ACTA ARITHMETICA
XCVII.4 (2001)

Elements of order 4 of the Hilbert kernel in quadratic number fields

by

QIN YUE (Shanghai and Jiangsu)

1. Introduction. Let O_F be the ring of integers of a number field F. Let A be a finite Abelian group. We denote the 2-Sylow subgroup of A by A_2, the 2-rank of A by $r_2(A)$, and the 4-rank of A by $r_4(A)$.

By [2, 5, 9], we have 2-rank and 4-rank formulas for K_2O_F. For quadratic fields, Browkin and Schinzel [3] have given 2-rank formulas and forms of elements of order 2 of K_2O_F; Qin [12, 13, 14] has obtained a method to calculate 4-ranks of K_2O_F. Recently, Hurrelbrink and Kolster [8] have presented an effective way of computing 4-ranks of K_2O_F for relative quadratic extensions via the determination of the F_2-ranks of certain matrices of local Hilbert symbols. In [17] we have proved the following formula:

$$r_4(K_2O_F) = a(F) + r_4(C(E)),$$

where $F = \mathbb{Q}(\sqrt{d})$, $E = \mathbb{Q}(\sqrt{-d})$, $a(F) = -1, 0$, or 1 is a constant determined effectively by the Rédei matrices of E, and $C(E)$ is the narrow class group of E.

In the present paper, we concentrate on the structure of the 2-Sylow subgroup of K_2O_F and use the method of [5, 9] to give the results of [12, 13, 14] and to express the forms of elements of order 4 of K_2O_F for quadratic fields F, which are simpler. Using these forms we discuss whether elements of order 4 of K_2O_F are contained in Hilbert kernel $\mathfrak{R}_2F$. Hence, we get the relation between $r_4(K_2O_F)$ and $r_4(\mathfrak{R}_2F)$ and we get some quadratic fields with elements of order 8 in K_2O_F. We also obtain the following result: if $F = \mathbb{Q}(\sqrt{p_1p_2})$, where p_1 and p_2 are primes with $p_1 \neq p_2$, $p_1 \equiv p_2 \equiv 5 \bmod 8$, then $K_2O_F \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$ if and only if $16 \mid h(-p_1p_2)$, where $h(-p_1p_2)$ is the class number of $E = \mathbb{Q}(\sqrt{-p_1p_2})$. For imaginary quadratic fields, we add some values of the Tate kernel to the tables of [13].

2000 *Mathematics Subject Classification*: 11R65, 11R70, 19C99, 19D50.

The paper is supported by Morningside Center of Math., CAS, Shanghai Postdoctoral Science Foundation, and 00KJB110006.

2. Elements of order 4 in the tame kernel. We use the method of [5, 9] to investigate the elements of order 4 of K_2O_F for quadratic fields F. Now, we describe the notations of [5]:

- $F=\mathbb{Q}(\sqrt{d}),\ E=\mathbb{Q}(\sqrt{-d}),\ M=F(i)$, $d>2$ a squarefree integer.
- S is the set of infinite and dyadic places of F.
- $G_F=\{\mathrm{cl}(b)\in F^*/F^{*2}\mid v_P(b)\equiv 0 \bmod 2 \text{ for all } P\notin S\}$.
- $H_F=\{\mathrm{cl}(b)\in G_F\mid b\in N_{M/F}(M^*)\}$.

In [5], there are defined maps:

$$\chi_1,\chi_2: H_F\to C_S(F)/C_S^2(F),$$
$$\chi_1:\mathrm{cl}(b)\mapsto\Big[\prod_{P\notin S}P^{v_P(b)/2}\Big],\qquad \chi_2:\mathrm{cl}(b)\mapsto\Big[\prod_{P\notin S}P^{v_{\mathcal{P}}(\alpha)}\Big],$$

where $C_S(F)$ is the S-ideal class group of F, $N_{M/F}(\alpha)=b$ for $\alpha\in M$, and $\mathcal{P}$ is a place of M over P. Let $\chi=\chi_1\chi_2$. Then $\ker\chi$ is determined by the elements of order 4 of K_2O_F and the elements $a\in F^*$ with $\{-1,a\}=1$ (see [5], Prop. 2.3, or [9], Prop. 1.5).

Browkin–Schinzel ([3], Theorem 2) gave the elements of order at most 2 of K_2O_F for a real quadratic field $F=\mathbb{Q}(\sqrt{d})$:

$$\{-1,m\gamma_j\},$$

where m is an odd divisor of d and $\gamma_j=u_j+\sqrt{d}$ with $u_j^2-jw_j^2=d$, $u_j,w_j\in\mathbb{N}$, $j\in N_{F/\mathbb{Q}}(F^*)\cap\{-1,\pm2\}$, $\gamma_1=1$. We denote $N_{F/\mathbb{Q}}(F^*)$ by NF.

By Bass–Tate theorem [10], $\beta\in K_2F$, $\beta^2=\{-1,m\gamma_j\}$ if and only if $m\gamma_j\in N_{M/F}(M^*)$. On the other hand, for all $P\notin S$, the tame symbols $\tau_P\{-1,m\gamma_j\}$ equal 1, so the Hilbert symbols $\eta_P(\{-1,m\gamma_j\})$ are 1 by [2], Theorem 2. By the Minkowski–Hasse theorem, we know that: if $d\not\equiv 1 \bmod 8$, then $m\gamma_j\in N_{M/F}(M^*)$ if and only if $m>0$ and $j=1,2$; if $d\equiv 1 \bmod 8$ and $2\notin NF$, then $m\gamma_j\in N_{M/F}(M^*)$ if and only if $m>0$ and $j=1$; if $d\equiv 1 \bmod 8$ and $u^2-2w^2=d$, where $u,w\in\mathbb{N}$, $w\equiv 0 \bmod 4$, then $m\gamma_j\in N_{M/F}(M^*)$ if and only if either $j=1$, $m>0$, and $m\equiv 1 \bmod 4$, or $j=2$, $m>0$, and $m+u\equiv 2 \bmod 4$.

Suppose that $\beta\in K_2F$ and

$$\beta^2=\{-1,m\gamma_j\}\in K_2O_F. \tag{2.1}$$

We will find conditions sufficient for $\beta\in K_2O_2$.

Case 1: *$j=1$ and m is an odd positive divisor of d in* (2.1). Since $m\in N_{M/F}(M^*)$, there are $X=x_1+x_2\sqrt{d}$, $Y=y_1+y_2\sqrt{d}\in F$ and $x_1,x_2,y_1,y_2\in\mathbb{Q}$ such that

$$m=X^2+Y^2=(x_1^2+y_1^2)+(x_2^2+y_2^2)d+2(x_1x_2+y_1y_2)\sqrt{d}.$$

Hence $x_1x_2 + y_1y_2 = 0$. First we assume that x_1, x_2, y_1, y_2 are all non-zero, and put $t = x_1/y_1 = -y_2/x_2$. By the last equality, $m = (1+t^2)(y_1^2 + x_2^2 d)$. Therefore, there is a squarefree positive integer k, with each odd prime factor $p_i \equiv 1 \bmod 4$, such that the Diophantine equation

$$mkz^2 = x^2 + dy^2 \tag{2.2}$$

is solvable in $\mathbb{Z}$. If $x_1 = y_1 = 0$, take $k = d/m$; if $x_2 = y_2 = 0$, take $k = m$; if $x_1 = y_2 = 0$ or $x_2 = y_1 = 0$, take $k = 1$.

When $k \geq 2$, there are $g, h \in \mathbb{N}$ such that

$$k = g^2 + h^2. \tag{2.3}$$

Take a relatively prime solution $(x, y, z) = (a, b, c)$ of the equation (2.2) in $\mathbb{N}$. Put $\alpha_1 = a + b\sqrt{-d}$, $\alpha_2 = g + hi$, and $\alpha = \alpha_1\alpha_2$. Then $N_{M/F}(\alpha) = mk^2c^2$ and $\mathrm{cl}(m) = \mathrm{cl}(mk^2c^2) \in H_F$. Below, we discuss the value of $\chi(\mathrm{cl}(m))$. For convenience, let p be an odd prime, P a place of F over p, and $\mathcal{P}$ a place of M over P, which we denote by $P|p$ and $\mathcal{P}|P$. Suppose $p \mid mk^2c^2$.

(i) If $p \nmid k,\ p \mid m$, then $p \mid a,\ p \nmid b,\ p \nmid c$ for the relatively prime solution $(x, y, z) = (a, b, c)$ of (2.2) in $\mathbb{N}$. Hence $v_P(mk^2c^2)/2 = v_P(m)/2 = 1$ and $v_{\mathcal{P}}(\alpha) = v_{\mathcal{P}}(\alpha_1) + v_{\mathcal{P}}(\alpha_2) = 1 + 0 = 1$.

(ii) If $p \nmid k,\ p \mid c$, then $p \nmid d,\ p \nmid a,\ p \nmid b$. Hence $v_P(mk^2c^2)/2 = v_p(c)$ and $v_{\mathcal{P}}(\alpha) \equiv 0 + 0 = 0 \bmod 2$.

(iii) If $p \mid k,\ p \mid m$, then $p \parallel a,\ p \mid b,\ p \nmid c$. Hence $v_P(mk^2c^2)/2 \equiv 1 \bmod 2$ and $v_{\mathcal{P}}(\alpha) \equiv 0 + 0 \equiv 0 \bmod 2$.

(iv) If $p \mid k,\ p \nmid m,\ p \mid d$, then $p \mid a,\ p \nmid b,\ p \nmid c$. Hence $v_P(mk^2c^2)/2 = v_P(k) \equiv 0 \bmod 2$ and $v_{\mathcal{P}}(\alpha) \equiv 1 + 0 \equiv 1 \bmod 2$.

(v) If $p \mid k,\ p \nmid d$, then $p \nmid a,\ p \nmid b$ in both cases $p \mid c$ and $p \nmid c$. Hence $v_P(mk^2c^2)/2 = v_P(k) + v_P(c) \equiv 1 + v_p(c) \bmod 2$. In this case, we investigate the value of $v_{\mathcal{P}}(\alpha)$.

There is a diagram of field extensions

$$\begin{tikzcd}[column sep=small]
 & M \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F = \mathbb{Q}(\sqrt{d}) \arrow[dr, dash] & L = \mathbb{Q}(i) \arrow[d, dash] & E = \mathbb{Q}(\sqrt{-d}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Since p splits in E and L, p splits completely in M. Let $\mathrm{Gal}(M/\mathbb{Q}) = \{1, \sigma, \varrho, \sigma\varrho\}$ be the Galois group of the finite extension $M/\mathbb{Q}$, where $\sigma : \sqrt{d} \mapsto \sqrt{d},\ i \mapsto -i$ and $\varrho : \sqrt{d} \mapsto -\sqrt{d},\ i \mapsto -i$. Then $pO_M = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$, $\mathcal{P}_2 = \sigma\mathcal{P}_1,\ \mathcal{P}_3 = \varrho\mathcal{P}_1,\ \mathcal{P}_4 = \sigma\varrho\mathcal{P}_1$, $pO_F = P_1P_2$, $P_1O_M = \mathcal{P}_1\mathcal{P}_2$, $P_2O_M =$

$\mathcal{P}_3\mathcal{P}_4$. Hence we have, modulo 2,

$$\begin{cases} v_{\mathcal{P}_1}(\alpha_1) = v_{\mathcal{P}_3}(\alpha_1) \equiv 0, \\ v_{\mathcal{P}_2}(\alpha_1) = v_{\mathcal{P}_4}(\alpha_1) \equiv 1, \end{cases} \quad \text{or} \quad \begin{cases} v_{\mathcal{P}_1}(\alpha_1) = v_{\mathcal{P}_3}(\alpha_1) \equiv 1, \\ v_{\mathcal{P}_2}(\alpha_1) = v_{\mathcal{P}_4}(\alpha_1) \equiv 0, \end{cases}$$

$$\begin{cases} v_{\mathcal{P}_1}(\alpha_2) = v_{\mathcal{P}_4}(\alpha_2) \equiv 0, \\ v_{\mathcal{P}_2}(\alpha_2) = v_{\mathcal{P}_3}(\alpha_2) \equiv 1, \end{cases} \quad \text{or} \quad \begin{cases} v_{\mathcal{P}_1}(\alpha_2) = v_{\mathcal{P}_4}(\alpha_2) \equiv 1 \\ v_{\mathcal{P}_2}(\alpha_2) = v_{\mathcal{P}_3}(\alpha_2) \equiv 0. \end{cases}$$

Therefore

$$\begin{cases} v_{\mathcal{P}_1}(\alpha) = v_{\mathcal{P}_2}(\alpha) \equiv 0, \\ v_{\mathcal{P}_3}(\alpha) = v_{\mathcal{P}_4}(\alpha) \equiv 1, \end{cases} \quad \text{or} \quad \begin{cases} v_{\mathcal{P}_1}(\alpha) = v_{\mathcal{P}_2}(\alpha) \equiv 1, \\ v_{\mathcal{P}_3}(\alpha) = v_{\mathcal{P}_4}(\alpha) \equiv 0. \end{cases} \tag{2.4}$$

Consequently, $\chi(\mathrm{cl}(m)) = [cI] = [I]$, where $I\bar{I} = kO_F$, $\bar{I}$ a conjugate ideal of I. Hence $\mathrm{cl}(m) \in \ker\chi$ if and only if $[I] \in C_S^2(F)$. Let $H(F)$ be the narrow class group of F. Then, by the Gauss theorem, $[J] \in H^2(F)$, where J is an ideal of F, if and only if $N_{F/\mathbb{Q}}(J) \in NF$. On the other hand, let $[A]$ be the narrow class containing the ideal $A = (\sqrt{d})$ and $[B]$ the narrow class containing $B \mid 2$. Put $H_2(F) = \langle [A], [B] \rangle$, the group generated by $[A]$, $[B]$. Then

$$C_S(F) = H(F)/H_2(F).$$

Therefore, we have

$$\begin{aligned} \mathrm{cl}(m) = \mathrm{cl}(mk^2c^2) \in \ker\chi \\ &\Leftrightarrow\ [I] \in C_S^2(F),\ \text{i.e., } [I][X] \in H^2(F),\ \text{where } [X] \in H_2(F) \\ &\Leftrightarrow\ N_{F/\mathbb{Q}}(IX) \in NF,\ \text{i.e., } k\varepsilon \in NF,\ \text{where } \varepsilon \in \{\pm 1, \pm 2\} \\ &\Leftrightarrow\ \text{the following equation is solvable in } \mathbb{Z}\text{:} \end{aligned}$$

$$\varepsilon k z^2 = x^2 - dy^2. \tag{2.5}$$

By (2.2) and (2.5), we get:

Theorem 2.1 ([14], Theorem 2.2). *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ a squarefree integer. Then, for every odd positive divisor m of d, there is $\beta \in K_2O_F$ with $\beta^2 = \{-1, m\}$ if and only if there is $\varepsilon \in \{\pm 1, \pm 2\}$ such that*

$$\left(\frac{\varepsilon d m^{-1}}{p}\right) = \left(\frac{\varepsilon m}{l}\right) = 1 \quad \textit{for any odd primes } p \mid m,\ l \mid dm^{-1}. \tag{2.6}$$

By [9], Prop. 1.5, and the preceding argument, we can find $y \in F^*$ such that $v_P(N_{M/F}(\alpha))/2 + v_{\mathcal{P}}(\alpha) + v_P(y) \equiv 0 \bmod 2$ for all $P \notin S$. Set

$$\begin{aligned} \beta &= \mathrm{tr}_{M/F}(\{i, \alpha\})\{-1, y\} \\ &= \mathrm{tr}_{M/F}(\{i, \alpha_1\})\,\mathrm{tr}_{M/F}(\{i, \alpha_2\})\{-1, y\} \\ &= \left\{-\frac{\sqrt{d}b}{a}, \frac{kmc^2}{a^2}\right\}\left\{-\frac{h}{g}, \frac{k}{g^2}\right\}\{-1, c\delta\}\{-1, e + f\sqrt{d}\}, \end{aligned} \tag{2.7}$$

where $(x,y,z)=(e,f,t)$ is a relatively prime solution of (2.5) in $\mathbb{N}$ and $\delta\,|\,k$, $\delta\in\mathbb{N}$. Then $\beta\in K_2O_F$ and $\beta^2=\{-1,m\}$.

In particular, suppose that (m,ε), $\varepsilon>0$, satisfies (2.6). Then take $k=\varepsilon$ in (2.2) and set

$$\beta=\left\{\frac{-\sqrt{d}b}{a},\frac{\varepsilon mc^2}{a^2}\right\}\{-1,c\}, \tag{2.8}$$

where $(x,y,z)=(a,b,c)$ is a relatively prime solution of $\varepsilon mz^2=x^2+dy^2$ in $\mathbb{N}$. Then $\beta\in K_2O_F$ and $\beta^2=\{-1,m\}$.

Case 2: *$j=2$ and m is an odd positive divisor of d in* (2.1). Since $2\in NF$, we have $u^2-2w^2=d,\ u,w\in\mathbb{N}$, and $\gamma_2=u+\sqrt{d}$. If $d\equiv 1 \bmod 8$, we take $w\equiv 0 \bmod 4$. Hence,

$$\begin{gathered}w^2+(u+w+\sqrt{d})^2=2(u+w)(u+\sqrt{d}),\\(u+2w)^2+d=2(u+w)^2,\end{gathered} \tag{2.9}$$

so d and $u+w$ are relatively prime. We assume $m\gamma_2\in N_{M/F}(M^*)$. Then $(u+w)m\in N_{M/F}(M^*)$ by (2.9). By the same method as in the first case, there is a squarefree positive integer k, with each odd prime divisor $p_i\equiv 1 \bmod 4$, such that the Diophantine equation

$$m(u+w)kz^2=x^2+dy^2,\qquad k=g^2+h^2,\ g,h\in\mathbb{N}, \tag{2.10}$$

is solvable in $\mathbb{Z}$. Take $\alpha_1=w+(u+w+\sqrt{d})i$, $\alpha_2=a+b\sqrt{-d}$, $\alpha_3=g+hi$, $\alpha=\alpha_1\alpha_2\alpha_3$, where $(x,y,z)=(a,b,c)$ is a relatively prime solution of (2.10) in $\mathbb{N}$. Then $N_{M/F}(\alpha)=2m(u+\sqrt{d})k^2(u+w)^2c^2$ and $\mathrm{cl}(m(u+\sqrt{d}))=\mathrm{cl}(N_{M/F}(\alpha))\in H_F$. We discuss the value of $\chi(\mathrm{cl}(m(u+\sqrt{d})))$. For p an odd prime, let $P|p$ in F and $\mathcal{P}|P$ in M. Suppose $P\,|\,N_{M/F}(\alpha)$. There are the following cases:

(i) If $p\nmid k,\ p\,|\,m$, then $p\nmid u+w,\ p\,|\,a,\ p\nmid b,\ p\nmid c,\ P\nmid u+\sqrt{d}$ for the relatively prime solution $(x,y,z)=(a,b,c)$ of (2.10) in $\mathbb{N}$. Hence $v_P(N_{M/F}(\alpha))/2=v_P(m)/2=1$ and $v_{\mathcal{P}}(\alpha)=v_{\mathcal{P}}(\alpha_2)=v_{\mathcal{P}}(a+b\sqrt{-d})=1$.

(ii) If $p\nmid k,\ P\,|\,u+\sqrt{d}$, then $p\nmid u+w,\ p\nmid d$. Hence $v_P(N_{M/F}(\alpha))/2=v_P(u+\sqrt{d})/2+v_p(c)$ and

$$\begin{aligned}v_{\mathcal{P}}(\alpha)&\equiv v_{\mathcal{P}}(\alpha_1)+0\equiv v_{\mathcal{P}}((u+\sqrt{d})i+w(1+i))\equiv v_{\mathcal{P}}(w)\\&\equiv v_P(u+\sqrt{d})/2 \bmod 2\end{aligned}$$

by (2.9) and $(u+\sqrt{d})(u-\sqrt{d})=2w^2$.

(iii) If $p\nmid k,\ p\,|\,u+w$, then $P\nmid u+\sqrt{d},\ p\nmid d$. Without loss of generality, assume $p\nmid a,\ p\nmid b$. Hence $v_P(N_{M/F}(\alpha))/2=v_p(u+w)+v_p(c)$ and

$$\begin{aligned}v_{\mathcal{P}}(\alpha)&=v_{\mathcal{P}}(\alpha_1)+v_{\mathcal{P}}(\alpha_2)=v_{\mathcal{P}}((u+w)i+(w+\sqrt{-d}))+v_{\mathcal{P}}(\alpha_2)\\&=v_{\mathcal{P}}((w+\sqrt{-d})(a+b\sqrt{-d})).\end{aligned}$$

(iv) If $p\,|\,k,\ p\,|\,m$, then $p\,\|\,a,\ p\,|\,b,\ p\nmid c$. Hence $v_P(N_{M/F}(\alpha))/2 = v_P(m)/2 + v_P(k) \equiv 1 \bmod 2$ and $v_{\mathcal{P}}(\alpha) = v_{\mathcal{P}}(\alpha_2) + v_{\mathcal{P}}(\alpha_3) \equiv 0 + 0 = 0 \bmod 2$.

(v) If $p\,|\,k,\ p\,|\,d,\ p\nmid m$, then $p\,|\,a,\ p\nmid b,\ p\,|\,c$. Hence $v_P(N_{M/F}(\alpha))/2 = v_P(k) \equiv 0 \bmod 2$ and $v_{\mathcal{P}}(\alpha) = v_{\mathcal{P}}(\alpha_2) + v_{\mathcal{P}}(\alpha_3) \equiv 1 + 0 = 1 \bmod 2$.

(vi) If $p\,|\,k,\ p\nmid d$, then $p\nmid a,\ p\nmid b$. Hence we have $v_P(N_{M/F}(\alpha))/2 = v_p(k)+v_p(u+w)+v_P(u+\sqrt{d})/2+v_p(c)$. Suppose $P\,|\,u+\sqrt{d}$. Then $v_{\mathcal{P}}(\alpha_1) = v_{\mathcal{P}}(u+\sqrt{d}+w(1+i)) = v_p(w) = v_P(u+\sqrt{d})/2$ as $(u+\sqrt{d})(u-\sqrt{d}) = 2w^2$. By the process of proving (v) in the first case, we can get the same result for $v_{\mathcal{P}}(\alpha_2\alpha_3)$ as in (2.4). Suppose $p\,|\,u+w$ and, without loss of generality, assume $p\nmid a,\ p\nmid b$. Then $v_{\mathcal{P}}(\alpha_1\alpha_2) = v_{\mathcal{P}}((w+\sqrt{-d})(a+b\sqrt{-d}))$ by (iii). By the process of proving (v) in Case 1, we can get the same result for $v_{\mathcal{P}}(\alpha)$ as in (2.4). Suppose $p\nmid u+w,\ P\nmid u+\sqrt{d}$. Then we can get the same result for $v_{\mathcal{P}}(\alpha)$ as in (2.4).

Consequently, $\chi(\mathrm{cl}(m(u+\sqrt{d}))) = [c\delta_1 I]$, where $\delta_1\,|\,u+w$ from (iii) and $I\bar{I} = kO_F$, $\bar{I}$ a conjugate ideal of I. By the method of Case 1, we have $\chi(\mathrm{cl}(m(u+\sqrt{d}))) \in \ker\chi$ if and only if the following equation is solvable in $\mathbb{Z}$, $\varepsilon \in \{\pm 1\}$:

$$\varepsilon k z^2 = x^2 - dy^2. \tag{2.11}$$

By (2.10) and (2.11), we get

Theorem 2.2 ([14], Theorem 3.3). *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ a squarefree integer. Suppose that $d = u^2 - 2w^2$ with $u, w \in \mathbb{N}$. Then, for every odd positive divisor m of d, there is $\beta \in K_2O_F$ with $\beta^2 = \{-1, m(u+\sqrt{d})\}$ if and only if there is $\varepsilon \in \{\pm 1\}$ such that*

$$\begin{aligned} &\left(\frac{\varepsilon d m^{-1}(u+w)}{p}\right) = 1 \qquad \textit{for every odd prime } p\,|\,m,\\ &\left(\frac{\varepsilon m(u+w)}{l}\right) = 1 \qquad \textit{for every odd prime } l\,|\,dm^{-1}. \end{aligned} \tag{2.12}$$

Suppose that (m,ε) satisfies (2.12). Then, by [9], Prop. 1.5 and the preceding argument, we can find $y \in F^*$ such that $v_P(N_{M/F}(\alpha))/2 + v_{\mathcal{P}}(\alpha) + v_P(y) \equiv 0 \bmod 2$ for all $P \notin S$. Set

$$\begin{aligned} \beta = &\left\{-\frac{u+w+\sqrt{d}}{w}, \frac{2(u+w)(u+\sqrt{d})}{w^2}\right\}\\ &\times\left\{-\frac{b\sqrt{d}}{a}, \frac{m(u+w)kc^2}{a^2}\right\}\\ &\times\left\{-\frac{h}{g}, \frac{k}{g^2}\right\}\{-1, c\delta_1\delta_2(e+f\sqrt{d})\}, \end{aligned} \tag{2.13}$$

where $\delta_1 \mid u+w,\ \delta_2 \mid k,\ \delta_i \in \mathbb{N},\ (x,y,z) = (a,b,c)$ is a relatively prime solution of (2.10) in $\mathbb{N}$, and $(x,y,z) = (e,f,t)$ is a relatively prime solution of (2.11) in $\mathbb{N}$. Then $\beta \in K_2O_F$ and $\beta^2 = \{-1, m(u+\sqrt{d})\}$.

In particular, $\varepsilon > 0$. We can take $k = 1$ in (2.10) and set

$$\beta = \left\{-\frac{u+w+\sqrt{d}}{w}, \frac{2(u+w)(u+\sqrt{d})}{w^2}\right\} \times \left\{-\frac{b\sqrt{d}}{a}, \frac{m(u+w)c^2}{a^2}\right\}\{-1, c\delta\}, \tag{2.14}$$

where $\delta \mid u+w,\ \delta \in \mathbb{N}$, and $(x,y,z) = (a,b,c)$ is a relatively prime solution of (2.10) in $\mathbb{N}$ with $k = 1$. Then $\beta \in K_2O_F$ and $\beta^2 = \{-1, m(u+\sqrt{d})\}$.

With the preceding method, we can also discuss an imaginary quadratic field $E = \mathbb{Q}(\sqrt{-d})$ to get results of [13] and the forms of elements of order 4 of K_2O_E.

Theorem 2.3 ([13], Theorems 3.10 and 3.13). *Let $F = \mathbb{Q}(\sqrt{d}),\ E = \mathbb{Q}(\sqrt{-d}),\ d > 2$ a squarefree integer, and m an odd positive divisor of d.*

(1) *There is $\beta \in K_2O_E$ with $\beta^2 = \{-1, m\}$ if and only if $\varepsilon m \in NF$, where $\varepsilon \in \{1, 2\}$.*

(2) *If $-d = u^2 - 2w^2,\ u, w \in \mathbb{N}$, then there is $\beta \in K_2O_E$ with $\beta^2 = \{-1, m(u+\sqrt{-d})\}$ if and only if $m(u+w) \in NF$.*

Similarly, suppose $m \mid d,\ \varepsilon m \in NF$, and set

$$\beta = \left\{-\frac{b\sqrt{-d}}{a}, \frac{\varepsilon m c^2}{a^2}\right\}\{-1, c\}, \tag{2.15}$$

where $(x,y,z) = (a,b,c)$ is a relatively prime solution of $\varepsilon z^2 = x^2 - dy^2$ in $\mathbb{N}$. Then $\beta \in K_2O_E$ and $\beta^2 = \{-1, m\}$.

Suppose $m \mid d,\ -d = u^2 - 2w^2,\ u, w \in \mathbb{N},\ m(u+w) \in NF$, and set

$$\beta = \left\{-\frac{u+w+\sqrt{-d}}{w}, \frac{2(u+w)(u+\sqrt{-d})}{w^2}\right\} \times \left\{-\frac{b\sqrt{-d}}{a}, \frac{m(u+w)c^2}{a^2}\right\}\{-1, c\delta\}, \tag{2.16}$$

where $\delta \mid u+w,\ \delta \in \mathbb{N}$, and $(x,y,z) = (a,b,c)$ is a relatively prime solution of $m(u+w)z^2 = x^2 - dy^2$ in $\mathbb{N}$. Then $\beta \in K_2O_E$ and $\beta^2 = \{-1, m(u+\sqrt{-d})\}$.

3. Real quadratic fields. To investigate whether $\varepsilon > 0$ in (2.6) and (2.12), we divide them into two cases.

Definition 3.1. Let $F=\mathbb{Q}(\sqrt{d})$, $d>2$ a squarefree integer. Set

$$S_0=\{m\,|\,m \text{ is an odd positive divisor of } d\},$$
$$S_1=\{\varepsilon m \mid m\in S_0 \text{ and } (m,\varepsilon),\ \varepsilon>0, \text{ satisfies (2.6) or (2.12)}\},$$
$$S_2=\{|\varepsilon|m \mid m\in S_0 \text{ and } (m,\varepsilon),\ \varepsilon<0, \text{ satisfies (2.6) or (2.12)}, \quad \text{but } m,2m\notin S_1\}.$$

In [17], we give the relation between S_1 and $C(E)$ (the narrow class group of the field $E=\mathbb{Q}(\sqrt{-d})$). In fact, if -1 or -2 is in NF, then $S_2=\emptyset$; if $d\equiv -1 \bmod 8$, then $S_2=\emptyset$ by the quadratic reciprocity law or by [17], Lemma 3.4. Below, we explain why $S_2\neq\emptyset$.

Lemma 3.1. *Let $\pi : B\to (c)$ be a surjective homomorphism of a finite Abelian p-group B. If $b\in B$ is an element of minimal order such that $\pi(b)=c$, then there exists a subgroup B' of B satisfying $B=(b)\times B'$ and $\pi(B')\subset(c^p)$.*

Proof. Since B is Abelian, we have $B=(b_1)\times\ldots\times(b_t)$. From the surjectivity of π it follows that $(\pi(b_j))=(c)$ for some j. We assume that b_1 is an element of minimal order among all b_j satisfying $(\pi(b_j))=(c)$; we can also assume that $\pi(b_1)=c$, because b_1 can be replaced by some power of b_1 if necessary.

For $i\geq 2$, if $(\pi(b_i))=(c)$, i.e., $\pi(b_i)=c^t$ with $p\nmid t$, then we take $b_i'=b_1^{p-t}b_i$. If $(\pi(b_i))\neq(c)$, i.e., $(\pi(b_i))\subset(c^p)$, then we take $b_i'=b_i$. Then the group B' generated by $b_2',\ldots,b_t'$ satisfies $B=(b_1)\times B'$ and $\pi(B')\subset(c^p)$.

Now let $x\in B$ be an element of minimal order satisfying $\pi(x)=c$. Then $x=b_1^jb'$ with $b'\in B'$. Consequently, $c=\pi(x)=\pi(b_1)^j\pi(b')=c^jc^{pk}$ for some $k\in\mathbb{Z}$. Hence $p\nmid j$.

From $1=x^{o(x)}=b_1^{jo(x)}b'^{o(x)}$, we get $b_1^{jo(x)}\in B'$, and hence $b_1^{o(x)}=1$. Therefore $o(b_1)\leq o(x)$. On the other hand, $o(x)\leq o(b_1)$, by the minimality of $o(x)$. It follows that $o(x)=o(b_1)$, and consequently $B=(x)\times B'$.

Theorem 3.1. *Let $F=\mathbb{Q}(\sqrt{d})$, $d>2$ squarefree.*

(1) *If $d\not\equiv\pm1 \bmod 8$, then $(K_2O_F)_2=(\alpha_1)\times(\alpha_2)\times H$, where $\alpha_1=\{-1,-1\}$, $H\subset\Re_2F$, and α_2 is an element of minimal order of $(K_2O_F)_2$ with Hilbert symbol $\eta_{\infty_i}(\alpha_2)=(-1)^i$, ∞_i real places, $i=1,2$.*

(2) *If $d\equiv 1 \bmod 8$, then $(K_2O_F)_2=(\alpha_1)\times(\alpha_2)\times(\alpha_3)\times H$, where $\alpha_1=\{-1,-1\}$, $H\subset\Re_2F$, and α_2, α_3 are elements of minimal order of K_2O_F satisfying $\eta_{\infty_i}(\alpha_2)=(-1)^i$, $\eta_{\infty_i}(\alpha_3)=1$, $\eta_{P_i}(\alpha_3)=-1$, $P_i\,|\,2$, $i=1,2$; moreover, either α_2 or α_3 is an element of order 2.*

(3) *If $d\equiv -1 \bmod 8$, then $(K_2O_F)_2=(\alpha_1)\times(\alpha_2)\times H$, where $\alpha_1=\{-1,-1\}$ and α_2 is an element of minimal order of K_2O_F satisfying $\eta_{\infty_i}(\alpha)=(-1)^i$, $i=1,2$. Moreover α_2 is of order at least 8.*

Proof. By [2], Theorem 2, or [10], §15, we obtain the commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & & \\
0 \arrow[r] & \Re_2 F \arrow[r] \arrow[d] & K_2F \arrow[r, "\eta"] \arrow[d, "\mathrm{id}"] & \coprod_{P\,\mathrm{nonc}} \mu_P \arrow[r] \arrow[d, "\lambda"] & \mu \arrow[r] & 0 \\
0 \arrow[r] & K_2O_F \arrow[r] & K_2F \arrow[r, "\tau"] \arrow[d] & \coprod_{P\,\mathrm{fin.}} \overline{F}_P^* \arrow[r] & 0 & \\
 & & 0 & & &
\end{tikzcd}$$

where the homomorphism λ is defined as follows:

$$\lambda : \coprod_{P\,\mathrm{nonc}} \mu_P \to \coprod_{P\,\mathrm{fin.}} \overline{F}_P^*,$$

$$\lambda(a_P) = \begin{cases} 1 & \text{if } P \text{ is real,} \\ a_P^{m_P/(NP-1)} & \text{if } P \text{ is finite,} \end{cases}$$

where μ_P is the group of roots of unity in the local completion field F_P, $a_P \in \mu_P$, $m_P = |\mu_P|$, $\overline{F}_P$ is the residue class field of the completion field F_P, and $NP = |\overline{F}_P|$.

By diagram chase, we get the exact sequence

$$0 \to \Re_2 F \to K_2O_F \xrightarrow{\eta} \operatorname{Im}\eta \cap \ker\lambda \to 0.$$

Since the group K_2O_F is finite, we obtain the exact sequence of their 2-Sylow subgroups

$$0 \to (\Re_2 F)_2 \to (K_2O_F)_2 \xrightarrow{\eta} (\operatorname{Im}\eta \cap \ker\lambda)_2 \to 0.$$

If $d \equiv -3 \bmod 9$, then $m_P = 3(NP-1)$ for P a place over 3 and $m_P = NP-1$ for all $P \notin S$ and $P \nmid 3$; otherwise $m_P = NP-1$ for $P \notin S$. Therefore $(\operatorname{Im}\eta \cap \ker\lambda)_2 = \operatorname{Im}\eta \cap (\mu_{\infty_1} \times \mu_{\infty_2} \times \coprod_{P|2} \mu_P^{NP-1})$.

(1) If $d \not\equiv \pm 1 \bmod 8$, then

$$(K_2O_F)_2/(\Re_2 F)_2 \cong \operatorname{Im}\eta \cap (\mu_{\infty_1} \times \mu_{\infty_2} \times \mu_P^{NP-1}) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2),$$

where $P \mid 2$ and $\mu_{\infty_i} = \mu_P^{NP-1} = \{\pm 1\}$. Since $\eta(\alpha_1) = \eta(\{-1,-1\}) = \beta_1 = (-1,-1,1)$ and $\beta_2 = (-1,1,-1)$ are two generators of $(\operatorname{Im}\eta \cap \ker\lambda)_2$ we have $(K_2O_F)_2 = (\alpha_1) \times \eta^{-1}(\beta_2)$, so we get α_2 by Lemma 3.1.

(2) If $d \equiv 1 \bmod 8$, then

$$\begin{aligned}(K_2O_F)_2/(\Re_2 F)_2 &\cong \operatorname{Im}\eta \cap (\mu_{\infty_1} \times \mu_{\infty_2} \times \mu_{P_1} \times \mu_{P_2}) \\ &\cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2),\end{aligned}$$

where $P_i \mid 2$ and $\mu_{P_i} = \{\pm 1\}$, $i = 1, 2$. Since $\eta(\alpha_1) = \eta(\{-1, -1\}) = \beta_1 = (-1, -1, -1, -1)$, $\beta_2 = (1, -1, 1, -1)$, $\beta_3 = (1, 1, -1, -1)$ are three generators of $(\operatorname{Im}\eta \cap \ker\lambda)_2$, we have $(K_2O_F)_2 = (\alpha_1) \times \eta^{-1}\{\beta_2, \beta_3\}$, where $\alpha_1 = \{-1, -1\}$.

Suppose $-1 \in NF$. Take $\alpha_2 = \{-1, u + \sqrt{d}\}$, where $u^2 + w^2 = d$, $u, w \in \mathbb{N}$. Hence $\eta(\alpha_2) = \beta_2$, so we get α_3 by Lemma 3.1.

Suppose $-1 \notin NF$. There is a prime divisor $p \equiv 3 \bmod 4$ of d. Take $\alpha_3 = \{-1, p\}$, so we also get α_2 by Lemma 3.1.

(3) If $d \equiv -1 \bmod 8$, then

$$(K_2O_F)_2/(\Re_2 F)_2 \cong \operatorname{Im}\eta \cap (\mu_{\infty_1} \times \mu_{\infty_2} \times \mu_P) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(4),$$

where $\mu_P = \{\pm 1, \pm i\}$ and $P \mid 2$. As $\eta(\alpha_1) = \eta(\{-1, -1\}) = \beta_1 = (-1, -1, 1)$ and $\beta_2 = (-1, 1, i)$ are two generators of $(\operatorname{Im}\eta \cap \ker\lambda)_2$, we have $(K_2O_F)_2 = (\alpha_1) \times \eta^{-1}(\beta_2)$. By [3], Theorem 2, we know that $r_2(K_2O_F) - r_2(\Re_2 F) = 1$ and $\alpha_1 = \{-1, -1\} \notin \Re_2 F$. Therefore, we get α_2 by Lemma 3.1, which is of order at least 8.

In Theorem 3.1, if α_2 and α_3 are elements of minimal order of K_2O_F, then there are also direct decompositions for K_2O_F.

Corollary 3.1. *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ a squarefree integer.*

(1) *If $S_2 \neq \emptyset$, then α_2 must be of order* 4 *in Theorem* 3.1 *and* $r_4(K_2O_F) = r_4(\Re_2 F) + 1$.

(2) *If $S_2 = \emptyset$ and $-1, -2 \notin NF$, then there is an 8-order element in K_2O_F.*

Proof. (1) Since $S_2 \neq \emptyset$ and $-1, -2 \notin NF$, we have $d \not\equiv -1 \bmod 8$ and $o(\alpha_2) > 2$ in Theorem 3.1 by [3], Theorem 2. Also $S_2 \neq \emptyset$ implies that $o(\alpha_2) \leq 4$ by (2.7) or (2.13). Therefore, α_2 must be of order 4 and $r_4(K_2O_F) = r_4(\Re_2 F) + 1$.

(2) Since $-1, -2 \notin NF$, we have $o(\alpha_2) > 2$ by [3], Theorem 2. Since $S_2 = \emptyset$, also $o(\alpha_2) > 4$ by (2.8) or (2.14). Therefore, α_2 is of order at least 8.

Theorem 3.2. *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ a squarefree integer, $d \equiv 1 \bmod 8$, $-1 \in NF$, and $2 \notin NF$. Then $o(\alpha_3) = 4$ in Theorem* 3.1 *if and only if there is an equation $\varepsilon m z^2 = x^2 + dy^2$ with $m \in S_0$, $m \neq 1, d$, and $\varepsilon \in \{1, 2\}$, which has a relatively prime solution $(x, y, z) = (a, b, c)$ in $\mathbb{N}$ such that either $m \equiv 1 \bmod 8$ and $c \equiv 3 \bmod 4$, or $m \equiv 5 \bmod 8$ and $c \equiv 1 \bmod 4$.*

Proof. Since $-1 \in NF$ and $2 \notin NF$, we have $o(\alpha_3) > 2$. Suppose that $\varepsilon m \in S_1$, $m \neq 1, d$, $\varepsilon \in \{1, 2\}$, i.e., the Diophantine equation $\varepsilon m z^2 =$

x^2+dy^2 has a relatively prime solution $(x,y,z)=(a,b,c)$ in $\mathbb{N}$. Then $\beta=\{-\frac{b\sqrt{d}}{a},\frac{\varepsilon mc^2}{a^2}\}\{-1,c\}\in K_2O_F$ and $\beta^2=\{-1,m\}$. Now, we discuss whether $\eta_{P_i}(\beta)=-1$, $P_i\,|\,2$, $i=1,2$. Since $d\equiv 1 \bmod 8$, the local field $Q_2(\sqrt{d})\cong Q_2$. In the local field Q_2, we compute the value of the Hilbert symbols $\left[-\frac{b\sqrt{d}}{a},\frac{\varepsilon mc^2}{a^2}\right]_2$.

(i) If $\varepsilon=2$ and $m\equiv 1 \bmod 8$, then a, b, c are odd and $-b\sqrt{d}/a$ is a solution of the equation

$$X^2=\varepsilon mc^2/a^2-1. \tag{3.17}$$

Since $\varepsilon mc^2/a^2-1\equiv 1 \bmod 16$, the equation (3.17) has two solutions $\gamma\equiv 1$ or 7 mod 8 by the Hensel lemma. By the table in [16], p. 250, $[-b\sqrt{d}/a,\varepsilon mc^2/a^2]_2=[\gamma,2]_2=1$.

(ii) If $\varepsilon=2$ and $m\equiv 5 \bmod 8$, then a, b, c are all odd, so $\varepsilon mc^2/a^2-1\equiv 9 \bmod 16$. Hence the equation (3.17) has two solutions $\gamma\equiv 3$ or $5 \bmod 8$ by the Hensel lemma. By the table in [16], p. 250, $[-b\sqrt{d}/a,\varepsilon mc^2/a^2]_2=[\gamma,2]_2=-1$.

(iii) If $\varepsilon=1$, $m\equiv 1 \bmod 8$ and $\varepsilon mc^2/a^2\in Q_2^2$, then $[-b\sqrt{d}/a,\varepsilon mc^2/a^2]_2=1$.

(iv) If $\varepsilon=1$, $m\equiv 5 \bmod 8$, then a or $b\equiv 2 \bmod 4$, and c is odd. Hence, by the table in [16], p. 250, $[-b\sqrt{d}/a,\varepsilon mc^2/a^2]_2=[\gamma,5]_2=-1$, where $\gamma\equiv 2$ or $6 \bmod 8$.

Therefore

$$\left[-\frac{b\sqrt{d}}{a},\frac{\varepsilon mc^2}{a^2}\right]_2=\begin{cases}1 & \text{if } m\equiv 1 \bmod 8,\\ -1 & \text{if } m\equiv 5 \bmod 8.\end{cases}$$

By the same table,

$$[-1,c]_2=\begin{cases}1 & \text{if } c\equiv 1 \bmod 4,\\ -1 & \text{if } c\equiv 3 \bmod 4.\end{cases}$$

In Theorem 3.1, $\alpha_3=\beta$, i.e., $\eta_{P_i}(\beta)=-1$, $P_i\,|\,2$, $i=1,2$, if and only if either $m\equiv 1 \bmod 8$ and $c\equiv 3 \bmod 4$, or $m\equiv 5 \bmod 8$ and $c\equiv 1 \bmod 4$.

Suppose that $(x,y,z)=(a',b',c')$ is another relatively prime solution of the equation $\varepsilon mz^2=x^2+dy^2$ in $\mathbb{N}$ with $c'\equiv c+2 \bmod 4$. We can also get β' by (2.7). But $\eta_{P_i}(\beta)=-\eta_{P_i}(\beta')$, i.e., $\eta_{P_i}(\beta\beta')=-1$, $P_i\,|\,2$, $i=1,2$. So $\alpha_3=\beta\beta'$ must be of order 2 in K_2O_F in contradiction with the assumption. Hence we obtain

COROLLARY 3.2. *Let $d=p_1\dots p_{r+s}\equiv 1 \bmod 8$, with each prime $p_i\equiv 1 \bmod 4$, $r,s\geq 1$, and some prime $p_i\equiv 5 \bmod 8$. If the Diophantine equation $\varepsilon mz^2=x^2+dy^2$, $\varepsilon\in\{1,2\}$, $m=p_1\dots p_r$, has a non-trivial solution in $\mathbb{Z}$, then for every relatively prime solution $(x,y,z)=(a,b,c)$ of this equation in $\mathbb{N}$ we have $c\equiv 1$ or $3 \bmod 4$.*

If $d = p_1 \dots p_r \equiv 1 \bmod 8$, with each prime $p_i \equiv 1 \bmod 8$, and $u^2 - 2w^2 = d,\ u, w \in \mathbb{N},\ w \equiv 0 \bmod 4,\ u \equiv 1 \bmod 4$, we can also get a result similar to Corollary 3.2.

Next, we investigate the property of $c \equiv 1$ or $3 \bmod 4$. In particular, if $F = \mathbb{Q}(\sqrt{d}),\ d = p_1 p_2$, with each prime $p_i \equiv 5 \bmod 8$, we get:

LEMMA 3.2. *Let $F = \mathbb{Q}(\sqrt{p_1 p_2}),\ E = \mathbb{Q}(\sqrt{-p_1 p_2})$, with each prime $p_i \equiv 5 \bmod 8$. By the Legendre theorem the Diophantine equation*

$$x^2 + p_1 p_2 y^2 = \varepsilon p_1 z^2, \qquad \varepsilon \in \{1, 2\}, \tag{3.18}$$

has a relatively prime solution $(x, y, z) = (a, b, c)$ in $\mathbb{N}$. Then $c \equiv 1 \bmod 4$ if and only if $16 \mid h(-p_1 p_2)$, which is the class number of the field $E = \mathbb{Q}(\sqrt{-p_1 p_2})$; in other words, $c \equiv 3 \bmod 4$ if and only if $8 \parallel h(-p_1 p_2)$.

Proof. By genus theory, $r_2(C(E)) = 2$, where $C(E)$ is the class group of E. If $\left(\frac{p_2}{p_1}\right) = 1$, the Diophantine equation $x^2 + p_1 p_2 y^2 = p_1 z^2$ is solvable in $\mathbb{Z}$; if $\left(\frac{p_2}{p_1}\right) = -1$, the Diophantine equation $x^2 + p_1 p_2 y^2 = 2 p_1 z^2$ is solvable in $\mathbb{Z}$.

Let P be an ideal of E with $P^2 = \varepsilon p_1 O_E$. Since (3.18) has a relatively prime solution $(x, y, z) = (a, b, c)$ in $\mathbb{N}$, we have $(a + b\sqrt{-p_1 p_2}) O_E = P C^2$, where $C\overline{C} = c O_E$, $\overline{C}$ a conjugate ideal of C. Hence $[P] = [C]^2 \in C^2(E)$, so $8 \mid h(-p_1 p_2)$ by genus theory. It is clear that

$$\left(\frac{-p_1 p_2}{c}\right) = \left(\frac{-1}{c}\right)\left(\frac{c}{p_1}\right)\left(\frac{c}{p_2}\right) = 1$$

by (3.18).

Assume that $c \equiv 1 \bmod 4$, i.e.,

$$\begin{aligned}
&\left(\frac{-1}{c}\right) = 1 \\
&\Leftrightarrow\ \left(\frac{c}{p_1}\right)\left(\frac{c}{p_2}\right) = 1,\ \text{i.e.,}\ \left(\frac{c}{p_1}\right) = \left(\frac{c}{p_2}\right) \\
&\Leftrightarrow\ \text{the Diophantine equation } \varepsilon' c z^2 = x^2 + p_1 p_2 y^2,\ \varepsilon' \in \{1, 2\}, \text{ is solvable} \\
&\qquad \text{in } \mathbb{Z} \\
&\Leftrightarrow\ N_{F/\mathbb{Q}}(P'C) \in NF,\ \text{where } P' \text{ is an ideal of } E \text{ such that } P'^2 = \varepsilon' O_E, \\
&\qquad \text{by the Gauss theorem} \\
&\Leftrightarrow\ [P'C] \in C^2(E),\ \text{i.e., } [C]^2 \in C^4(E) \\
&\Leftrightarrow\ 16 \mid h(-p_1 p_2).
\end{aligned}$$

Hence, Lemma 3.2 follows.

THEOREM 3.3. *Let $F = \mathbb{Q}(\sqrt{p_1p_2})$, $E = \mathbb{Q}(\sqrt{-p_1p_2})$, with each prime $p_i \equiv 5 \bmod 8$. Then $(K_2O_F)_2 \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(4)$ if and only if $16 \mid h(-p_1p_2)$; in other words, K_2O_F has an element of order 8 if and only if $8 \parallel h(-p_1p_2)$.*

Proof. This follows from Lemma 3.2 and Theorem 3.2.

EXAMPLE 1: $F = \mathbb{Q}(\sqrt{5\cdot 13})$. Since the Diophantine equation $x^2 + 5\cdot 13y^2 = 10z^2$ has a solution $(x,y,z) = (5,1,3)$, we have $8 \parallel h(-5\cdot 13)$ and K_2O_F has an element of order 8 by Lemma 3.2 and Theorem 3.2.

EXAMPLE 2: $F = \mathbb{Q}(\sqrt{5\cdot 37})$. Since the Diophantine equation $x^2 + 5\cdot 37y^2 = 10z^2$ has a solution $(x,y,z) = (25,1,9)$, we have $(K_2O_F)_2 \cong \mathbb{Z}/(2)\oplus\mathbb{Z}/(2)\oplus\mathbb{Z}/(4)$ and $16 \mid h(-5\cdot 37)$.

THEOREM 3.4. *Let $F=\mathbb{Q}(\sqrt{d})$, $d>2$ a squarefree integer, $d\equiv -1 \bmod 8$, and $2 \notin NF$. Then*

$$r_4(K_2O_F) = \begin{cases} r_4(\Re_2F)+1 & \text{if } \varepsilon m \in S_1,\ m \equiv \pm 3 \bmod 8, \\ r_4(\Re_2F) & \text{otherwise.} \end{cases}$$

Moreover, in the second case, there is an element of order 16 in K_2O_F.

Proof. Since $d \equiv -1 \bmod 8$, we have $S_2 = \emptyset$ by [17], Lemma 3.4. If $\varepsilon m \in S_1$, then $\beta = \{-\frac{b\sqrt{d}}{a}, \frac{\varepsilon mc^2}{a^2}\}\{-1,c\} \in K_2O_F$ and $\beta^2 = \{-1,m\}$, where $(x,y,z) = (a,b,c)$ is a relatively prime solution of $\varepsilon mz^2 = x^2+dy^2$ in $\mathbb{N}$.

In the completion field $F_P \cong Q_2(i)$, $P \mid 2$, we have $\eta_P\{-1,c\} = [-1,c]_P = 1$ by the Artin–Hasse theorem [11]. Let $\delta = -b\sqrt{d}/a$, $\varepsilon mb^2/a^2 = 1+\delta^2$. Then

$$\begin{aligned}\eta_P(\beta) &= [\delta, 1+\delta^2]_P[-1,c]_P = [\delta,(1+i\delta)(1-i\delta)]_P \\ &= [1+\delta^2, i]_P[1+i\delta,-1]_P = [\varepsilon m, i]_P[a+bi\sqrt{d},-1]_P.\end{aligned}$$

Since $d \equiv -1 \bmod 8$, we have $a+bi\sqrt{d} \in Q_2$. By the Artin–Hasse theorem, $[-1, a+bi\sqrt{d}]_P = 1$ and

$$[i,2m]_P = [i,m]_P = i^{(m^2-1)/4} = \begin{cases} 1 & \text{if } m \equiv \pm 1 \bmod 8, \\ -1 & \text{if } m \equiv \pm 3 \bmod 8. \end{cases}$$

Therefore, $\beta \in \Re_2F$ if and only if $m \equiv \pm 1 \bmod 8$. By Theorem 3.1, we get the assertion of Theorem 3.4.

By Theorem 3.4, we get the following result: if $F = \mathbb{Q}(\sqrt{d})$, $d = pq$, p, q prime, $p \equiv -q \equiv 3 \bmod 8$, then $(K_2O_F)_2 \cong \mathbb{Z}/(2)\oplus\mathbb{Z}/(8)$, which is proved in another way in [4]. On the other hand, we can generalize it.

THEOREM 3.5. *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ a squarefree integer, $d \equiv -1 \bmod 8$, and $2 \notin NF$. Suppose that $d = pqr$, where p, q, r are primes, i.e., $(p,q,r) \equiv (1,3,5)$ or $(7,5,5)$ or $(7,3,3) \bmod 8$.*

(1) *If* $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = 1$, *then* $(K_2O_F)_2 \cong \mathbb{Z}/(2^i) \oplus \mathbb{Z}/(2^j) \oplus \mathbb{Z}/(2)$, *where* $i \geq 3$, $j \geq 2$.

(2) *If* $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = -1$, *then* $(K_2O_F)_2 \cong \mathbb{Z}/(2^i) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$, *where* $i \geq 4$.

(3) *If* $\left(\frac{q}{p}\right) \neq \left(\frac{r}{p}\right)$, *then* $(K_2O_F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Proof. (1) If $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = 1$, $r_4(K_2O_F) = 2$ by the tables of [14]. We get the result by Theorem 3.1.

(2) If $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = -1$, then $r_4(K_2O_F) = 1$ by the tables of [14]. In fact, if $(p, q, r) \equiv (1, 3, 5)$ or $(7, 5, 5) \bmod 8$, then $(m, \varepsilon) = (p, 2)$ satisfies (2.6); if $(p, q, r) \equiv (7, 3, 3) \bmod 8$, then $(m, \varepsilon) = (p, 1)$ satisfies (2.6). By Theorem 3.4, we get $r_4(K_2O_F) = r_4(\Re_2 F) = 1$ and $o(\alpha_2) \geq 16$ in Theorem 3.1.

(3) If $\left(\frac{q}{p}\right) \neq \left(\frac{r}{p}\right)$, then $r_4(K_2O_F) = 1$ by the tables of [14]. There is (m, ε) with $m \equiv \pm 3 \bmod 8$ and $\varepsilon \in \{1, 2\}$ satisfying (2.6). By Theorem 3.4, we get $r_4(K_2O_F) = r_4(\Re_2 F) + 1 = 1$ and $o(\alpha_2) = 8$ in Theorem 3.1.

4. Imaginary quadratic fields. In this section, we consider imaginary quadratic fields $E = \mathbb{Q}(\sqrt{-d})$, $d > 2$ a squarefree integer. By [15], we have $[\Delta : E^*] = 4$, where $\Delta = \{z \in E^* \mid \{-1, z\} = 1\}$ is called the *Tate kernel*. Since $2 \in \Delta$, we have

$$\Delta = {E^*}^2 \cup 2{E^*}^2 \cup \delta {E^*}^2 \cup 2\delta {E^*}^2.$$

Below, we find such elements $\delta \in \Delta$ for some imaginary quadratic fields.

From [2], we know the following relation between K_2O_E and $\Re_2 E$ (the Hilbert kernel of E):

$$(K_2O_E/\Re_2 E)_2 \cong \begin{cases} 0 & \text{if } d \not\equiv \pm 1 \bmod 8, \\ \mathbb{Z}/(2) & \text{if } d \equiv -1 \bmod 8, \\ \mathbb{Z}/(2) & \text{if } d \equiv 1 \bmod 8. \end{cases}$$

If $d \equiv -1 \bmod 8$, then there is a prime divisor p of d with $p \equiv 3 \bmod 4$. Hence $\alpha = \{-1, p\} \in K_2O_E$, but $\alpha \notin \Re_2 E$, so $(K_2O_E)_2 \cong (\alpha) \times (\Re_2 E)_2$ by Lemma 3.1.

If $d \equiv 1 \bmod 8$, then $r_2(K_2O_E) = r_2(\Re_2 E)$ by [3], Theorem 4. Hence, by Lemma 3.1, $(K_2O_E)_2 \cong (\alpha) \times H$, where $\eta_P(\alpha) = -1$, $P \mid 2$, $o(\alpha) \geq 4$, and $H \subset (\Re_2 E)_2$. Therefore, $r_4(K_2O_E) = r_4(\Re_2 E) + 1$ if $o(\alpha) = 4$, and $r_4(K_2O_E) = r_4(\Re_2 E)$ if $o(\alpha) \geq 8$.

THEOREM 4.1. *Let* $E = \mathbb{Q}(\sqrt{-d})$, $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ *a squarefree integer*, $d \equiv 1 \bmod 8$, *and* $2 \notin NE$. *Then* $r_4(K_2O_E) = r_4(\Re_2 E) + 1$ *if and only if there is an odd positive divisor* $m \equiv \pm 3 \bmod 8$ *of* d *such that* $\varepsilon m \in NF$, $\varepsilon \in \{1, 2\}$.

Proof. By the preceding argument, Lemma 3.1, and (2.15), $r_4(K_2O_E) = r_4(\Re_2 E) + 1$ if and only if there is $\beta = \left\{-\frac{b\sqrt{-d}}{a}, \frac{\varepsilon m c^2}{a^2}\right\}\{-1, c\} \notin \Re_2 E$, where $m \mid d$ is positive and $(x, y, z) = (a, b, c)$ is a relatively prime solution of $\varepsilon m z^2 = x^2 - dy^2$, $\varepsilon \in \{1, 2\}$, in $\mathbb{N}$. By the process of proving Theorem 3.4, we know that $\beta \notin \Re_2 E$, i.e., $\eta_P(\beta) = -1,\ P \mid 2$, if and only if $m \equiv \pm 3 \bmod 8$.

By Theorem 4.1, we add some values to the tables in [13]:

Table 1

E	$p, q \bmod 8$	r_4	r_8	δ
$\mathbb{Q}(\sqrt{-d})$	$3, 3$	1	0	-1
	$5, 5$	1	0	-1

Table 2

E	$p, q, r \bmod 8$	The Legendre symbols	r_4	r_8	δ
$\mathbb{Q}(\sqrt{-pqr})$	7, 5, 3	$(\frac{p}{q}) = (\frac{p}{r})$	1	0	p
		otherwise	1	0	$-p$
	1, 5, 5	$(\frac{q}{p}) = (\frac{r}{p}) = 1$	2		
		$(\frac{q}{p}) = (\frac{r}{p}) = -1$	1	1	
		$(\frac{q}{p}) \neq (\frac{r}{p})$	1	0	-1
	1, 3, 3	$(\frac{q}{p}) = (\frac{r}{p}) = 1$	2		
		$(\frac{q}{p}) = (\frac{r}{p}) = -1$	1	1	
		$(\frac{q}{p}) \neq (\frac{r}{p})$	1	0	-1

Proof. 1. For Table 1, we need to consider the case $(p, q) \equiv (5, 5) \bmod 8$. If $\left(\frac{q}{p}\right) = 1$, then $p, pq \in NF$; if $\left(\frac{q}{p}\right) = -1$, then $2p, pq \in NF$. By the tables of [13] and Theorem 4.1, $r_4(K_2 O_E) = r_4(\Re_2 E) + 1 = 1$ and $\{-1, pq\} = 1$, i.e., $\{-1, -1\} = 1$.

2. For Table 2:

The case $(p, q, r) \equiv (7, 5, 3) \bmod 8$. By the tables of [13], $r_4(K_2 O_E) = 1$. Suppose $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = 1$ (similarly for $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1$). If $\left(\frac{r}{q}\right) = 1$, then $q, p \in NF$; if $\left(\frac{r}{q}\right) = -1$, then $2q, p \in NF$. Hence, by Theorem 4.1, $r_4(K_2 O_E) = r_4(\Re_2 E) + 1 = 1$ and $\{-1, p\} = 1$.

Suppose $\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right) = 1$ (similarly for $\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right) = -1$). If $\left(\frac{r}{q}\right) = 1$, then $q, qr \in NF$; if $\left(\frac{r}{q}\right) = -1$, then $2q, qr \in NF$. Hence, by Theorem 4.1, $r_4(K_2 O_E) = r_4(\Re_2 E) + 1 = 1$ and $\{-1, qr\} = 1$, i.e., $\{-1, -p\} = 1$.

The case $(p, q, r) \equiv (1, 5, 5) \bmod 8$. If $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = 1$, then $r_4(K_2 O_E) = 2$ by the tables of [13].

If $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = -1$ then $r_4(K_2 O_E) = 1$ by the tables of [13] and $2p, pqr \in NF$. Hence $r_4(K_2 O_E) = r_4(\Re_2 E) = 1$ and $r_8(K_2 O_E) = 1$ by Theorem 4.1.

Suppose $\left(\frac{q}{p}\right) = -\left(\frac{r}{p}\right) = 1$ (similarly for $\left(\frac{q}{p}\right) = -\left(\frac{r}{p}\right) = -1$). If $\left(\frac{r}{q}\right) = 1$, then $q, pqr \in NF$; if $\left(\frac{r}{q}\right) = 1$, then $2q, pqr \in NF$. Hence, by the tables of [13] and Theorem 4.1, $r_4(K_2O_E) = r_4(\Re_2 E) + 1 = 1$ and $\{-1, pqr\} = 1$, i.e., $\{-1, -1\} = 1$.

The case $(p, q, r) \equiv (1, 3, 3) \bmod 8$. If $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = 1$, then $r_4(K_2O_E) = 2$ by the tables of [13].

If $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = -1$, then $r_4(K_2O_E) = 1$ by the tables of [13] and $2p, 2pqr \in NF$. Hence, by Theorem 4.1, $r_4(K_2O_E) = r_4(\Re_2 E) = 1$ and $r_8(K_2O_E) = 1$.

Suppose $\left(\frac{q}{p}\right) = -\left(\frac{r}{p}\right) = 1$ (similarly for $\left(\frac{q}{p}\right) = -\left(\frac{r}{p}\right) = -1$). If $\left(\frac{q}{r}\right) = 1$, then $2q, 2pqr \in NF$; if $\left(\frac{q}{r}\right) = -1$, then $q, 2pqr \in NF$. Hence, by the tables of [13] and Theorem 4.1, $r_4(K_2O_E) = r_4(\Re_2 E) + 1 = 1$ and $\{-1, 2pqr\} = 1$, i.e., $\{-1, -1\} = 1$.

Acknowledgements. The author would like to thank Professors Feng Keqin and Qin Hourong for their helpful suggestions and many valuable conversations; he would also like to thank the referee for many corrections.

References

[1] B. Brauckmann, *The 2-Sylow-subgroup of the tame kernel of number fields*, Canad. J. Math. 43 (1991), 255–264.

[2] J. Browkin, *The functor K_2 of the ring of integers of a number fields*, in: Universal Algebra and Application, Banach Center Publ. 9, PWN, Warszawa, 1982, 187–195.

[3] J. Browkin and A. Schinzel, *On Sylow 2-subgroups of K_2O_F for quadratic fields F*, J. Reine Angew. Math. 331 (1982), 104–113.

[4] A. Candiotti and K. Kramer, *On the 2-Sylow subgroup of the Hilbert kernel of K_2 of number fields*, Acta Arith. 52 (1989), 49–65.

[5] P. E. Conner and J. Hurrelbrink, *The 4-rank of K_2O_F*, Canad. J. Math. 41 (1989), 932–960.

[6] —, —, *On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields*, Acta Arith. 73 (1995), 59–65.

[7] E. Hecke, *Lecture on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, 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] M. Kolster, *The structure of the 2-Sylow subgroup of $K_2(O)$, I*, Comment. Math. Helv. 61 (1986), 576–588.

[10] J. Milnor, *Introduction to Algebraic K-theory*, Ann. of Math. Stud. 72, Princeton Univ. Press, 1971.

[11] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

[12] H. Qin, *The 2-Sylow subgroups of K_2O_F for real quadratic fields F*, Science in China Ser. A 23 (12) (1993), 1254–1263 (in Chinese).

[13] —, *The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. 69 (1995), 153–169.

[14] H. Qin, *The 4-rank of K_2O_F for real quadratic fields F*, ibid. 72 (1995), 323–333.
[15] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. 36 (1976), 257–274.
[16] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.
[17] Q. Yue and K. Feng, *The 4-rank of the tame kernel versus the 4-rank of the narrow class group in quadratic number fields*, Acta Arith. 96 (2000), 155–166.

Institute of Mathematics
Fudan University
Shanghai 200433, P.R. China

Department of Mathematics
Xuzhou Normal University
Jiangsu 221009, P.R. China
E-mail: yue–qin@263.net

Received on 13.10.1998
and in revised form on 29.6.2000 (3481)