ACTA ARITHMETICA
LXIX.2 (1995)

The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields

by

HOURONG QIN (Nanjing)

To Professor Zhou Boxun (Cheo Peh-hsuin) on his 75th birthday

1. Introduction. Let F be a number field and O_F the ring of its integers. Many results are known about the group K_2O_F, the tame kernel of F. In particular, many authors have investigated the 2-Sylow subgroup of K_2O_F. As compared with real quadratic fields, the 2-Sylow subgroups of K_2O_F for imaginary quadratic fields F are more difficult to deal with. The objective of this paper is to prove a few theorems on the structure of the 2-Sylow subgroups of K_2O_F for imaginary quadratic fields F.

In our Ph.D. thesis (see [11]), we develop a method to determine the structure of the 2-Sylow subgroups of K_2O_F for real quadratic fields F. The present paper is motivated by some ideas in the above thesis.

2. Notations and preliminaries. Let F be a number field and O_F the ring of integers in F. Let Ω be the set of all places of F. For any finite place $\mathcal{P}$, denote by $v_\mathcal{P}(\ )$ the discrete valuation on F corresponding to $\mathcal{P}$. For any $\{x, y\} \in K_2F$, the tame symbol is defined by

$$\tau_\mathcal{P}\{x, y\} \equiv (-1)^{v_\mathcal{P}(x)v_\mathcal{P}(y)} x^{v_\mathcal{P}(y)} y^{-v_\mathcal{P}(x)} \pmod{\mathcal{P}}.$$

For any $\mathcal{P} \in \Omega$, the Hilbert symbol $\left(\frac{\cdot}{\mathcal{P}}\right)$ of order 2 on $F_\mathcal{P}$, the completion of F at $\mathcal{P}$, is defined as follows: Given non-zero elements $\alpha, \beta \in F_\mathcal{P}$, $\left(\frac{\alpha,\beta}{\mathcal{P}}\right) = 1$ if $\alpha\xi^2 + \beta\eta^2 = 1$ has a solution $\xi, \eta \in F_\mathcal{P}$, otherwise the symbol is defined to be -1. In particular, suppose $\mathcal{P}$ is a non-dyadic place in Ω. By a formula in Theorem 5.4 of [9],

if $\{x, y\} \in K_2F$ and $\tau_\mathcal{P}\{x, y\} = 1$ then

$$\left(\frac{x, y}{\mathcal{P}}\right) = 1. \tag{2.1}$$

And if $F=\mathbb{Q}$, the rational numbers field, and x, y are the units in $\mathbb{Q}_2$, then

$$\left(\frac{x,y}{2}\right)=(-1)^{((x-1)/2)\cdot((y-1)/2)} \tag{2.2}$$

(see Theorem 5.6 in [9]).

The following Product Formula for the Hilbert symbol is well known:

$$\prod_{\mathcal{P}\in\Omega}\left(\frac{\alpha,\beta}{\mathcal{P}}\right)=1. \tag{2.3}$$

For any odd prime p, let $\left(\frac{}{p}\right)$ denote the Legendre symbol. We have

LEMMA 2.1 (Legendre). *Suppose a,b,c are square free, $(a,b)=(b,c)=(c,a)=1$, and a,b,c do not have the same sign. Then the Diophantine equation*

$$ax^2+by^2+cz^2=0$$

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

Proof. See Theorem 4.1 and its Corollary 2 in [3].

In this paper, we use $(K_2O_F)_2$ to denote the 2-Sylow subgroup of K_2O_F.

Let F be an imaginary quadratic field. By [13], we have $[\Delta : F^{\cdot 2}]=4$, where $\Delta=\{z\in F^{\cdot}\mid\{-1,\,z\}=1\}$. In Section 5, we will determine Δ for some imaginary quadratic fields.

3. General results

LEMMA 3.1. *Let $F=\mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer). For any $\alpha=x+y\sqrt{-d}\in F^{\cdot}$, put $S=\{\mathcal{P}_1,\dots,\mathcal{P}_n\}=\{\mathcal{P}\mid\tau_{\mathcal{P}}\{-1,\alpha\}=-1\}$. Without loss of generality, we can assume that $p_i=\mathcal{P}_i\cap\mathbb{Z}$ is not inert for $1\le i\le n$. Then $x^2+dy^2=\varepsilon p_1\dots p_nz^2$, where $\varepsilon\in\{1,2\}$ and $z\in\mathbb{Q}$. Conversely, suppose that $p_1,\dots,p_n$ are distinct primes in $\mathbb{Z}$ and $\mathcal{P}_1,\dots,\mathcal{P}_n$ are prime ideals of O_F such that $\mathcal{P}_i\cap\mathbb{Z}=p_i$ for $1\le i\le n$. If there is an $\varepsilon\in\{1,2\}$ such that the equation $x^2+dy^2=\varepsilon p_1\dots p_nz^2$ is solvable in $\mathbb{Q}$ (equivalently in $\mathbb{Z}$), then there is an $\alpha\in F^{\cdot}$ such that $S=\{\mathcal{P}\,|\,\tau_{\mathcal{P}}\{-1,\alpha\}=-1\}=\{\mathcal{P}_1,\dots,\mathcal{P}_n\}$.*

Proof. Suppose $\alpha=x+y\sqrt{-d}\in F^{\cdot}$ and $S=\{\mathcal{P}_1,\dots,\mathcal{P}_n\}=\{\mathcal{P}\,|\,\tau_{\mathcal{P}}\{-1,\alpha\}=-1\}$. Then $(x+y\sqrt{-d})=\mathfrak{q}^{\sigma}\mathcal{P}_1\dots\mathcal{P}_n\mathfrak{a}^2$, where $\mathfrak{q}\,|\,2$ and $\sigma=0$ or 1 and $\mathfrak{a}$ is a fractional ideal of O_F in F. Hence, $x^2+dy^2=\varepsilon p_1\dots p_nz^2$.

Conversely, if $x^2+dy^2=\varepsilon p_1\dots p_nz^2$ has a solution $x,y,z\in\mathbb{Z}$, then for any $1\le i\le n$, either $x+y\sqrt{-d}\in\mathcal{P}_i$ or $x-y\sqrt{-d}\in\mathcal{P}_i$. So suitably choosing $\delta\in\mathbb{Q}$, we can assume that $(\delta(x+y\sqrt{-d}))=\mathfrak{q}^e\mathcal{P}_1\dots\mathcal{P}_n\mathfrak{a}^2$, where $\mathfrak{q}\,|\,2$, $e=0$

or 1 and $\mathfrak{a}$ is a fractional ideal of O_F in F. Then taking $\alpha = \delta(x + y\sqrt{-d})$ yields the result.

THEOREM 3.2. *Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer), and $m \mid d$, a positive integer. If any prime factor of m satisfies $p_i \equiv 1 \pmod 4$, for $1 \le i \le n$, then there is an $\alpha \in K_2O_F$ with $\alpha^2 = \{-1, m\}$ if and only if there is an $\varepsilon \in \{1, 2\}$ such that the Diophantine equation $\varepsilon m Z^2 = X^2 + dY^2$ is solvable in $\mathbb{Z}$.*

P r o o f. From the assumption, we have $m = x^2 + y^2$, where $x, y \in \mathbb{Z}$. Let

$$\alpha' = \left\{\frac{x}{y}, \frac{x^2+y^2}{y^2}\right\} = \left\{\frac{x}{y}, \frac{m}{y^2}\right\}.$$

Then $\alpha'^2 = \{-1, m\}$. It is easy to check that $\{\mathcal{P} \mid \tau_{\mathcal{P}}\alpha' = -1\} = \{\mathcal{P}_1, \dots \dots, \mathcal{P}_n\}$, where $\mathcal{P}_i \cap \mathbb{Z} = p_i$ $(1 \le i \le n)$. Therefore, the result follows from Lemma 3.1.

LEMMA 3.3. *Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer). ŁThen $m = x^2 + y^2$ for $x, y \in F$, where m is an integer satisfying: $m \mid d$ if $d \not\equiv -1 \pmod 8$ or $m \mid d$ together with $m \not\equiv 3 \pmod 4$ if $d \equiv -1 \pmod 8$.*

P r o o f. Let Ω denote the set of all places of F. In view of the Hasse–Minkowski Theorem (see [10]), it is enough to prove that $\left(\frac{-1,m}{\mathcal{P}}\right) = 1$ for any $\mathcal{P} \in \Omega$.

Clearly, if $\mathcal{P}$ is the unique Archimedean place in Ω, then $\left(\frac{-1,m}{\mathcal{P}}\right) = 1$.

In the non-dyadic cases, $\left(\frac{-1,m}{\mathcal{P}}\right) = 1$ follows from (2.1).

If $d \not\equiv -1 \pmod 8$, then there is a unique dyadic place $\mathcal{P}$ in Ω. Then the Product Formula yields $\left(\frac{-1,m}{\mathcal{P}}\right) = 1$.

Now suppose $d \equiv -1 \pmod 8$. Here $m \not\equiv 3 \pmod 4$. Let $\mathcal{P}_1, \mathcal{P}_2$ denote the two dyadic places in Ω. Then $F_{\mathcal{P}_1} \cong F_{\mathcal{P}_2} \cong \mathbb{Q}_2$. Hence, by (2.2), we have $\left(\frac{-1,m}{\mathcal{P}_i}\right) = 1$ for $i = 1, 2$. This completes the proof.

R e m a r k. By a theorem due to Bass and Tate (see [8]), a necessary and sufficient condition for $\{-1, m\} = \alpha^2$ with $\alpha \in K_2F$ is that $m = x^2 + y^2$ for $x, y \in F$. On the other hand, if $d \equiv -1 \pmod 8$, $m \mid d$ and $m \equiv 3 \pmod 4$, then by (2.2), $\left(\frac{-1,m}{\mathcal{P}_i}\right) = -1$, where $i = 1, 2$, and $\mathcal{P}_1, \mathcal{P}_2$ are the two dyadic places of F. So $\{-1, m\} \ne \alpha^2$ for any $\alpha \in K_2F$.

Now, let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. Suppose $m = -1$ or $m = \delta q_1 \dots q_r$, where $\delta = 1$ or -1 for $1 \le i \le r$, $q_i \equiv 3 \pmod 4$ is a prime, and suppose $m = X^2 + Y^2$ for $X, Y \in F$. Write

$$X = \frac{x + y\sqrt{-d}}{z}, \quad Y = \frac{x' + y'\sqrt{-d}}{z}, \quad \text{where } x, y, x', y', z \in \mathbb{Z}.$$

Clearly $m = X^2 + Y^2$ implies that $xy = -x'y'$ and

$$mz^2 = x^2 - dy^2 + x'^2 - dy'^2. \tag{3.1}$$

Without loss of generality, we can assume that $(x, y, x', y') = 1$ below.

LEMMA 3.4. *Notations being as above, suppose $k \geq 0$ is an integer and p is a prime with $p^{2k+1} \parallel (x^2 + x'^2)$. Then there is a prime ideal $\mathcal{P}$ of F such that $v_{\mathcal{P}}(x+y\sqrt{-d}) > 0, v_{\mathcal{P}}(x'+y'\sqrt{-d}) > 0$. Conversely, if $v_{\mathcal{P}}(x+y\sqrt{-d}) > 0$ and $v_{\mathcal{P}}(x' + y'\sqrt{-d}) > 0$, then $v_{\mathcal{P}}(x^2 + x'^2) > 0$.*

P r o o f. It follows from (3.1) that $mx^2z^2 = (x^2 + x'^2)(x^2 - dy'^2)$. Then $p^{2k+1} \parallel (x^2 + x'^2)$ implies $p \,|\, (x^2 - dy'^2)$ (note that $p \equiv 1 \pmod 4$). But $(x + y\sqrt{-d})(x - y\sqrt{-d}) = x^2 + dy^2 \equiv -x'^2 + dy^2 \equiv 0 \pmod{\mathcal{P}}$. So we may assume that $v_{\mathcal{P}}(x + y\sqrt{-d}) > 0$. Similarly, $v_{\mathcal{P}}(x' + y'\sqrt{-d}) > 0$.

Conversely, suppose $v_{\mathcal{P}}(x + y\sqrt{-d}) > 0$ and $v_{\mathcal{P}}(x' + y'\sqrt{-d}) > 0$. Let $p = \mathcal{P} \cap \mathbb{Z}$. Then $p \,|\, (x^2 + dy^2)$, $p \,|\, (x'^2 + dy'^2)$. If $p \,|\, x$, then $p \,|\, x'$ or $p \,|\, y'$ since $xy = -x'y'$. But $p \,|\, y'$ also implies $p \,|\, x'$. Hence $p \,|\, (x^2 + x'^2)$. Now we assume that $p \nmid x$ and $p \nmid x'$. It is easy to verify that

$$x' + y'\sqrt{-d} = \frac{x'}{x}\left(\frac{x + x'^2}{x'^2} \cdot x - (x + y\sqrt{-d})\right). \tag{3.2}$$

So, $v_{\mathcal{P}}(x^2 + x'^2) > 0$.

LEMMA 3.5. *With notations being as above, suppose $\mathcal{P}$ is a non-dyadic prime ideal of $O_F, \mathcal{P} \cap \mathbb{Z} = p$ and $p \nmid m$. If $v_{\mathcal{P}}(x^2 + x'^2) > 0$ and $v_{\mathcal{P}}(x + y\sqrt{-d}) > 0$, then $v_p(x^2 + x'^2) \equiv v_{\mathcal{P}}(x + y\sqrt{-d}) \pmod 2$.*

P r o o f. First suppose that $v_{\mathcal{P}}(x) = 0$. Then p is unramified in O_F, hence $v_p(x^2 + x'^2) = v_{\mathcal{P}}(x^2 + x'^2)$ and $v_{\mathcal{P}}(x + y\sqrt{-d}) = v_{\mathcal{P}}(x^2 + dy^2)$. It can be deduced from the identity

$$m = \left(\frac{x + y\sqrt{-d}}{z}\right)^2 + \left(\frac{x' + y'\sqrt{-d}}{z}\right)^2$$

that $v_{\mathcal{P}}(x + y\sqrt{-d}) = v_{\mathcal{P}}(x' + y'\sqrt{-d})$. If $v_{\mathcal{P}}(x + y\sqrt{-d}) \neq v_{\mathcal{P}}(x^2 + x'^2)$, then (3.2) yields $v_{\mathcal{P}}(x^2 + x'^2) > v_{\mathcal{P}}(x + y\sqrt{-d}) = v_{\mathcal{P}}(x^2 + dy^2)$. Hence,

$$v_{\mathcal{P}}(x^2 + dy^2) = v_{\mathcal{P}}(x^2 + dy^2 - (x^2 + x'^2)) = v_{\mathcal{P}}(-x'^2 + dy^2).$$

Now, $v_{\mathcal{P}}(x^2+x'^2) \equiv v_{\mathcal{P}}(x^2+x'^2) \pmod 2$ is a consequence of the observation that

$$(x'^2 - dy^2)\left(\frac{x^2 + x'^2}{x'^2}\right) = mz^2. \tag{3.3}$$

Then suppose that $v_{\mathcal{P}}(x) > 0$. In this case, the only possibility is that $p \,|\, d$, $p \nmid y$ and $p \nmid y'$. Then

$$(x^2 - dy'^2)\left(\frac{x^2 + x'^2}{x^2}\right) = mz^2$$

implies

$$v_{\mathcal{P}}(x + y\sqrt{-d}) \equiv v_{\mathcal{P}}(x^2 + x'^2) \equiv 1 \pmod 2.$$

THEOREM 3.6. *Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer), and let m be an integer with $m \mid d$ if $d \not\equiv -1 \pmod 8$, and with $m \mid d$ and $m \not\equiv 3 \pmod 4$ if $d \equiv -1 \pmod 8$. Moreover, if $m \neq -1$, then for any prime factor of m, $p \equiv 3 \pmod 4$. Then there is an $\alpha \in K_2O_F$ with $\alpha^2 = \{-1, m\}$ if and only if there is an $\varepsilon \in \{1, 2\}$ such that*

$$\left(\frac{d/m}{p}\right) = \left(\frac{-\varepsilon}{p}\right) \quad \text{for any prime } p \mid m;$$

$$\left(\frac{m}{p}\right) = \left(\frac{\varepsilon}{p}\right) \quad \text{for any prime } p \mid d,\ p \nmid m.$$

P r o o f. We know that there are $x, y, x', y', z \in \mathbb{Z}$ with $(x, y, x', y') = 1$ such that $mz^2 = (x + y\sqrt{-d})^2 + (x' + y'\sqrt{-d})^2$. Write

$$\beta = \left\{ \frac{x' + y'\sqrt{-d}}{x + y\sqrt{-d}}, \frac{mz^2}{(x + y\sqrt{-d})^2} \right\}.$$

Then $\beta^2 = \{-1, m\}$ and it is not hard to check that

$$\tau_{\mathcal{P}}\beta = \begin{cases} (-1)^{v_{\mathcal{P}}(z) - v_{\mathcal{P}}(x+y\sqrt{-d})} \\ \quad \text{if } \mathcal{P} \cap \mathbb{Z} = p \nmid m \text{ and } v_{\mathcal{P}}(x + y\sqrt{-d}) = v_{\mathcal{P}}(x' + y'\sqrt{-d}), \\ 1 \quad \text{otherwise.} \end{cases}$$

In view of Lemma 3.5 and replacing β by $\beta\{-1, \delta\}$ for a suitable $\delta \in \mathbb{Z}$ if necessary allows us to assume that $\tau_{\mathcal{P}}\beta = -1$ if and only if $p^{2k+1} \parallel (x^2 + x'^2)$, where $p = \mathcal{P} \cap \mathbb{Z}$ and k is a non-negative integer. Hence, by Lemma 3.1 we conclude that there is a $\beta \in K_2O_F$ with $\beta^2 = \{-1, m\}$ if and only if there is an $\varepsilon \in \{1, 2\}$ such that the Diophantine equation

$$\varepsilon(x^2 + x'^2)Z^2 = X^2 + dY^2 \tag{3.4}$$

is solvable in $\mathbb{Z}$.

Obviously, we can assume that $x^2 + x'^2$ is square-free.

Let us assume that c is the greatest common divisor of $\varepsilon(x^2 + x'^2)$ and d. Then (3.4) can be written as

$$\frac{\varepsilon(x^2 + x'^2)}{c} Z^2 = cX^2 + \frac{d}{c} Y^2.$$

By Lemma 2.1, it is solvable in $\mathbb{Z}$ if and only if

$$\left(\frac{c}{p}\right) = \left(\frac{-d/c}{p}\right) \quad \text{for any prime } p \,\Big|\, \frac{x^2 + x'^2}{c}, \tag{3.5}$$

$$\left(\frac{\varepsilon(x^2 + x'^2)}{p}\right) = \left(\frac{d/c}{p}\right) \quad \text{for any prime } p \mid c, \tag{3.6}$$

and

$$\left(\frac{c}{p}\right) = \left(\frac{\varepsilon(x^2+x'^2)/c}{p}\right) \quad \text{for any prime } p \,\Big|\, \frac{d}{c}. \tag{3.7}$$

Note that the identity (3.3) can be written as

$$mc\overline{x}^2 - \frac{d}{mc}\overline{y}^2 = \frac{x^2+x'^2}{c}\overline{z}^2, \tag{3.8}$$

so that

$$\left(\frac{mc}{p}\right) = \left(\frac{d/mc}{p}\right) \quad \text{for any prime } p \,\Big|\, \frac{x^2+x'^2}{c}.$$

This is equivalent to (3.5), because $p \,|\, \frac{x^2+x'^2}{c}$ implies that $p \equiv 1 \pmod 4$. In other words, (3.5) is trivial. If $p \,|\, c$, then

$$\left(\frac{-d/mc}{p}\right) = \left(\frac{(x^2+x'^2)/c}{p}\right).$$

So (3.6) is equivalent to

$$\left(\frac{-d/mc}{p}\right) = \left(\frac{\varepsilon d/c}{p}\right), \quad \text{i.e.,} \quad \left(\frac{m}{p}\right) = \left(\frac{\varepsilon}{p}\right).$$

So does the case $p \,|\, d$, $p \nmid c$ and $p \nmid m$. If $p \,|\, m$, then

$$\left(\frac{-d/mc}{p}\right) = \left(\frac{(x^2+x'^2)/c}{p}\right).$$

In this case, (3.7) is equivalent to

$$\left(\frac{-d/mc}{p}\right) = \left(\frac{\varepsilon c}{p}\right), \quad \text{i.e.,} \quad \left(\frac{d/m}{p}\right) = \left(\frac{-\varepsilon}{p}\right).$$

This concludes the proof.

Corollary 3.7. *Let the assumptions and the notations be as in Theorem* 3.6, *and assume that* n *is a positive integer satisfying* $n \,|\, d$ *and for any prime factor of* n, $p \equiv 1 \pmod 4$. *Then there is a* $\beta \in K_2O_F$ *such that* $\beta^2 = \{-1, mn\}$ *if and only if*

(i) *for any prime* $p \,|\, mn$, $\left(\frac{d/mn}{p}\right) = \left(\frac{-\varepsilon}{p}\right)$,
(ii) *for any prime* $p \,|\, d$, $p \nmid mn$, $\left(\frac{mn}{p}\right) = \left(\frac{\varepsilon}{p}\right)$, *where* $\varepsilon = 1$ *or* 2.

Proof. Consider $\varepsilon(x^2+x'^2)nZ^2 = X^2 + dY^2$ in place of (3.4).

Corollary 3.8. *Let* $F = \mathbb{Q}(\sqrt{-d})$ *be an imaginary quadratic field. Then* $\{-1,-1\} = \alpha^2$ *with* $\alpha \in K_2O_F$ *if either* $d = 1$ *or* $d = 2$ *or for any odd prime* $p \,|\, d$, $p \equiv 1 \pmod 4$ *or for any odd prime* $p \,|\, d$, $p \equiv 1$ *or* $3 \pmod 8$.

Otherwise, $\{-1,-1\} \neq \alpha^2$ *for any* $\alpha \in K_2O_F$, *in particular,* $\{-1,-1\} \neq 1$.

Lemma 3.9. *Let* $m \equiv 3 \pmod 4$ *and* $d \equiv -1 \pmod 8$. *Then for* $\varepsilon = 1$ *or* 2, *the Diophantine equation* $\varepsilon m Z^2 = X^2 - dY^2$ *has no solutions in* $\mathbb{Z}$.

P r o o f. Consider the congruence

$$\varepsilon m Z^2 \equiv X^2 - dY^2 \pmod 8, \quad \text{i.e.,} \quad \varepsilon m Z^2 \equiv X^2 + Y^2 \pmod 8.$$

Note that for any $a \in \mathbb{Z}$, $a^2 \equiv 0$ or 4 or $1 \pmod 8$. Then the result follows.

As a consequence of Lemma 2.1, Corollary 3.7 and Lemma 3.9, we have:

THEOREM 3.10. *Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer), and $m \mid d$ an integer. Then there is an $\alpha \in K_2O_F$ with $\alpha^2 = \{-1, m\}$ if and only if there is an $\varepsilon \in \{1, 2\}$ such that the Diophantine equation $\varepsilon m Z^2 = X^2 - dY^2$ is solvable in $\mathbb{Z}$.*

Next, we consider the case when $2 \in NF$. Just as before, we always discuss imaginary quadratic fields.

Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer). Then $2 \in NF$ if and only if $-d = u^2 - 2w^2$ with $u, w \in \mathbb{Z}$ (see [2]). When d is not a prime, the symbol $\left(\frac{}{d}\right)$ denotes the Jacobi symbol. Note that $\left(\frac{u+w}{d}\right) = \left(\frac{u-w}{d}\right)$. For simplicity of notation, denote by ψ the Jacobi symbol $\left(\frac{u+w}{d}\right)$.

LEMMA 3.11. *Let d be a positive square-free integer with $-d = u^2 - 2w^2$, where $u, w \in \mathbb{Z}$. Then there is a prime $p \equiv 1 \pmod 4$ with $p \nmid d$, $p \nmid (u + w)$ and $p \nmid uw$ such that the Diophantine equation*

$$X^2 - dY^2 = (u + w)pZ^2 \tag{3.9}$$

is solvable in $\mathbb{Z}$ if $d \not\equiv -1 \pmod 8$, and

$$X^2 - dY^2 = \psi(u + w)pZ^2 \tag{3.10}$$

is solvable in $\mathbb{Z}$ if $d \equiv -1 \pmod 8$.

P r o o f. Clearly, $\left(\frac{d}{u+w}\right) = 1$. Hence, if $-d \equiv 7 \pmod 8$, then by the properties of the Jacobi symbol (see [6]), we have $\left(\frac{u+w}{d}\right) = 1$. For any prime $l \mid d$, we choose a prime $p \equiv 1 \pmod 4$ with $p \nmid (u + w)$ and $p \nmid uw$ such that $\left(\frac{p}{l}\right) = \left(\frac{u+w}{l}\right)$.

Put $d = 2d'$ if $2 \mid d$. For any prime $l \mid d'$, we choose a prime p with $p \nmid (u + w)$, $p \nmid uw$ such that $\left(\frac{p}{l}\right) = \left(\frac{u+w}{l}\right)$ and $p \equiv 1 \pmod 8$ if $\left(\frac{d'}{p}\right) = 1$ or $p \equiv 5 \pmod 8$ if $\left(\frac{d'}{p}\right) = -1$. In both cases, $\left(\frac{d}{p}\right) = 1$.

If $d \equiv -1 \pmod 8$, we choose a prime $p \equiv 1 \pmod 4$ such that $p \nmid (u + w)$, $p \nmid uw$ and for any prime $l \mid d$, $\left(\frac{p}{l}\right) = \left(\frac{\psi(u+w)}{l}\right)$. We also have $\left(\frac{d}{p}\right) = 1$.

Then by Lemma 2.1, the result follows.

R e m a r k. In the proof of the above theorem, we used the remarkable fact that any arithmetic progression contains infinitely many primes.

By choice of X, Y, Z, a solution of equation (3.9) or (3.10), we can find $g, h \in \mathbb{Z}$ such that $h = Y, (u + w)g + wh = X$ and $(g, h) = 1$. Put

$$\alpha = g^2 + h^2, \quad \theta = (g^2 - h^2 + 2gh)w. \tag{3.11}$$

Clearly, if $d \equiv -1 \pmod 8$ and $\left(\frac{u+w}{d}\right) = -1$, then $\left(\frac{-(u+w)}{d}\right) = 1$. Without loss of generality, we can assume that $\psi = 1$. Then

$$(\alpha u+\theta)(u+w) = ((u+w)g+wh)^2+(u^2-2w^2)h^2 = X^2-dY^2 = (u+w)pZ^2,$$

hence,

$$\alpha u + \theta = pZ^2. \tag{3.12}$$

Therefore,

$$2\left(u + \frac{\theta}{\alpha}\right) = \frac{2\alpha(\alpha u + \theta)}{\alpha^2} = \xi^2 + \eta^2, \tag{3.13}$$

where $\xi, \eta \in \mathbb{Q}$ with $\alpha\xi$, $\alpha\eta \in \mathbb{Z}$. It follows from $p \nmid uw$ and $(g, h) = 1$ that $(p, \alpha) = (p, \theta) = 1$. Moreover, we can assume that $(\alpha\xi, p) = (\alpha\eta, p) = 1$.

Let

$$x = \alpha\xi pZ^2 + \alpha\eta\lambda, \quad y = \alpha^2\xi, \tag{3.14}$$

$$a = \alpha\eta pZ^2 - \alpha\xi\lambda, \quad b = \alpha^2\eta, \tag{3.15}$$

where $\lambda = (g^2 - h^2 - 2gh)w$. Note that $\lambda^2 + \theta^2 = 2\alpha^2w^2$. Then

$$(x + y\sqrt{-d})^2 + (a + b\sqrt{-d})^2 = (u + \sqrt{-d})(2p\alpha Z^2)^2. \tag{3.16}$$

On the other hand, $\alpha^2(\xi^2 + \eta^2) \equiv 0 \pmod{pZ^2}$, hence,

$$\begin{aligned} x^2 + dy^2 &\equiv (\alpha\eta\lambda)^2 + d\alpha^4\eta^2 = (\alpha\eta\lambda)^2 + (u^2 - 2w^2)\alpha^4\eta^2 \\ &= (\alpha\eta)^2(\lambda^2 + \alpha^2u^2 - 2\alpha^2w^2) = (\alpha\eta)^2(-\theta^2 + \alpha^2u^2) \\ &\equiv 0 \pmod{pZ^2} \end{aligned}$$

and

$$x^2 + dy^2 \equiv (\alpha\xi pZ^2)^2 - u^2(\alpha^2\xi)^2 = \alpha^2\xi^2((pZ^2)^2 - \alpha^2u^2) \equiv 0 \pmod w.$$

Similarly,

$$a^2 + db^2 \equiv 0 \pmod{pZ^2} \quad \text{and} \quad a^2 + db^2 \equiv 0 \pmod w.$$

Lemma 3.12. *With the notations as above, set* $E = x + y\sqrt{-d}$, $F = a + b\sqrt{-d}$ *and*

$$\beta = \left\{\frac{E}{F}, \frac{E^2 + F^2}{F^2}\right\}.$$

Then $\beta^2 = \{-1, u + \sqrt{-d}\} \in K_2O_F$ *and there is a* $\beta' \in K_2O_F$ *with* $\beta'^2 = \{-1, u + \sqrt{-d}\}$ *if and only if the Diophantine equation*

$$(u + w)N^2 = S^2 - dT^2 \tag{3.17}$$

is solvable in $\mathbb{Z}$.

Proof. We only need to consider non-dyadic places of F. It is easy to see that for any place $\mathcal{P}$, if $v_\mathcal{P}(E) \neq v_\mathcal{P}(F)$, then $\tau_\mathcal{P}\beta = 1$ and if $v_\mathcal{P}(E) = v_\mathcal{P}(F)$,

then

$$\tau_{\mathcal{P}}\beta = (-1)^{v_{\mathcal{P}}(\alpha Z^2 pw/F)}. \tag{3.18}$$

Obviously, if $v_{\mathcal{P}}(E) = v_{\mathcal{P}}(F)$, then $\mathcal{P} \cap \mathbb{Z} = p' \,|\, dZ^2pw$. We deduce from $\alpha \,|\, y$, $\alpha \,|\, b$ and $(p, \alpha) = 1$ that for any place $\mathcal{P}$, if $\mathcal{P} \cap \mathbb{Z} = p' \,|\, \alpha$, then $\tau_{\mathcal{P}}\beta = \tau_{\bar{\mathcal{P}}}\beta$, where $\overline{\mathcal{P}} \neq \mathcal{P}$ is the conjugation of $\mathcal{P}$. Thus, multiplying β by $\{-1, c\}$ for a suitable $c \in \mathbb{Z}$ if necessary allows us to assume that $\tau_{\mathcal{P}}\beta = 1$ for any $\mathcal{P} \cap \mathbb{Z} = p' \,|\, \alpha$. On the other hand, if $\mathcal{P} \cap \mathbb{Z} = p' \,|\, w$, $v_{\mathcal{P}}(E) = v_{\mathcal{P}}(F)$, then $v_{\mathcal{P}}(F) = v_{\mathcal{P}}(w)$, since $x^2 + dy^2 \equiv a^2 + db^2 \equiv 0 \pmod{w}$. Hence $\tau_{\mathcal{P}}\beta = 1$ for any $\mathcal{P} \cap \mathbb{Z} = p' \,|\, w$. Finally, since $\left(\frac{d}{p}\right) = 1$, $p = \mathcal{P}\overline{\mathcal{P}}$. It follows from $x^2 + dy^2 \equiv a^2 + db^2 \equiv 0 \pmod{pZ^2}$, $(p, \alpha) = 1$ and (3.16) that if $v_{\mathcal{P}}(E) + v_{\mathcal{P}}(F) \neq 0$ then either $v_{\mathcal{P}}(E)$ or $v_{\mathcal{P}}(F) \equiv 1 \pmod 2$. Hence, $\tau_{\mathcal{P}}\beta = 1$ and $\tau_{\bar{\mathcal{P}}}\beta = -1$. If $v_{\mathcal{P}}(E) = v_{\mathcal{P}}(F) = 0$, then $\tau_{\mathcal{P}}\beta = -1$ and $\tau_{\bar{\mathcal{P}}}\beta = 1$. By Lemma 3.1, we see that there is a $\beta' \in K_2O_F$ with $\beta'^2 = \{-1, u + \sqrt{-d}\}$ if and only if the Diophantine equation

$$\varepsilon p N^2 = S^2 + dT^2 \tag{3.19}$$

is solvable in $\mathbb{Z}$ for $\varepsilon = 1$ or 2. This is equivalent to saying that the Diophantine equation (3.17) is solvable in $\mathbb{Z}$. This proves our theorem.

The following theorem is a consequence of the above lemma and Theorem 3.6.

THEOREM 3.13. *Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer) with $-d = u^2 - 2w^2$ for $u, w \in \mathbb{Z}$, and let $m \,|\, d$. Then there is a $\beta \in K_2O_F$ with $\beta^2 = \{-1, m(u + \sqrt{-d})\}$ if and only if the Diophantine equation*

$$m(u + w)N^2 = S^2 - dT^2 \tag{3.20}$$

is solvable in $\mathbb{Z}$.

Proof. First, we observe that if $d \equiv -1 \pmod 8$ and $\left(\frac{u+w}{d}\right) = -1$ together with $m \equiv 1 \pmod 4$, then (3.20) has no solutions in $\mathbb{Z}$. In fact, consider $m(u + w)N^2 = S^2 - dT^2 \pmod 4$, i.e., $3N^2 = S^2 + T^2 \pmod 4$; then the result follows.

Next, if $d \equiv -1 \pmod 8$ and $\left(\frac{u+w}{d}\right) = -1$ together with $m \equiv 1 \pmod 4$, then there is no $\beta \in K_2F$ with $\beta^2 = \{-1, m(u + \sqrt{-d})\}$.

Then, by Lemma 3.12 and Theorem 3.6, the assertion follows.

4. 4-rank K_2O_F. For any number fields F a 4-rank K_2O_F formula is proved in [7] (compare also [5]). For quadratic field, we refer to [1], [11]. Here, we apply Theorems 3.10 and 3.13 to determine the 4-rank K_2O_F for any imaginary quadratic field F. Let $F = \mathbb{Q}(\sqrt{-d})$ (d a positive square-free integer). Put $d' = \frac{1}{2}d$ or d according as $2 \,|\, d$ or not. Write $K = \{m \mid m \,|\, d, m \neq 1, -d', 2\nmid m\}$ and $V = \{(u + \sqrt{-d})m \mid -d = u^2 - 2w^2$ with $u, w \in \mathbb{Z}$,

$w > 0$, $m \in K \cup \{1, -d'\}\}$ and put

$$\overline{K} = \{k \in K \mid \varepsilon k Z^2 = X^2 - dY^2 \text{ is solvable in } \mathbb{Z} \text{ for } \varepsilon = 1 \text{ or } 2\},$$
$$\overline{V}_0 = \{m(u+\sqrt{-d}) \mid m(u+\sqrt{-d}) \in V, \; m(u+w)Z^2 = X^2 - dY^2 \text{ is solvable in } \mathbb{Z}\},$$
$$\overline{V} = \{m(u+w) \mid m(u+\sqrt{-d}) \in \overline{V}_0\}.$$

THEOREM 4.1. *With the above notations, let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. Then $r_4 = 4 - \operatorname{rank} K_2O_F = \log_2 \frac{r+2}{4}$, where $r = \#(\overline{K} \cup \overline{V})$.*

Proof. For any positive integer n, let ${}_n(K_2O_F)$ denote the subgroup generated by all elements of order n. By [2], ${}_2(K_2O_F)$ can be generated by the following elements:

$\{-1, k\}$ $(k \in K)$,

$\{-1,\ m(u+\sqrt{-d})\}$ $(m(u+\sqrt{-d}) \in V$ if $-d = u^2 - 2w^2$ with $u, w \in \mathbb{Z})$.

Since $[\Delta : F^{\cdot 2}] = 4$, there are the only two elements $\delta, -d'/\delta \in \overline{K}$ or $\delta, (-d'/\delta)(u+\sqrt{-d})^2 \in \overline{V}_0$ satisfying $\delta, -d/\delta \in \Delta$. Suppose that $a_1, \ldots, a_{r_4}$ generate ${}_4(K_2O_F)$. Then $a_i^2 = \{-1, b_i\} \in {}_2(K_2O_F)$ $(1 \le i \le r_4)$. Set $b_0 = \delta$. Then by Theorems 3.10 and 3.13,

$$\#\{b_{i_1} \ldots b_{i_k}, -d/b_{i_1} \ldots b_{i_k} \mid i_1, \ldots, i_k \in \{0, 1, \ldots, r_4\}\} = \#(\overline{K} \cup \overline{V}_0) = \#(\overline{K} \cup \overline{V}).$$

It is easy to verify that $r = \#(\overline{K} \cup \overline{V}) = 2^{r_4+2} - 2$. So $r_4 = \log_2 \frac{r+2}{4}$ as desired.

COROLLARY 4.2. *$r_4 = 0$ if and only if $r = \#(\overline{K} \cup \overline{V}) = 2$.*

COROLLARY 4.3. *$r_4 = r_2$ if and only if $K = \overline{K}$ and $\#V = \#\overline{V}$.*

5. The structure of $(K_2O_F)_2$. In this section, we apply Theorems 3.10, 3.13 and 4.1 to determine the structure of $(K_2O_F)_2$ for imaginary quadratic fields F.

THEOREM 5.1. *Let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with d either pq or $2pq$ or pqr or $2pqr$, where p, q, r are distinct odd primes. If $2 \in NF$, put $v = u + w$, where $u, w \in \mathbb{Z}$ are such that $-d = u^2 - 2w^2$. Let δ be an element such that $\Delta = F^{\cdot 2} \cup 2F^{\cdot 2} \cup \delta F^{\cdot 2} \cup 2\delta F^{\cdot 2}$. Then we have the tables given below.*

If F is a field as in Table III, *then $r_2 = 2$, $r_4 = 0$, otherwise* (*except for the case $d = 2pqr$ with $p, q, r \equiv 7, 5, 3 \pmod 8$*) *$r_2 = 2$, $r_4 = 1$.*

Notes. 1. Only when $2 \mid d$ and $d/2 \equiv 1 \pmod 8$, the alternative $(*)$ can occur in Table II.

Table I

F	$p, q \pmod 8$	r_2	r_4	δ
$\mathbb{Q}(\sqrt{-pq})$	$5, 7$	1	0	$\left(\frac{q}{p}\right)p$
$\mathbb{Q}(\sqrt{-2pq})$	$3, 7$	1	0	$\left(\frac{p}{q}\right)p$
$\mathbb{Q}(\sqrt{-pq})$	$3, 5$ [2]	1	0	$-p$
$\mathbb{Q}(\sqrt{-2pq})$	$5, 5$	1	0	-1
	$3, 5$	1	0	p
	$3, 3$	1	0	-1

Table II

F	$p, q \pmod 8$	The Legendre symbols		r_4 (δ)
$\mathbb{Q}(\sqrt{-pq})$ $\mathbb{Q}(\sqrt{-2pq})$	$1, 1$	$\left(\frac{q}{p}\right) = -1$	$\left(\frac{v}{p}\right) = -\left(\frac{v}{q}\right)(*)$	0
			$\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right)$	1
		$\left(\frac{q}{p}\right) = 1$	$\left(\frac{v}{p}\right) = -1$ or $\left(\frac{v}{q}\right) = -1$	1
			$\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = 1$	2
	$1, 3$	$\left(\frac{q}{p}\right) = -1$		0 ($\delta = -1$)
		$\left(\frac{q}{p}\right) = 1$		1
	$1, 5$	$\left(\frac{q}{p}\right) = -1$		0 ($\delta = -1$)
		$\left(\frac{q}{p}\right) = 1$		1
	$1, 7$	$\left(\frac{q}{p}\right) = -1$		0
		$\left(\frac{q}{p}\right) = 1$	$\left(\frac{v}{p}\right) = -1$	0
			$\left(\frac{v}{p}\right) = 1$	1
	$7, 7$		$\left(\frac{v}{p}\right) = -\left(\frac{v}{q}\right)(*)$	0
			$\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right)$	1
$\mathbb{Q}(\sqrt{-pq})$	$3, 3$			1
	$5, 5$			1

2. If $p \equiv q \pmod 8$ (or $q \equiv r \pmod 8$ or $p \equiv q \equiv r \pmod 8$), then the condition on the Legendre symbols, say $(\cdot)$, should be understood as: if there is a choice of p, q, r with the Legendre symbols satisfying $(\cdot)$. For example, in the case $7, 7, 5$ in Table III, the condition on the Legendre symbol is

Table III

F	$p,q,r \pmod 8$	The Legendre symbols	δ
$\mathbb{Q}(\sqrt{-pqr})$ $\mathbb{Q}(\sqrt{-2pqr})$	$7,7,5$	$\left(\frac{p}{r}\right)=-1$	$-r$ if $\left(\frac{q}{r}\right)=-1$; $\left(\frac{q}{p}\right)q$ if $\left(\frac{q}{r}\right)=1$
	$7,7,3$	$\left(\frac{p}{r}\right)=1$	$-r$ if $\left(\frac{r}{q}\right)=-1$; $\left(\frac{q}{p}\right)q$ if $\left(\frac{r}{q}\right)=1$
	$7,5,1$	$\left(\frac{p}{r}\right)=-1$	$-r$ if $\left(\frac{r}{q}\right)=-1$; $\left(\frac{q}{p}\right)q$ if $\left(\frac{r}{q}\right)=1$
		$\left(\frac{q}{r}\right)=-1$	$-\left(\frac{q}{p}\right)p$ if $\left(\frac{r}{p}\right)=1$
	$7,3,1$	$\left(\frac{p}{r}\right)=-1$	$-r$ if $\left(\frac{r}{q}\right)=-1$; $\left(\frac{q}{p}\right)q$ if $\left(\frac{r}{q}\right)=1$
		$\left(\frac{q}{r}\right)=-1$	$\left(\frac{p}{q}\right)p$ if $\left(\frac{p}{r}\right)=1$
	$3,3,3$	$\left(\frac{p}{q}\right)=\left(\frac{q}{r}\right)=\left(\frac{r}{p}\right)$	-1
$\mathbb{Q}(\sqrt{-pqr})$	$7,5,5$	$\left(\frac{q}{p}\right)=-1$	r if $\left(\frac{p}{r}\right)=1$; $-p$ if $\left(\frac{p}{r}\right)=-1$
	$7,3,3$	$\left(\frac{q}{p}\right)=1$	$-p$ if $\left(\frac{p}{r}\right)=-1$; $-r$ if $\left(\frac{p}{r}\right)=1$
	$5,5,3$	$\left(\frac{p}{r}\right)=-1$	r if $\left(\frac{q}{r}\right)=-1$; $\left(\frac{q}{p}\right)q$ if $\left(\frac{q}{r}\right)=1$
	$5,3,3$	$\left(\frac{q}{p}\right)=-1$	$-p$ if $\left(\frac{r}{p}\right)=-1$; $\left(\frac{r}{q}\right)r$ if $\left(\frac{r}{p}\right)=1$
	$5,3,1$	$\left(\frac{r}{p}\right)=-1$	r if $\left(\frac{r}{q}\right)=-1$; $-q$ if $\left(\frac{r}{q}\right)=1$
		$\left(\frac{r}{q}\right)=-1$	p if $\left(\frac{r}{p}\right)=1$
$\mathbb{Q}(\sqrt{-2pqr})$	$7,5,5$	$\left(\frac{q}{p}\right)=1$	$-p$ if $\left(\frac{p}{r}\right)=1$; $-r$ if $\left(\frac{p}{r}\right)=-1$
	$7,5,3$		$-\left(\frac{qr}{p}\right)p$
	$7,3,3$	$\left(\frac{q}{p}\right)=-1$	$-p$ if $\left(\frac{p}{r}\right)=-1$; r if $\left(\frac{p}{r}\right)=1$
	$5,5,3$	$\left(\frac{p}{r}\right)=-1$	r if $\left(\frac{q}{r}\right)=1$; $-\left(\frac{q}{p}\right)q$ if $\left(\frac{q}{r}\right)=-1$
	$5,5,1$	$\left(\frac{pq}{r}\right)=-1$	-1
	$5,3,3$	$\left(\frac{q}{p}\right)=1$	$-p$ if $\left(\frac{r}{p}\right)=1$; $\left(\frac{q}{r}\right)r$ if $\left(\frac{r}{p}\right)=-1$
	$5,3,1$	$\left(\frac{r}{p}\right)=-1$	r if $\left(\frac{r}{q}\right)=-1$; q if $\left(\frac{r}{q}\right)=1$
		$\left(\frac{r}{q}\right)=-1$	$-p$ if $\left(\frac{r}{p}\right)=1$
	$3,3,1$	$\left(\frac{pq}{r}\right)=-1$	-1

$\left(\frac{p}{r}\right)=-1$. In practice, we identify $\left(\frac{q}{r}\right)=-1$ with $\left(\frac{p}{r}\right)=-1$. Hence, if $\left(\frac{q}{r}\right)=-1$ then we also have $r_2=0$.

Proof of Theorem 5.1. We will repeatedly use the notations $K, \overline{K}$, V and $\overline{V}$ which are defined in Section 4.

It is not hard to verify the correctness of the statement $r_4=0$ when δ

Table IV

F	$p,q,r \pmod 8$	The Legendre symbols	r_4	δ
$\mathbb{Q}(\sqrt{-pqr})$	$7,5,3$		1	
	$5,5,5$	$\left(\frac{q}{p}\right)=\left(\frac{r}{p}\right)=-1$	0	-1
		$\left(\frac{q}{p}\right)=\left(\frac{p}{r}\right)=\left(\frac{r}{q}\right)=1$	2	
		otherwise	1	
	$5,5,1$	$\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$	2	
		otherwise	1	
	$3,3,1$	$\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$	2	
		otherwise	1	
$\mathbb{Q}(\sqrt{-2pqr})$	$5,5,5$	$\left(\frac{q}{p}\right)=\left(\frac{p}{r}\right)=1$	0	-1
		$\left(\frac{q}{p}\right)=\left(\frac{p}{r}\right)=\left(\frac{r}{p}\right)=-1$	2	
		otherwise	1	
$\mathbb{Q}(\sqrt{-pqr})$ $\mathbb{Q}(\sqrt{-2pqr})$	$5,1,1$	$\left(\frac{q}{p}\right)=\left(\frac{r}{p}\right)=-1$	0	-1
		$\left(\frac{p}{q}\right)=\left(\frac{r}{q}\right)=-1$	0	-1
		$\left(\frac{q}{p}\right)=\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$	2	
		otherwise	1	
	$3,1,1$	$\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=-1$	0	-1
		$\left(\frac{q}{p}\right)=\left(\frac{r}{p}\right)=-1$	0	-1
		$\left(\frac{q}{p}\right)=\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$	2	
		otherwise	1	

has been listed. In fact, one can easily check that $\overline{K}=\{\delta,-d/\delta\}$ (or $\overline{K}=\{\delta,-d/(2\delta)\}$) and $\overline{V}=\emptyset$. Then the result follows from Theorem 4.1.

On the other hand, $r_4=r_2$ if and only if $K=\overline{K}$ and $V=\overline{V}$. Hence, it is also easy to verify the correctness of the statement $r_4=r_2$.

Now, for Tables I, II we only need to consider the following cases: 1,1; 1,7; 7,7.

The case $1,1$. Clearly, $r_2=2$ and $-1\in\overline{K}$. Suppose $\left(\frac{q}{p}\right)=-1$. Then $pZ^2=X^2-dY^2$ has no solutions in $\mathbb{Z}$, hence $\pm p\notin\overline{K}$, so $r_4\le 1$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=1$, then $v\in\overline{V}$, hence $r_4\ge 1$, therefore $r_4=1$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=-1$, then $pv\in\overline{V}$, hence $r_4=1$. If $\left(\frac{v}{p}\right)=-\left(\frac{v}{q}\right)$, then $\overline{V}=\emptyset$, hence $r_4=0$. Suppose $\left(\frac{q}{p}\right)=1$. Then $\pm p\in\overline{K}$, hence $r_4\ge 1$. If $\left(\frac{v}{p}\right)=-1$, or $\left(\frac{v}{q}\right)=-1$,

Table V

F	$p,q,r \pmod 8$	The Legendre symbols		r_4
$\mathbb{Q}(\sqrt{-pqr})$ $\mathbb{Q}(\sqrt{-2pqr})$ $r_2=3$	$7,7,7$ $\left(\frac{p}{r}\right)=1$	$\left(\frac{q}{r}\right)=1$	$\left(\frac{v}{p}\right)=\left(\frac{v}{r}\right)$	1
			$\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)$	1
		$\left(\frac{q}{p}\right)=\left(\frac{q}{r}\right)=-1$	$\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)$	1
		otherwise		0
	$7,7,1$	$\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$	$\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right),\left(\frac{v}{r}\right)=1$	2
			otherwise	1
		otherwise	$\left(\frac{v}{pqr}\right)=1$	1
			$\left(\frac{v}{pqr}\right)=-1(*)$	0
	$7,1,1$	$\left(\frac{q}{p}\right)=\left(\frac{r}{p}\right)=\left(\frac{r}{q}\right)=1$	$\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=1$	2
			otherwise	1
		$\left(\frac{q}{p}\right)=-1,\ \left(\frac{r}{p}\right)=\left(\frac{r}{q}\right)=1$	$\left(\frac{v}{r}\right)=1$	1
		$\left(\frac{r}{q}\right)=-1,\ \left(\frac{q}{p}\right)=\left(\frac{r}{p}\right)=1$	$\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)$	1
		otherwise		0
	$1,1,1$	$\left(\frac{q}{p}\right)=\left(\frac{r}{p}\right)=\left(\frac{r}{q}\right)=1$	$\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=1$	3
			otherwise	2
		$\left(\frac{q}{p}\right)=-1,\ \left(\frac{r}{p}\right)=\left(\frac{r}{q}\right)=1$	$\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right),\ \left(\frac{v}{r}\right)=1$	2
			otherwise	1
		otherwise	$\left(\frac{v}{pqr}\right)=1$	1
			$\left(\frac{v}{pqr}\right)=-1(*)$	0

then $v \notin \overline{V}$, hence $r_4 \le 1$, so $r_4 = 1$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = 1$, then $K = \overline{K}$ and $V = \overline{V}$, hence $r_4 = 2$.

The case $1,7$. We have $r_2 = 2$ and $-1 \notin \overline{K}$, hence $r_4 \le 1$. Suppose $\left(\frac{q}{p}\right) = -1$. Then $\pm p \notin \overline{K}$, hence $r_4 = 0$. Suppose $\left(\frac{q}{p}\right) = 1$. If $\left(\frac{v}{p}\right) = -1$, then $\overline{K} = \{p, -q\}, \overline{V} = \emptyset$, hence $r_4 = 0$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = 1$, then $v \in \overline{K}$, hence $r_4 \ge 1$, so $r_4 = 1$.

The case $7,7$. We have $r_2 = 2$ and $-1 \notin \overline{K}$, hence $r_4 \le 1$. Suppose $\left(\frac{q}{p}\right) = 1$. Then $q \in \overline{K}$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = 1$, then $v \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = -1$, then $-v \in \overline{V}$, hence $r_4 \ge 1$, so $r_4 = 1$; if $\left(\frac{v}{p}\right) = -\left(\frac{v}{q}\right)$, then $\overline{V} = \emptyset$, hence $r_4 = 0$.

The proof of Table III is direct.

For Table IV, we only need to consider the three cases: $7,5,3,\ 5,5,1$ and $3,3,1$ ($d=pqr$).

For the case $7,5,3$, we have $-1\notin\overline{K}$, hence $r_4\le 1$. But it is easy to see that $-\left(\frac{qr}{p}\right)p, \left(\frac{p}{q}\right)q\in\overline{K}$, $V=\overline{V}=\emptyset$, hence $r_4\ge 1$, so $r_4=1$.

For the case $5,5,1$ or $3,3,1$, we have $-1\in\overline{K}$, $V=\overline{V}=\emptyset$. If $\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$, then $K=\overline{K}$, hence $r_4=2$. Otherwise, we have $\left(\frac{p}{r}\right)=-1$ or $\left(\frac{q}{r}\right)=-1$. If $\left(\frac{p}{r}\right)=-1$, $\left(\frac{q}{r}\right)=1$, then $\pm p\notin\overline{K}$, $\pm q\in\overline{K}$; if $\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=-1$, then $\pm r\in\overline{K}$, hence, we have $r_4=1$.

Finally, we consider Table V. Clearly, in any case, $r_2=3$. Without loss of generality, when $2\nmid d$, or $pqr\equiv 7 \pmod 8$, we can assume $\left(\frac{v}{pqr}\right)=1$. On the other hand, when $d=2pqr$ with $pqr\equiv 1 \pmod 8$, if $\left(\frac{v}{pqr}\right)=-1$, then it is easy to see that $\overline{V}=\emptyset$. Hence, we always assume $\left(\frac{v}{pqr}\right)=1$.

The case $7,7,7$. We have $-1,p,q,r\notin\overline{K}$, hence $r_4\le 1$. Suppose $\left(\frac{p}{r}\right)=\left(\frac{r}{q}\right)=\left(\frac{q}{p}\right)$, then $\pm p,\pm q,\pm r\notin\overline{K}$, hence $r_4=0$. Since $\left(\frac{p}{r}\right)=1$, there are the following possibilities:

$$\left(\frac{q}{p}\right)=\left(\frac{q}{r}\right)=1,\qquad \left(\frac{p}{q}\right)=\left(\frac{q}{r}\right)=1,\qquad \left(\frac{p}{q}\right)=\left(\frac{r}{q}\right)=1.$$

Suppose $\left(\frac{q}{p}\right)=\left(\frac{q}{r}\right)=1$. Then $-r\in\overline{K}$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=1$, then $v\in\overline{V}$, and if $\left(\frac{v}{p}\right)=\left(\frac{v}{r}\right)=-1$, $\left(\frac{v}{q}\right)=1$, then $-pv\in\overline{V}$, hence $r_4\ge 1$, so $r_4=1$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=-1$, $\left(\frac{v}{r}\right)=1$, or $\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=-1$, $\left(\frac{v}{p}\right)=1$, then $\overline{V}=\emptyset$, hence $r_4=0$.

Similarly, suppose $\left(\frac{p}{q}\right)=\left(\frac{q}{r}\right)=1$. Then $-r\in\overline{K}$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=1$, then $v\in\overline{V}$, and if $\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=-1$, $\left(\frac{v}{p}\right)=1$, then $-pv\in\overline{V}$, hence $r_4=1$. Otherwise, $r_4=0$.

Suppose $\left(\frac{p}{q}\right)=\left(\frac{r}{q}\right)=1$. Then $-q\in\overline{K}$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=1$, then $v\in\overline{V}$, and if $\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=-1$, $\left(\frac{v}{p}\right)=1$, then $-pv\in\overline{V}$, hence $r_4=1$. Otherwise $r_4=0$.

The case $7,7,1$. We have $-1\notin\overline{K}$. Suppose $\left(\frac{p}{r}\right)=-1$. Then $\pm p\notin\overline{K}$. If $\left(\frac{q}{r}\right)=1$, then $\left(\frac{q}{p}\right)q\in\overline{K}$ and $\pm r,\left(\frac{p}{q}\right)q\notin\overline{K}$, and if $\left(\frac{q}{r}\right)=-1$, then $-r\in\overline{K}$ and $\pm q,r\notin\overline{K}$. Hence $r_4\le 1$. If $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=1$, then $v\in\overline{V}$; if $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=-1$, and $\left(\frac{v}{r}\right)=1$, then $-v\in\overline{V}$; if $\left(\frac{v}{p}\right)=\left(\frac{v}{r}\right)=-1$ and $\left(\frac{v}{q}\right)=1$, then $\left(\frac{p}{q}\right)pv\in\overline{V}$; if $\left(\frac{v}{q}\right)=\left(\frac{v}{r}\right)=-1$ and $\left(\frac{v}{p}\right)=1$, then $\left(\frac{q}{p}\right)pv\in\overline{V}$. Hence $r_4\ge 1$. So $r_4=1$. This discussion also works for $\left(\frac{q}{r}\right)=-1$.

Suppose $\left(\frac{p}{r}\right)=\left(\frac{q}{r}\right)=1$. Then $\left(\frac{p}{q}\right)p,\left(\frac{q}{p}\right)q\in\overline{K}$. If $\left(\frac{v}{r}\right)=-1$, then either $\left(\frac{v}{p}\right)=-1$ and $\left(\frac{v}{q}\right)=1$, or $\left(\frac{v}{p}\right)=1$ and $\left(\frac{v}{q}\right)=-1$. In both cases, $\pm pv,\pm qv,\pm rv\notin\overline{V}$. If $\left(\frac{v}{r}\right)=1$, then either $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=1$ or $\left(\frac{v}{p}\right)=\left(\frac{v}{q}\right)=-1$, therefore either $v\in\overline{V}$ or $-v\in\overline{V}$, hence $r_4\ge 2$, so $r_4=2$.

The case $7,1,1$. We have $-1 \notin \overline{K}$, hence $r_4 \le 2$. Suppose $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = 1$. Then $-p, q, r \in \overline{K}$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $v \in \overline{V}$, hence $r_4 \ge 2$, so $r_4 = 2$. Otherwise, $\pm v \notin \overline{V}$, hence $\pm pv, \pm qv, \pm rv \notin \overline{V}$, since $-p, q, r \in \overline{K}$. Hence $r_4 = 1$.

Suppose $\left(\frac{p}{r}\right) = \left(\frac{q}{r}\right) = -1$ or $\left(\frac{p}{r}\right) = \left(\frac{q}{p}\right) = -1$ or $\left(\frac{q}{r}\right) = \left(\frac{q}{p}\right) = -1$. Then $\pm p, \pm q, \pm r \notin \overline{K}$, hence $r_4 = 0$.

Suppose $\left(\frac{q}{p}\right) = -1$ and $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = 1$. Then $r \in \overline{K}$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $v \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = -1$ and $\left(\frac{v}{r}\right) = 1$, then $qv \in \overline{V}$, hence $r_4 = 1$. Otherwise, $\overline{V} = \emptyset$, hence $r_4 = 0$. Suppose $\left(\frac{r}{q}\right) = -1$ and $\left(\frac{r}{p}\right) = \left(\frac{q}{p}\right) = 1$. Then $q \in \overline{K}$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $v \in \overline{V}$, and if $\left(\frac{v}{p}\right) = 1$ and $\left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = -1$, then $rv \in \overline{V}$, hence $r_4 = 1$. Otherwise, $\overline{V} = \emptyset$, hence $r_4 = 0$.

The case $1,1,1$. We have $-1 \in \overline{K}$. Suppose $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = 1$. Then $K = \overline{K}$, hence $r_4 \ge 2$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $V = \overline{V}$, hence $r_4 = 3$. Otherwise, $v \notin \overline{K}$, hence $r_4 = 2$.

Suppose $\left(\frac{q}{p}\right) = \left(\frac{q}{r}\right) = -1$, $\left(\frac{r}{p}\right) = 1$. Then $\pm p, \pm q, \pm r \notin \overline{K}$, hence $r_4 \le 1$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $v \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = -1$ and $\left(\frac{v}{r}\right) = 1$, then $pv \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{r}\right) = -1$ and $\left(\frac{v}{q}\right) = 1$, then $qv \in \overline{V}$; if $\left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = -1$ and $\left(\frac{v}{p}\right) = 1$, then $rv \in \overline{V}$. In any case, $r_4 \ge 1$, so $r_4 = 1$.

Suppose $\left(\frac{q}{p}\right) = \left(\frac{q}{r}\right) = \left(\frac{r}{p}\right) = -1$. Then $r_4 \le 1$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $v \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = -1$ and $\left(\frac{v}{r}\right) = 1$, then $rv \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{r}\right) = -1$ and $\left(\frac{v}{q}\right) = 1$, then $qv \in \overline{V}$; if $\left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = -1$ and $\left(\frac{v}{p}\right) = 1$, then $pv \in \overline{V}$. In any case, $r_4 \ge 1$, so $r_4 = 1$.

Suppose $\left(\frac{q}{p}\right) = -1$ and $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = 1$. Then $\pm r \in \overline{K}$, $\pm p, \pm q \notin \overline{K}$. If $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = \left(\frac{v}{r}\right) = 1$, then $v \in \overline{V}$; if $\left(\frac{v}{p}\right) = \left(\frac{v}{q}\right) = -1$ and $\left(\frac{v}{r}\right) = 1$, then $qv \in \overline{V}$. In both cases, $r_4 = 2$. Otherwise $\overline{V} = \emptyset$, hence $r_4 = 1$.

This concludes the proof of the theorem.

Remarks. 1. Our method can be applied to any imaginary quadratic field.

2. Similar result for real quadratic fields have been obtained by the author (see [12]).

Acknowledgements. I would like to thank the referee for the valuable comments and sending me the paper [4] from which I know that most results of Tables I and II have been obtained by P. E. Conner and J. Hurrelbrink by a different method. I would also like to thank Prof. J. Browkin for the helpful suggestions which have been incorporated herein. Finally, I would like to thank Prof. Tong Wenting for his help.

References

[1] B. Brauckmann, *The* 2*-Sylow subgroup of the tame kernel of number fields*, Canad. J. Math. 43 (1991), 215–264.

[2] 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.

[3] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, London, 1978.

[4] P. E. Conner and J. Hurrelbrink, *Examples of quadratic number fields with* $K_2(O)$ *containing no elements of order four*, preprint.

[5] —, —, *The* 4*-rank of* $K_2(O)$, Canad. J. Math. 41 (1989), 932–960.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.

[7] M. Kolster, *The structure of the* 2*-Sylow subgroup of* $K_2(O)$, I, Comment. Math. Helv. 61 (1986), 576–588.

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

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

[10] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, Berlin, 1963.

[11] H. Qin, K_2 *and algebraic number theory*, Ph.D. Thesis, Nanjing University, 1992.

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

[13] J. Tate, *Relations between* K_2 *and Galois cohomology*, Invent. Math. 36 (1976), 257–274.

DEPARTMENT OF MATHEMATICS
NANJING UNIVERSITY
NANJING, 210008, P.R. CHINA

Received on 3.9.1993
and in revised form on 18.1.1994 (2478)