square-free odd and positive integers. For any prime $l \mid w'$, $(\frac{p}{l}) = 1$, hence, $w \equiv \alpha^2 \pmod p$ since 2 is a square $\pmod p$. On the other hand, for any prime $l \mid u'$, $(\frac{-2p}{l}) = 1$, hence, $|u| \equiv 1, 3 \pmod 8$ implies that $u \equiv \alpha^2 \pmod p$. Therefore, $\gamma^4 \equiv 2 \pmod p$ is solvable and so $p = x^2 + 64y^2$. □

Lemma 4.5 *Let $d = 2p_1 \dots p_k$ with $p_1 \equiv \cdots \equiv p_k \equiv 1 \pmod 8$. Assume that $p_i = u_i^2 - 2w_i^2$, $v_i = u_i + w_i (u_i > 0)$. If we write $p_1 \dots p_k = u^2 - 2w^2$, and*

$2p_1 \dots p_k = U^2 - 2W^2, U > 0$, *then* $u \equiv u_1 \dots u_k \pmod 8$ *and* $U + W \equiv u$ *or* $3u \pmod 8$. *Moreover,* $U + W \equiv 5$, *or* $7 \pmod 8$ *if and only if an odd number of the primes* $p_1, \dots, p_k$ *fail to be represented over* $\mathbb{Z}$ *by the quadratic form* $x^2 + 64y^2$.

Proof Assume that $a = u^2 - 2w^2$ and $b = \mu^2 - 2\omega^2$. Then we have

$$ab = (u\mu + 2w\omega)^2 - 2(u\omega + \mu w)^2. \tag{8}$$

Note that if both $a, b \equiv 1 \pmod 8$, it is easy to see w and ω are even, so $u\mu + 2w\omega \equiv u\mu \pmod 8$. By induction, we have $u \equiv u_1 \dots u_k \pmod 8$. Observe that

$$2a = (2u + 2w)^2 - 2(u + 2w)^2. \tag{9}$$

Since $(2u + 2w) + (-u - 2w) = u$ and $(2u + 2w) + (u + 2w) = 3u + 4w \equiv 3u \pmod 8$, $U + W \equiv u$ or $3u \pmod 8$.

If $k = 1$ and $d = 2p_1 = U^2 - 2W^2$, by Lemma 4.4, $p_1 \neq x^2 + 64y^2$ if and only if $U + W \equiv 5, 7 \pmod 8$. Observe that if $u_1 \equiv 1, 3 \pmod 8$, $u_2 \equiv 1, 3 \pmod 8$ or $u_1 \equiv 5, 7 \pmod 8$, $u_2 \equiv 5, 7 \pmod 8$, then $u_1u_2 \equiv 1, 3 \pmod 8$, and if $u_1 \equiv 1, 3 \pmod 8$, $u_2 \equiv 5, 7 \pmod 8$, then $u_1u_2 \equiv 5, 7 \pmod 8$. Therefore, by (8) and (9), if an odd number of the primes $p_1, \dots, p_k$ fail to be represented by $x^2 + 64y^2$, then $U + W \equiv 5$, or $7 \pmod 8$, and vice versa. □

Proof of Theorem 2.2 As in the proof of Theorem 2.1, we apply again Theorem 3.3 to compute $r_4(K_2O_F)$.

Write $2d = u^2 - 2w^2$, $u > 0$, $v = u + w$. We claim that for any $m \mid 2d$, $\{-1, m(u + \sqrt{2d})\} \notin \nabla^2$.

Indeed, by Theorem 3.3 and Lemma 3.1, if for some positive factor m of $2d$, $\{-1, m(u + \sqrt{2d})\} \in \nabla^2$, then

$$vmZ^2 = X^2 + 2dY^2 \tag{10}$$

is solvable in $\mathbb{Z}$. By Lemma 3.1, we can assume that m is odd. Since $2d \equiv 2 \pmod 8$, one has $X^2 + 2dY^2 \equiv 1, 2, 3, 6 \pmod 8$ if $(X, Y) = 1$. It follows from Lemma 4.5 that the assumption (ii) implies that $v \equiv 5, 7 \pmod 4$. Hence, $vmZ^2 \equiv 0, 4, 5, 7 \pmod 8$ and so (10) has no solution with $(X, Y, Z) = 1$.

Note that $\{-1, 2m\} = \{-1, m\}$. Therefore, the same discussion as in the proof of Theorem 2.1 shows that

$$r_4(K_2O_F) = r_4(C(E)).$$

□

Proof of Theorem 2.3 The assumption that the norm of the fundamental unit of F is -1 implies that there is an ideal $\wp$ of F, which is non-principal with $\wp^2 = (2)$. But in K_2O_F, $\{-1, 2\} = 1$. Then the proof is analogous to that of Theorem 2.2. □

We turn to prove Theorems 2.4 and 2.5. Let $m \mid d$. We introduce the following notation.

$$V(m, p_1, \ldots, p_k) = (\epsilon_1, \ldots, \epsilon_k),$$

where

$$\epsilon_i = \begin{cases} \left(\frac{\frac{d}{m}}{p_i}\right) \text{ if } p_i \mid m, \\ \left(\frac{m}{p_i}\right) \text{ if } p_i \nmid m. \end{cases} \tag{11}$$

It is easy to check that $\sqcap_{i=1}^{k} \epsilon_i = 1$. Similarly, we put

$$V(m(u + \sqrt{d}), p_1, \ldots, p_k) = (\epsilon_1, \ldots, \epsilon_k),$$

where

$$\epsilon_i = \begin{cases} \left(\frac{\frac{vd}{m}}{p_i}\right) \text{ if } p_i \mid m, \\ \left(\frac{vm}{p_i}\right) \text{ if } p_i \nmid m. \end{cases} \tag{12}$$

By Theorem 3.3, $\{-1, m\} \in \nabla^2$ if and only if $V(m, p_1, \ldots, p_k) = (1, \ldots, 1)$. If $m, n \mid d$ and $(m, n) = t$, we write $V(mn, p_1, \ldots, p_k) = V(mn/t^2, p_1, \ldots, p_k)$. Moreover, if $V(m, p_1, \ldots, p_k) = (\epsilon_1, \ldots, \epsilon_k)$ and $V(n, p_1, \ldots, p_k) = (\delta_1, \ldots, \delta_k)$, then $V(mn, p_1, \ldots, p_k) = (\epsilon_1\delta_1, \ldots, \epsilon_k\delta_k)$. Similarly, $V(m(u+\sqrt{d}), p_1, \ldots, p_k) = (\epsilon_1, \ldots, \epsilon_k)$, and $V(n, p_1, \ldots, p_k) = (\delta_1, \ldots, \delta_k)$, then $V(mn(u+\sqrt{d}), p_1, \ldots, p_k) = (\epsilon_1\delta_1, \ldots, \epsilon_k\delta_k)$.

Proof of Theorem 2.4 If both (i) and (ii) are satisfied, then by Theorem 2.1, we have $r_4(K_2(\mathcal{O}_E)) = 0$, i.e., the 2-primary part of $K_2(\mathcal{O}_E)$ is elementary abelian.

Conversely, if the 2-primary part of $K_2(\mathcal{O}_E)$ is elementary abelian, then by Lemma 4.2, Lemma 3.1 and Theorem 3.3, we see that the norm of the fundamental unit of E is -1. We show that $\{-1, m(u + \sqrt{d})\} \notin \nabla^2$ implies condition (ii), which in turn shows that $v \equiv 3 \pmod 4$ as we can see from Lemma 4.1.

Since $r_4(K_2O_E) = 0$, for any $m \mid d$,

$$mZ^2 = X^2 + dY^2$$

and equivalently,

$$mZ^2 = X^2 - dY^2$$

has no integer solutions. Hence, we have proved that $r_4(C(E)) = 0$.

Since $r_4(K_2O_E) = 0$, for any $m \mid d$, $m \neq \pm 1, \pm d$, $V(m, p_1, \ldots, p_k) \neq (1, \ldots, 1)$. By a suitable choice of integers m_i dividing d, we may assume that

$\{-1,-1\}, \{-1, m_1\}, \ldots, \{-1, m_{k-1}\}, \{-1, u+\sqrt{d}\}, \{-1, u_{-1}+\sqrt{d}\}$ generate ${}_2K_2O_E$, where $u_{-1}^2 - d = -w_{-1}^2$, and the $m_j's$ are chosen in such a way that, for $1 \le i \le k-1, \epsilon_k = \epsilon_i = -1$ and for $j \ne i, k, \epsilon_j = 1$.

Suppose that $v \equiv 1 \pmod 4$. We have $(u+w)(u-w) - w^2 = d$ since $u^2 - 2w^2 = d$, hence $\left(\frac{-d}{v}\right) = 1$ and so $\left(\frac{v}{d}\right) = 1$. On the other hand, if $m \mid d$ with $m \equiv 1 \pmod 8$, then $\left(\frac{\frac{d}{m}}{m}\right)\left(\frac{m}{\frac{d}{m}}\right) = 1$. For any odd and positive $m \mid d$, assuming that $V(m(u+\sqrt{d}), p_1, \ldots, p_k) = (\epsilon_1, \ldots, \epsilon_k)$, we have $\sqcap_{i=1}^{k}\epsilon_i = \left(\frac{\frac{vd}{m}}{m}\right)\left(\frac{vm}{\frac{d}{m}}\right) = \left(\frac{v}{d}\right)\left(\frac{\frac{d}{m}}{m}\right)\left(\frac{m}{\frac{d}{m}}\right) = \left(\frac{v}{d}\right) = 1$. Therefore, there exists $n \mid d$ such that $V(n(u+\sqrt{d}), p_1, \ldots, p_k) = (1, \ldots, 1)$. This contradicts the assumption that $r_4(K_2O_E) = 0$. Hence, $v \equiv 3 \pmod 4$, and so we have (ii). □

Proof of Theorem 2.5 The proof is analogous to that of Theorem 2.4.

Applying Theorem 2.2, we see that (i) and (ii) imply that $r_4(K_2(\mathcal{O}_F)) = 0$.

Conversely, the assumption that $r_4(K_2(\mathcal{O}_F)) = 0$ implies that $r_4(C(E)) = 0$ and the norm of the fundamental unit of E is -1, i.e., (i) holds. To prove (ii), by Lemma 4.5, it is sufficient for us to show that $V = U + W \equiv 5, 7 \pmod 8$.

Since $U^2 - 2W^2 = 2d$, $\left(\frac{-2d}{V}\right) = 1$. Hence, $\left(\frac{V}{d}\right) = 1$ if and only if $V \equiv 1, 3 \pmod 8$. If $V \equiv 1, 3 \pmod 8$, then for any odd and positive $m \mid d$, assuming that $V(m(U+\sqrt{d}), p_1, \ldots, p_k) = (\epsilon_1, \ldots, \epsilon_k)$, we have $\sqcap_{i=1}^{k}\epsilon_i = \left(\frac{V}{d}\right) = 1$. Therefore, one can find $n \mid d$ such that $V(n(U+\sqrt{d}), p_1, \ldots, p_k) = (1, \ldots, 1)$, i.e., $r_4(K_2(\mathcal{O}_F)) > 0$, a contradiction!

This completes the proof. □

Acknowledgements The author would like to thank the referee for insightful and useful suggestions that improved the presentation of this paper.

References

1. Barrucand, P., Cohn, H.: Note on primes of type $x^2 + 32y^2$, class number, and residuacity. J. Reine Angew. Math. **238**, 67–70 (1969)
2. Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi Sums. Wiley, New York (1998)
3. Browkin, J., Schinzel, A.: On Sylow 2-subgroups of $K_2\mathcal{O}_F$ for quadratic number fields F. J. Reine Angew. Math. **331**, 104–113 (1982)
4. Conner, P.E., Hurrelbrink, J.: On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields. Acta Arith. **73**, 59–65 (1995)
5. Ireland, K., Rosen, M.: A Classical Introduction To Modern number Theory. Graduate Texts in Mathematics, vol. 84. Springer, New York (1972)
6. Keune, F.: On the structure of K_2 of the ring of integers in a number field. K-theory **2**, 625–645 (1989)
7. Kolster, M.: The 2-part of the narrow class group of a quadratic number field. Ann. Sci. Math. Que. **29**, 73–96 (2005)
8. Qin, H.R.: 2-Sylow subgroup of $K_2\mathcal{O}_F$ for real quadratic fields F. Sci. China **37**, 1302–1313 (1994)
9. Qin, H.R.: The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields. Acta Arith. **69**, 153–169 (1995)
10. Qin, H.R.: The 4-rank of $K_2(\mathcal{O})$ for real quadratic fields F. Acta Arith. **72**, 323–333 (1995)
11. Qin, H.R.: Tame kernels and Tate kernels of quadratic number fields. J. Reine Angew. Math. **530**, 105–144 (2001)

12. Qin, H.R.: The structure of the tame kernels of quadratic number fields(I). Acta Arith. **113**, 203–240 (2004)
13. Tate, J.: Relations between K_2 and Galois Cohomology. Invent. Math. **36**, 257–274 (1976)
14. Vazzana, A.: On the 2-primary part of K_2 of rings of integers in certain quadratic number fields. Acta Arith. **80**, 225–235 (1997)
15. Vazzana, A.: Elementary abelian 2-primary parts of $K_2\mathcal{O}$ and related graphs in certain quadratic number fields. Acta Arith. **81**, 253–264 (1997)