ACTA ARITHMETICA
LXXII.4 (1995)

The 4-rank of K_2O_F for real quadratic fields F

by

HOURONG QIN (Nanjing)

1. Introduction. Let F be a number field, and let O_F be the ring of its integers. Several formulas for the 4-rank of K_2O_F are known (see [7], [5], etc.). If $\sqrt{-1} \notin F$, then such formulas are related to S-ideal class groups of F and $F(\sqrt{-1})$, and the numbers of dyadic places in F and $F(\sqrt{-1})$, where S is the set of infinite dyadic places of F. In [11], the author proposes a method which can be applied to determine the 4-rank of K_2O_F for real quadratic fields F with $2 \notin NF$. The author also lists many real quadratic fields with the 2-Sylow subgroups of K_2O_F being isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. In [12], the author gives a 4-rank K_2O_F formula for imaginary quadratic fields F. By the formula, it is enough to compute some Legendre symbols when one wants to know 4-rank K_2O_F for a given imaginary quadratic field F. In the present paper, we give a similar formula for real quadratic fields F. Then we give 4-rank K_2O_F tables for real quadratic fields $F = \mathbb{Q}(\sqrt{d})$ whose discriminants have at most three odd prime divisors.

2. Preliminaries. Given integers a, b with $b \neq 0$, (a/b) denotes the Jacobi symbol, in particular, if $b = p$, an odd prime, then (a/p) is the Legendre symbol. Denote by $\mathbb{N}$ the set of all positive integers. Let $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$ squarefree. Put $\Delta = \{c \in F^{\cdot} \mid \{-1, c\} = 1\}$. Then by a result of Tate [13], it is quite easy to see that for any real quadratic field F, $[\Delta : F^{\cdot 2}] = 2$, and if $F \neq \mathbb{Q}(\sqrt{2})$, then $\Delta = F^{\cdot 2} \cup 2F^{\cdot 2}$. By [2], we know that if $c \in \{-1, 2, -2\} \cap NF$, then there are $u, w \in \mathbb{N}$ such that $d = u^2 - cw^2$. Also by [2], we have:

LEMMA 2.1. *Let $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$ squarefree. Then the subgroup of K_2O_F consisting of all elements of order ≤ 2 can be generated by the following elements*:

- $\{-1, m\}$, $m \mid d$;
- $\{-1, u_i + \sqrt{d}\}$ *with* $d = u_i^2 - c_i w_i^2$, *where* $c_i \in \{-1, 2, -2\}$ *and* $u_i, w_i \in \mathbb{N}$.

In [11], the author shows the following theorem.

THEOREM 2.2. *Let $F=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{N}$ squarefree. Then for every $m\,|\,d$ with $m\in\mathbb{N}$, there exists $\alpha\in K_2O_F$ with $\alpha^2\in\{-1,m\}$ if and only if there exists $\varepsilon\in\{\pm1,\pm2\}$ such that*

$$(dm^{-1}/p)=(\varepsilon/p)\quad \text{for every odd prime } p\,|\,m;$$

and

$$(m/l)=(\varepsilon/l)\quad \text{for every odd prime } l\,|\,dm^{-1}.$$

In the next section, we shall deal with the case when $2\in NF$. Then we can obtain the 4-rank K_2O_F formula for a real quadratic field F.

3. The 4-rank of K_2O_F. Let $F=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{N}$ squarefree. Suppose that $2\in NF$. Then $d=u^2-2w^2$ with $u,w\in\mathbb{N}$. We want to know when there exists $\alpha\in K_2O_F$ such that $\alpha^2=\{-1,u+\sqrt{d}\}$. By a theorem due to Bass and Tate [8], we see that there exists $\beta\in K_2F$ such that $\{-1,u+\sqrt{d}\}=\beta^2$ if and only if there exist $x,y\in F$ with $x^2+y^2=u+\sqrt{d}$.

LEMMA 3.1. *Let $F=\mathbb{Q}(\sqrt{d}),d\in\mathbb{N}$ squarefree. Assume that $d=u^2-2w^2\equiv1 \pmod 8$, where $u,w\in\mathbb{N}$. If $(u+w/d)=-1$, then in F, $u+\sqrt{d}$ cannot be represented by the sum of two squares.*

Proof. Since $d\equiv1\pmod 8$, $2O_F=P\overline{P}$, where $P\neq\overline{P}$ is a prime ideal of F. We have F_P (the completion of F at P) $\cong\mathbb{Q}_2$. We may assume that $F\subseteq\mathbb{Q}_2$.

It follows from $d=u^2-2w^2$ that $(-d/u+w)=1$. Hence, $(u+w/d)=-1$ implies that $u+w\equiv3\pmod 4$. We note that if v is a unit in $\mathbb{Q}_2$, then the Hilbert symbol $\left(\frac{-1,v}{2}\right)_2=(-1)^{(v-1)/2}$ (see [9]). Hence, $x^2+y^2=-(u+w)$ is solvable in $\mathbb{Q}_2$. Therefore, $x^2+dy^2=-(u+w)$ is solvable in $\mathbb{Q}_2$. Suppose $x_0,y_0\in\mathbb{Q}_2$ is a solution of the equation $x^2+dy^2=-(u+w)$. Choose $g,h\in\mathbb{Q}_2$ such that $h=y_0$, $(u+w)g+wh=x_0$ and put $\alpha=g^2+h^2$, $\theta=(g^2-h^2+2gh)w$, $\lambda=(g^2-h^2-2gh)w$. A computation shows that

$$\begin{aligned}\alpha u+\theta&=(\alpha u+\theta)(u+w)(u+w)^{-1}\\&=(((u+w)g+wh)^2+(u^2-2w^2)h^2)(u+w)^{-1}\\&=(x_0^2+dy_0^2)(u+w)^{-1}=-1.\end{aligned}$$

Hence, there are $\xi,\eta\in\mathbb{Q}_2$ such that

$$2(u+\theta/\alpha)=2\alpha(\alpha u+\theta)/\alpha^2=-(\xi^2+\eta^2).$$

Let

$$\begin{aligned}x&=-\xi+\lambda\eta, & y&=\alpha\xi;\\ a&=-\eta-\lambda\xi, & b&=\alpha\eta.\end{aligned}$$

Then

$$\left(\frac{x+y\sqrt{d}}{2}\right)^2+\left(\frac{a+b\sqrt{d}}{2}\right)^2=-(u+\sqrt{d}).$$

If $u+\sqrt{d}=e^2+f^2$ with $e,f\in F\subseteq\mathbb{Q}_2$, then there are $s,t\in\mathbb{Q}_2$ such that $-1=s^2+t^2$. But in $\mathbb{Q}_2$, $\left(\frac{-1,-1}{2}\right)_2=-1$, contradiction. This concludes the proof.

THEOREM 3.2. *Let $F=\mathbb{Q}(\sqrt{d}), d\in\mathbb{N}$ squarefree. Assume that $d=u^2-2w^2$ with $u,w\in\mathbb{N}$. Then there exists $\beta\in K_2O_F$ such that $\beta^2=\{-1,u+\sqrt{d}\}$ if and only if there exists $\varepsilon\in\{\pm1,\pm2\}$ (equivalently, $\varepsilon\in\{\pm1\}$) such that $(\varepsilon(u+w)/p)=1$ for every odd prime $p\mid d$.*

P r o o f. First, if $d\not\equiv 1\pmod 8$, or $d\equiv 1\pmod 8$ and $(u+w/d)=1$, then analogously to the proof of Lemma 3.11 in [12], it can be shown that there exists a prime $p\equiv 1\pmod 4$ with $p\nmid d$, $p\nmid(u+w)$ and $p\nmid uw$ such that the Diophantine equation $X^2+dY^2=(u+w)pZ^2$ has nonzero solutions in $\mathbb{Z}$.

Second, entirely similarly to the proof of Lemma 3.12 in [12], it can be shown that there exists $\alpha\in K_2O_F$ with $\alpha^2=\{-1,u+\sqrt{d}\}$ if and only if there exists $\varepsilon\in\{\pm1,\pm2\}$ such that the Diophantine equation $\varepsilon pN^2=S^2-dT^2$ has nonzero solutions in $\mathbb{Z}$. It amounts to the same thing to say that $(\varepsilon(u+w)/p)=1$ for every odd prime $p\mid d$.

Finally, if $d\equiv 1\pmod 8$ and $(u+w/d)=-1$, then the number of primes p with $p\mid d$ and $(u+w/p)=-1$ must be odd. If there exists a prime $p\equiv 1\pmod 8$ with $p\mid d$ and $(u+w/p)=-1$, then $(\varepsilon(u+w)/p)=-1$ for every $\varepsilon\in\{\pm1,\pm2\}$. Otherwise, we may assume that for every $p\mid d$ with $(u+w/p)=-1$, $p\equiv 7\pmod 8$. Observe that $d\equiv 1\pmod 8$ and $2\in NF$. Hence, we can find a prime $p\equiv 7\pmod 8$, $p\mid d$ and $(u+w/p)=1$. For every $\varepsilon\in\{\pm1,\pm2\}$, we can find a prime $p\mid d$ such that $(\varepsilon(u+v)/p)=-1$. Our theorem is proved.

We now put Theorems 2.2 and 3.2 together and give the following theorem.

THEOREM 3.3. *Let $F=\mathbb{Q}(\sqrt{d}), d\in\mathbb{N}$ squarefree. Suppose that $d=u^2-2w^2$ with $u,w\in\mathbb{N}$. Then for every $m\mid d$ with $m\in\mathbb{N}$, there exists $\alpha\in K_2O_F$ with $\alpha^2=\{-1,m(u+\sqrt{d})\}$ if and only if we can find $\varepsilon\in\{\pm1,\pm2\}$ (in fact, $\varepsilon\in\{\pm1\}$ will be enough) such that*

$$(\varepsilon(u+w)/p)=(dm^{-1}/p)\quad \textit{for every odd prime } p\mid m$$

and

$$(\varepsilon(u+w)/p)=(m/p)\quad \textit{for every odd prime } p\mid dm^{-1}.$$

R e m a r k. When d has two odd prime divisors, a similar result has been obtained by B. Brauckmann (see [1]).

We conclude this section by giving a 4-rank K_2O_F formula for real quadratic fields F.

Let $F=\mathbb{Q}(\sqrt{d}), d\in\mathbb{N}$ squarefree. Put

$K_0=\{m \mid m\in\mathbb{N},\ m\,|\,d,\ m\neq 1, d, \frac{1}{2}d$ and $2\nmid m\}$,

$K=\{m \mid m\in K_0$, there exists $\varepsilon\in\{\pm1,\pm2\}$ such that $(dm^{-1}/p)=(\varepsilon/p)$ for every odd prime $p\,|\,m$ and $(m/l)=(\varepsilon/l)$ for every odd prime $l\,|\,dm^{-1}\}$,

$V_1=\{m(u+\sqrt{d}) \mid d=u^2-2w^2$ with $u,w\in\mathbb{N},\ m\in K_0\cup\{1,d\}\}$,

$V_0=\{m(u+\sqrt{d}) \mid m(u+\sqrt{d})\in V_1$, there exists $\varepsilon\in\{\pm1,\pm2\}$ such that $(\varepsilon(u+w)/p)=(dm^{-1}/p)$ for every odd prime $p\,|\,m$ and $(\varepsilon(u+v)/p)=(m/p)$ for every odd prime $p\,|\,dm^{-1}\}$,

$V=\{m(u+w) \mid m(u+\sqrt{d})\in V_0\}$.

THEOREM 3.4. *Notations being as above, let* $r=\#(K\cup V)$. *Then* $r_4=$ 4-rank $K_2O_F=\log_2\frac{1}{2}(r+2)$.

Proof. If $x\in F$ with $x<0$ or $N(x)<0$, then one can easily verify that there is no $\beta\in K_2F$ with $\{-1,x\}=\beta^2$. Hence, if $y\in K_2O_F$ is an element of order 4, then $y^2=\{-1,t\}$, by Theorems 2.2 and 3.3, $t\in K$ or $t\in V_0$. Therefore, we have $r=\#(K\cup V)=2^{r_4+1}-2$, this gives the desired 4-rank K_2O_F formula.

4. 4-rank K_2O_F tables

THEOREM 4.1. *Let* $F=\mathbb{Q}(\sqrt{d}), d\in\mathbb{N}$ *squarefree. Suppose that* $d=pq$, *or* $2pq$ *or* pqr *or* $2pqr$, *where* p, q, r *are odd primes. When* $2\in NF$, $d=u^2-2w^2$. *For simplicity, we write* $v=u+w$. *Then we have the following tables.*

Table I

F	$p,q\ (\mathrm{mod}\ 8)$	The Legendre symbols		4-rank K_2O_F
$\mathbb{Q}(\sqrt{pq})$ $\mathbb{Q}(\sqrt{2pq})$	$7,7$			1
	$7,1$	$(q/p)=1$	$(v/q)=1$	2
			$(v/q)=-1$	1
		$(q/p)=-1$		1
	$1,1$	$(q/p)=1$	$(v/p)=(v/q)=1$	2
			$(v/p)=-1$ or $(v/q)=-1$	1
		$(q/p)=-1$	$(v/p)=(v/q)$	1
			otherwise	0

Table II

F	$p, q \pmod 8$	The Legendre symbols	4-rank K_2O_F
$\mathbb{Q}(\sqrt{pq})$ $\mathbb{Q}(\sqrt{2pq})$	$7, 5$		1
	$7, 3$		1
	$5, 3$		1
	$5, 1$	$(q/p) = 1$	1
		otherwise	0
	$3, 1$	$(q/p) = 1$	1
		otherwise	0
$\mathbb{Q}(\sqrt{pq})$	$5, 5$		1
	$3, 3$		0
$\mathbb{Q}(\sqrt{2pq})$	$5, 5$		0
	$3, 3$		1

R e m a r k. Most results of Tables I and II have been listed by P. E. Conner and J. Hurrelbrink [4].

Table III

F	$p, q, r \pmod 8$	The Legendre symbols		4-rank K_2O_F
$\mathbb{Q}(\sqrt{pqr})$ $\mathbb{Q}(\sqrt{2pqr})$	$7, 7, 7$ $(q/p) = 1$	$(r/p) = (r/q)$	$(v/p) = (v/q)$	2
		otherwise		1
	$7, 7, 1$ $(q/p) = 1$	$(r/p) = (r/q) = 1$	$(v/r) = 1$	2
		$(r/p) = (r/q) = -1$	$(v/p) = (v/q)$	2
		otherwise		1
	$7, 1, 1$	$(q/p) = (r/p) = (r/q) = 1$	$(v/q) = (v/r) = 1$	3
			otherwise	2
		$(q/p) = (r/p) = 1$ $(r/q) = -1$	$(v/q) = (v/r)$	2
		$(r/p) = (r/q) = 1$ $(q/p) = -1$	$(v/r) = 1$	2
		otherwise		1
	$1, 1, 1$	$(q/p) = (r/p) = (r/q) = 1$	$(v/p) = (v/q) = (v/r) = 1$	3
			otherwise	2
		$(r/p) = (r/q) = 1$ $(q/p) = -1$	$(v/p) = (v/q)$, $(v/r) = 1$	2
			otherwise	1
		$(q/p) = (r/p) = -1$	$(v/(pqr)) = 1$	1
			otherwise	0

N o t e. In Table IV, C1 means that either $(q/p) = (r/p) = 1$, $(r/q) = -1$ or $(q/p) = (r/q) = 1$, $(r/p) = -1$ or $(r/p) = (r/q) = 1$, $(q/p) = -1$. C2 means that either $(q/p) = (r/p) = -1$, $(r/q) = 1$ or $(q/p) = (r/q) = -1$, $(r/p) = 1$ or $(r/p) = (r/q) = -1$, $(q/p) = 1$.

Table IV

F	$p, q, r \pmod 8$	The Legendre symbols	4-rank K_2O_F
$\mathbb{Q}(\sqrt{pqr})$ $\mathbb{Q}(\sqrt{2pqr})$	$7, 7, 5$	$(r/p) = (r/q) = -1$	2
		otherwise	1
	$7, 7, 3$	$(r/p) = (r/q) = -1$	2
		otherwise	1
	$7, 5, 3$		1
	$7, 5, 1$	$(r/p) = (r/q) = 1$	2
		otherwise	1
	$7, 3, 1$	$(r/p) = (r/q) = 1$	2
		otherwise	1
	$5, 3, 1$	$(r/p) = (r/q) = 1$	2
		otherwise	1
	$5, 1, 1$	$(q/p) = (r/p) = (r/q) = 1$	2
		C1	1
		otherwise	0
	$3, 3, 3$ $(q/p) = 1$	$(r/p) = 1$	1
		$(r/p) = (r/q) = -1$	1
		otherwise	0
	$3, 1, 1$	$(q/p) = (r/p) = (r/q) = 1$	2
		C1	1
		otherwise	0
$\mathbb{Q}(\sqrt{pqr})$	$7, 5, 5$	$(q/p) = (r/p) = 1$	2
		otherwise	1
	$7, 3, 3$	$(q/p) = (r/p) = 1$	2
		otherwise	1
	$5, 5, 5$	$(q/p) = (r/p) = (r/q) = 1$	2
		C1	1
		otherwise	0
	$5, 5, 3$	$(r/p) = (r/q) = 1$	2
		otherwise	1
	$5, 5, 1$	$(r/p) = (r/q) = 1$	2
		otherwise	1
	$5, 3, 3$	$(q/p) = (r/p) = -1$	2
		otherwise	1
	$3, 3, 1$	$(r/p) = (r/q)$	1
		otherwise	0
$\mathbb{Q}(\sqrt{2pqr})$	$7, 5, 5$	$(q/p) = (r/p) = -1$	2
		otherwise	1
	$7, 3, 3$	$(q/p) = (r/p) = -1$	2
		otherwise	1
	$5, 5, 5$	$(q/p) = (r/p) = (r/q) = -1$	2
		C2	1
		otherwise	0

Table IV (cont.)

F	$p, q, r \pmod 8$	The Legendre symbols	4-rank K_2O_F
$\mathbb{Q}(\sqrt{2pqr})$	$5,5,3$	$(r/p) = (r/q) = -1$	2
		otherwise	1
	$5,5,1$	$(r/p) = (r/q)$	1
		otherwise	0
	$5,3,3$	$(q/p) = (r/p) = 1$	2
		otherwise	1
	$3,3,1$	$(r/p) = (r/q) = 1$	2
		otherwise	1

When $p \equiv q \pmod 8$, or $q \equiv r \pmod 8$ or $p \equiv q \equiv r \pmod 8$, in view of symmetry, we omit some possibilities.

Proof of Theorem 4.1. By Theorem 3.4, it is enough to give K and V for each case.

In what follows, the symbol ε (ε') always stands for an element of the set $\{\pm 1, \pm 2\}$.

The verification of Tables I and II is direct. In fact, we have either $K = \emptyset$, or $\#(K) = 2$ and $\#(K) = 2$ if and only if $(\varepsilon/p) = (dp^{-1}/p)$ and $(\varepsilon/q) = (dq^{-1}/q)$. When $2 \in NF$, either $V = \emptyset$, or $\#(V) = 2$, or $\#(V) = 4$. We see that $\#(V) = 2$ if and only if either $(\varepsilon v/p) = (\varepsilon v/q) = 1$ or $(\varepsilon' v/p) = (q/p)$ together with $(\varepsilon' v/q) = (p/q)$, but not both, and $\#(V) = 4$ if and only if $(\varepsilon v/p) = (\varepsilon v/q) = 1$, $(\varepsilon' v/p) = (q/p)$ together with $(\varepsilon' v/q) = (p/q)$.

Next, we shall deal with the case when d has three odd prime divisors.

The case 7, 7, 7. Clearly, we can assume that $(q/p) = 1$. Suppose $(p/r) = (q/r) = 1$, then $K = \{q, pr\}$, if $(v/p) = (v/q) = (v/r)$, then $V = \{v, dv, qv, prv\}$, if $(v/p) = (v/q) = -(v/r)$, then $V = \{pv, qv, qrv, prv\}$; otherwise, $V = \emptyset$.

Suppose $(p/r) = -1$, $(q/r) = 1$. By a permutation $(p \leftrightarrow r)$, we see that this situation coincides with that of $(p/r) = (q/r) = 1$.

Suppose $(p/r) = (q/r) = -1$. By a permutation $(p \to r, q \to p, r \to q)$, we see that this situation also coincides with that of $(p/r) = (q/r) = 1$.

Suppose $(p/r) = 1$, $(q/r) = -1$. Then $K = \emptyset$. If $(v/p) = (v/q) = (v/r)$, then $V = \{v, dv\}$; if $(v/q) = (v/r) = -(v/p)$, then $V = \{qv, prv\}$; if $(v/p) = (v/q) = -(v/r)$, then $V = \{pv, qrv\}$; if $(v/p) = (v/r) = -(v/q)$, then $V = \{rv, pqv\}$.

The case 7, 7, 1. Assume $(q/p) = 1$. Suppose $(r/p) = (r/q) = 1$. Then $K = \{r, pq\}$ and for $(v/r) = 1$, we have: if $(v/p) = (v/q)$, then $V = \{v, dv, rv, pqv\}$; if $(v/p) = -(v/q)$, then $V = \{pv, qv, prv, qrv\}$. For $(v/r) = -1$, we have $V = \emptyset$.

Suppose $(r/p) = (r/q) = -1$. Then $K = \{r, pq\}$ and for $(v/p) = (v/q)$, we have: if $(v/r) = 1$, then $V = \{v, dv, rv, pqv\}$; if $(v/r) = -1$, then $V = \{pv, qv, prv, qrv\}$.

Suppose $(r/p) = 1$, $(r/q) = -1$. Then $K = \emptyset$. For $(v/r) = 1$, we have: if $(v/p) = (v/q)$, then $V = \{v, dv\}$; if $(v/p) = -(v/q)$, then $V = \{pv, qrv\}$. For $(v/r) = -1$, we have: if $(v/p) = (v/q)$, then $V = \{qv, prv\}$; if $(v/p) = -(v/q)$, then $V = \{rv, pqv\}$.

Similarly, suppose $(r/p) = -1$, $(r/q) = 1$. Then $K = \emptyset$ and $\#(V) = 2$.

The case 7, 1, 1. Suppose $(q/p) = (r/p) = (r/q) = 1$. Then $p, q, r \in K$, hence $\#(K) = 6$. If $(v/q) = (v/r) = 1$, then $\#(V) = 8$; otherwise, $V = \emptyset$.

Suppose $(q/p) = (r/p) = 1$, $(q/r) = -1$. Then $K = \{p, qr\}$. If $(v/q) = (v/r) = 1$, then $V = \{v, dv, pv, qrv\}$; if $(v/q) = (v/r) = -1$, then $V = \{qv, rv, pqv, prv\}$; otherwise, $V = \emptyset$.

Suppose $(q/p) = -1$, $(r/p) = (r/q) = 1$. Then $K = \{r, pq\}$. If $(v/q) = (v/r) = 1$, then $V = \{v, dv, rv, pqv\}$; if $(v/q) = -1$, $(v/r) = 1$, then $V = \{pv, qrv, prv, qrv\}$; otherwise, $V = \emptyset$.

Suppose $(q/p) = (r/p) = -1$, $(r/q) = 1$. Then $K = \emptyset$. If $(v/q) = (v/r) = 1$, then $V = \{v, dv\}$; if $(v/q) = (v/r) = -1$, then $V = \{pv, qrv\}$; if $(v/q) = -1$, $(v/r) = 1$, then $V = \{qv, prv\}$; if $(v/q) = 1$, $(v/r) = -1$, then $V = \{rv, pqv\}$.

Similarly, suppose $(q/p) = 1$, $(r/p) = (r/q) = -1$ or $(q/p) = (r/q) = 1$, $(r/p) = -1$ or $(q/p) = (r/p) = (r/q) = -1$. Then $K = \emptyset$ and $\#(V) = 2$.

The case 1, 1, 1. We only need to consider the following four possibilities:

1. $(q/p) = (r/p) = (r/q) = 1$;
2. $(q/p) = -1$, $(r/p) = (r/q) = 1$;
3. $(q/p) = (r/p) = -1$, $(r/q) = 1$;
4. $(q/p) = (r/p) = (r/q) = -1$.

In case 1, we have $p, q, r \in K$, hence $\#(K) = 6$. If $(v/p) = (v/q) = (v/r) = 1$, then $V = V_0$, hence $\#(V) = 8$, so $r_4 = 3$. Otherwise, $V = \emptyset$. Hence, $r_4 = 2$. In case 2, we have $K = \{r, pq\}$. If $(v/p) = (v/q) = (v/r) = 1$, then $V = \{v, dv, rv, pqv\}$; if $(v/p) = (v/q) = -1$, $(v/r) = 1$, then $V = \{pv, qv, prv, qrv\}$; otherwise, $V = \emptyset$. In cases 3 and 4, we have $K = \emptyset$. If $(v/p) = (v/q) = (v/r) = 1$, then $V = \{v, dv\}$; if $(v/p) = 1$, $(v/q) = (v/r) = -1$, then $V = \{pv, qrv\}$; if $(v/q) = 1$, $(v/p) = (v/r) = -1$, then $V = \{qv, prv\}$; if $(v/r) = 1$, $(v/p) = (v/q) = -1$, then $V = \{rv, pqv\}$.

The case 7, 7, 5 and the case 7, 7, 3. For $(r/p) = -1$, we have: if $(r/q) = -1$, then $p, q, r \in K$, hence, $\#(K) = 6$; if $(r/q) = 1$, then $K = \{p, qr\}$. For $(r/p) = 1$, we have: if $(r/q) = -1$, then $K = \{q, pr\}$; if $(r/q) = 1$, then $K = \{r, pq\}$.

The case $7,5,5$. Suppose $2\nmid d$. If $(q/p)=(r/p)=1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=-1$, then $K=\{p,qr\}$; if $(q/p)=1$, $(r/p)=-1$, then $K=\{q,pr\}$; if $(q/p)=-1$, $(r/p)=1$, then $K=\{r,pq\}$.

Suppose $2\mid d$. If $(q/p)=(r/p)=-1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=1$, then $K=\{p,qr\}$; if $(q/p)=-1$, $(r/p)=1$, then $K=\{q,pr\}$; if $(q/p)=1$, $(r/p)=-1$, then $K=\{r,pq\}$.

The case $7,5,3$. If $2\nmid d$, then $K=\{q,pr\}$. If $2\mid d$, then $K=\{r,pq\}$.

The case $7,5,1$. If $(r/p)=(r/q)=1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(r/p)=1$, $(r/q)=-1$, then $K=\{p,qr\}$; if $(r/p)=-1$, $(r/q)=1$, then $K=\{q,pr\}$; if $(r/p)=(r/q)=-1$, then $K=\{r,pq\}$.

The case $7,3,3$. Suppose $2\nmid d$. If $(q/p)=(r/p)=1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=-1$, then $K=\{p,qr\}$; if $(q/p)=1$, $(r/p)=-1$, then $K=\{q,pr\}$; if $(q/p)=-1$, $(r/p)=1$, then $K=\{r,pq\}$.

Suppose $2\mid d$. If $(q/p)=(r/p)=-1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=1$, then $K=\{p,qr\}$; if $(q/p)=-1$, $(r/p)=1$, then $K=\{q,pr\}$; if $(q/p)=1$, $(r/p)=-1$, then $K=\{r,pq\}$.

The case $7,3,1$. If $(r/p)=(r/q)=1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(r/p)=1$, $(r/q)=-1$, then $K=\{p,qr\}$; if $(r/p)=-1$, $(r/q)=1$, then $K=\{q,pr\}$; if $(r/p)=(r/q)=-1$, then $K=\{r,pq\}$.

The case $5,5,5$. Suppose $2\nmid d$. If $(q/p)=(r/p)=(r/q)=1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=1$, $(r/q)=-1$, then $K=\{p,qr\}$; if $(r/p)=(r/q)=-1$, then $K=\emptyset$.

Suppose $2\mid d$. If $(q/p)=(r/p)=(r/q)=-1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=-1$, $(r/q)=1$, then $K=\{p,qr\}$; if $(r/p)=(r/q)=1$, then $K=\emptyset$.

The case $5,5,3$. Suppose $2\nmid d$. If $(r/p)=1$, $(r/q)=-1$, then $K=\{p,qr\}$; if $(r/p)=-1$, $(r/q)=1$, then $K=\{q,pr\}$; if $(r/p)=(r/q)=1$, then $K=\{r,pq\}$.

Suppose $2\mid d$. If $(r/p)=-1$, $(r/q)=1$, then $K=\{p,qr\}$; if $(r/p)=1$, $(r/q)=-1$, then $K=\{q,pr\}$; if $(r/p)=(r/q)=1$, then $K=\{r,pq\}$.

The case $5,5,1$. Suppose $2\nmid d$. If $(r/p)=(r/q)=1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(r/p)=1$, $(r/q)=-1$, then $K=\{p,qr\}$; if $(r/p)=-1$, $(r/q)=1$, then $K=\{q,pr\}$; if $(r/p)=(r/q)=-1$, then $K=\{r,pq\}$.

Suppose $2\mid d$. If $(r/p)=(r/q)$, then $K=\{r,pq\}$; if $(r/p)=-(r/q)$, then $K=\emptyset$.

The case $5,3,3$. Suppose $2\nmid d$. If $(q/p)=(r/p)=-1$, then $p,q,r\in K$, hence, $\#(K)=6$; if $(q/p)=(r/p)=1$, then $K=\{p,qr\}$; if $(q/p)=-1$, $(r/p)=1$, then $K=\{q,pr\}$; if $(q/p)=1$, $(r/p)=-1$, then $K=\{r,pq\}$.

Suppose $2 \mid d$. If $(q/p) = (r/p) = 1$, then $p, q, r \in K$, hence, $\#(K) = 6$; if $(q/p) = (r/p) = -1$, then $K = \{p, qr\}$; if $(q/p) = 1$, $(r/p) = -1$, then $K = \{q, pr\}$; if $(q/p) = -1$, $(r/p) = 1$, then $K = \{r, pq\}$.

The case 5, 3, 1. If $(r/p) = (r/q) = 1$, then $p, q, r \in K$, hence, $\#(K) = 6$; if $(r/p) = 1$, $(r/q) = -1$, then $K = \{p, qr\}$; if $(r/p) = -1$, $(r/q) = 1$, then $K = \{q, pr\}$; if $(r/p) = (r/q) = -1$, then $K = \{r, pq\}$.

The case 5, 1, 1. If $(q/p) = (r/p) = (r/q) = 1$, then $p, q, r \in K$, hence, $\#(K) = 6$; if $(q/p) = (r/p) = 1$, $(r/q) = -1$, then $K = \{p, qr\}$; if $(q/p) = (r/q) = 1$, $(r/p) = -1$, then $K = \{q, pr\}$; if $(q/p) = -1$, $(r/p) = (r/q) = 1$, then $K = \{r, pq\}$; otherwise, $K = \emptyset$.

The case 3, 3, 3. Let $(q/p) = 1$. Suppose $2 \nmid d$. If $(r/q) = -1$, then $K = \{q, pr\}$; if $(r/p) = (r/q) = 1$, then $K = \{r, pq\}$; if $(r/p) = -1$, $(r/q) = 1$, then $K = \emptyset$.

Suppose $2 \mid d$. If $(r/p) = 1$, then $K = \{p, qr\}$; if $(r/p) = (r/q) = -1$, then $K = \{r, pq\}$; if $(r/p) = -1$, $(r/q) = 1$, then $K = \emptyset$.

The case 3, 3, 1. Suppose $2 \nmid d$. If $(r/p) = (r/q)$, then $K = \{r, pq\}$; otherwise, $K = \emptyset$.

Suppose $2 \mid d$. If $(r/p) = (r/q) = 1$, then $p, q, r \in K$, hence, $\#(K) = 6$; if $(r/p) = 1$, $(r/q) = -1$, then $K = \{p, qr\}$; if $(r/p) = -1$, $(r/q) = 1$, then $K = \{q, pr\}$; if $(r/p) = (r/q) = -1$, then $K = \{r, pq\}$.

The case 3, 1, 1. If $(q/p) = (r/p) = (r/q) = 1$, then $p, q, r \in K$, hence, $\#(K) = 6$; if $(q/p) = (r/p) = 1$, $(r/q) = -1$, then $K = \{p, qr\}$; if $(q/p) = (r/q) = 1$, $(r/p) = -1$, then $K = \{q, pr\}$; if $(q/p) = -1$, $(r/p) = (r/q) = 1$, then $K = \{r, pq\}$; otherwise, $K = \emptyset$.

The proof is complete.

Acknowledgements. I would like to thank Prof. Zhou Boxun and Prof. Tong Wenting for their help. And I am also very grateful to Prof. J. Browkin for his valuable suggestions.

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] 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.

[4] P. E. Conner and J. Hurrelbrink, *Examples of quadratic number fields with $K_2\mathcal{O}$ containing no element of order four*, preprint.

[5] —, —, *The 4-rank of $K_2\mathcal{O}$*, 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, *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).
[12] —, *The* 2-*Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. 69 (1995), 153–169.
[13] J. Tate, *Relations between* K_2 *and Galois cohomology*, Invent. Math. 36 (1976), 257–274.
[14] J. Urbanowicz, *On the* 2-*primary part of a conjecture of Birch and Tate*, Acta Arith. 43 (1983), 69–81.

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

Received on 24.5.1994
and in revised form on 21.10.1994 (2619)