MATHEMATICS OF COMPUTATION
Volume 69, Number 232, Pages 1667–1683
S 0025-5718(00)01182-0
Article electronically published on March 15, 2000

COMPUTING THE TAME KERNEL OF QUADRATIC IMAGINARY FIELDS

JERZY BROWKIN,
WITH AN APPENDIX BY KARIM BELABAS, AND HERBERT GANGL

ABSTRACT. J. Tate has determined the group $K_2\mathcal{O}_F$ (called the tame kernel) for six quadratic imaginary number fields $F = \mathbb{Q}(\sqrt{d})$, where $d = -3, -4, -7, -8, -11, -15$. Modifying the method of Tate, H. Qin has done the same for $d = -24$ and $d = -35$, and M. Skałba for $d = -19$ and $d = -20$.

In the present paper we discuss the methods of Qin and Skałba, and we apply our results to the field $\mathbb{Q}(\sqrt{-23})$.

In the Appendix at the end of the paper K. Belabas and H. Gangl present the results of their computation of $K_2\mathcal{O}_F$ for some other values of d. The results agree with the conjectural structure of $K_2\mathcal{O}_F$ given in the paper by Browkin and Gangl.

1. INTRODUCTION

J. Tate [T] has determined the tame kernel of all quadratic imaginary Euclidean fields F and of $F = \mathbb{Q}\left(\sqrt{-15}\right)$. He proved that all mappings ∂_v (see notation below) are isomorphisms if the norm of the prime ideal v of the field F is sufficiently large. Then he investigated the remaining v's (with small norms) performing necessary computations with symbols.

Unfortunately, for quadratic imaginary fields F with large discriminants, the number of exceptional v's which should be investigated individually, increases very fast.

Skałba [S] used a generalization of the classical theorem of Thue to get a reasonable bound for norms of exceptional v's, and he applied his result to the fields $\mathbb{Q}\left(\sqrt{-19}\right)$ and $\mathbb{Q}\left(\sqrt{-20}\right)$.

In the present paper we improve the estimates of Skałba essentially, and we get much smaller bounds for norms of exceptional v's. We apply these estımations in the case $F = \mathbb{Q}\left(\sqrt{-23}\right)$. Our estimations give reasonable bounds also for several other quadratic imaginary fields (see the Appendix by K. Belabas and H. Gangl at the end of this paper).

Let us remark that for real quadratic fields F much more is known; e.g., we can describe the tame kernel of every real quadratic field of discriminant less than, say, 5000. It is due to the fact that the order of the tame kernel for any real quadratic field can be expressed by means of corresponding Bernoulli numbers, or equivalently by Kronecker symbols, and consequently it can be easily computed.

Received by the editor January 14, 1998 and, in revised form, December 7, 1998.
1991 *Mathematics Subject Classification.* Primary 19C20; Secondary 11R11, 11R70, 11Y40.
Key words and phrases. Tame kernel, quadratic imaginary fields, Thue's theorem.

2. Notation

We shall use the notation of Tate [T] with minor changes, which will be described below.

For any number field F let

$$v_1,\ v_2,\ v_3,\dots \tag{1}$$

be all finite places of F ordered in such a way that $Nv_{m-1} \le Nv_m$, for $m = 2, 3, \dots$.

For $m \ge 0$ let $S_m = \{v_1, \dots, v_m\}$, thus $S_0 = \emptyset$. Denote by $\mathcal{O}_{S_m}$ the ring of S_m-integers of F, by U_{S_m} the group of S_m-units, and by k_{v_m} the residue field of the valuation v_m. Thus $\mathcal{O}_{S_0}$ is the ring $\mathcal{O}_F$ of integers of F, and U_{S_0} is the group U_F of units of F.

Let $K_2^{S_m}(F)$ be the subgroup of K_2F generated by symbols $\{a, b\}$, where $a, b \in U_{S_m}$. Then $K_2F = \bigcup_{m=1}^{\infty} K_2^{S_m}(F)$.

Let $\partial_{v_m} : K_2F \longrightarrow k_{v_m}^*$ be the tame symbol corresponding to v_m. Then $\partial_{v_m}(K_2^{S_{m-1}}(F)) = 0$, and we have the induced homomorphism (also denoted by ∂_{v_m})

$$\partial_{v_m} : K_2^{S_m}(F)/K_2^{S_{m-1}}(F) \longrightarrow k_{v_m}^*.$$

If the prime ideal of $\mathcal{O}_{S_m}$ corresponding to v_m is principal generated by π_m, we get the following commutative diagram

$$\begin{tikzcd}
 & U_{S_{m-1}} \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\
K_2^{S_m}(F)/K_2^{S_{m-1}}(F) \arrow[rr, "\partial v_m"] & & k_{v_m}^*
\end{tikzcd}$$

where $\alpha(u) = \{u, \pi_m\} \pmod{K_2^{S_{m-1}}(F)}$ and $\beta(u) = u \pmod{\pi_m}$, for $u \in U_{S_{m-1}}$.

Let $\partial = \bigoplus_{j=1}^{\infty} \partial_{v_j} \ :\ K_2F \longrightarrow \bigoplus_{j=1}^{\infty} k_{v_j}^*$, then $K_2\mathcal{O}_F = \ker \partial$.

Therefore if we prove, for some m and all $j \ge m$, that ∂_{v_j} is an isomorphism, then $\ker \partial \subset K_2^{S_{m-1}}(F)$. Since the group $U_{S_{m-1}}$ has a finite number of generators, they determine a finite set of generators of the group $K_2^{S_{m-1}}(F)$, which can be given explicitly. Then after some additional computations it is usually possible to determine the group $K_2\mathcal{O}_F$ itself.

Since we shall assume below that m is fixed, we simplify the notation as follows:

$$S := S_m,\ S' := S_{m-1},\ v := v_m,\ k = k_v := k_{v_m},\ \partial_v := \partial_{v_m},\ \pi := \pi_m,\ U := U_{S_{m-1}}.$$

Moreover, we denote by U_1 the group generated by $(1 + \pi U) \cap U$.

3. When is ∂_v an isomorphism?

We shall use the following general theorem of Tate.

Theorem 1 ([T], Proposition 1). *Suppose that W, C and G are subsets of U satisfying*

(1) *$W \subset CU_1$ and W generates U.*

(2) *$CG \subset CU_1$ and $\beta(G)$ generates k^*.*

(3) *$1 \in C \cap \ker \beta \subset U_1$.*

Then ∂_v is bijective. □

3.1. **Preliminary information on the class group.** Denote by q_F the least number such that in every class of ideals of $\mathcal{O}_F$ there is an ideal of norm $\leq q_F$. It is well known (see e.g., [C], p.141) that $q_F \leq \sqrt{|d|/3}$ for the quadratic imaginary field F of discriminant d.

Let Q be a set of representatives $\mathfrak{q}$ of all ideal classes satisfying $N\mathfrak{q} \leq q_F$. Moreover assume that $(1) \in Q$ represents the principal class.

Thus for every ideal $\mathfrak{a}$ of $\mathcal{O}_F$ there is a unique ideal $\mathfrak{q} \in Q$ such that the ideal $\mathfrak{a}\,\mathfrak{q}$ is principal.

In the next lemma we determine the values of q_F for some quadratic imaginary fields F.

Lemma 1. *Let $F = \mathbb{Q}(\sqrt{d})$ be the quadratic imaginary field with the discriminant d and the class number h_F.*

(i) *We have $q_F = 1$ iff $h_F = 1$,*
i.e., iff $d = -3, -4, -7, -8, -11, -19, -43, -67$ or -163.

(ii) *We have $q_F = 2$ iff $h_F = 2$ or 3 and $(\frac{d}{2}) \neq -1$,*
i.e., iff $d = -15, -20, -24, -40, -52, -88, -148$ or -232, for $h_F = 2$,
and $d = -23$ or -31, for $h_F = 3$.

(iii) *If $h_F = 2$ or 3 and $(\frac{d}{2}) = -1$ and $(\frac{d}{3}) \neq -1$, then $q_F = 3$,*
i.e., if $d = -35, -51, -123$ or -267, for $h_F = 2$,
and $d = -59, -83$ or -107, for $h_F = 3$.

(iv) *For other discriminants d, $-151 \leq d < 0$, we have the following values of q_F.*

d	-39	-47	-55	-56	-68	-71	-79	-84	-87
The class group	$\mathbb{Z}/4$	$\mathbb{Z}/5$	$\mathbb{Z}/4$	$\mathbb{Z}/4$	$\mathbb{Z}/4$	$\mathbb{Z}/7$	$\mathbb{Z}/5$	$(\mathbb{Z}/2)^2$	$\mathbb{Z}/6$
q_F	3	3	4	3	3	4	4	5	4
d	-91	-95	-103	-104	-111	-115	-116	-119	
The class group	$\mathbb{Z}/2$	$\mathbb{Z}/8$	$\mathbb{Z}/5$	$\mathbb{Z}/6$	$\mathbb{Z}/8$	$\mathbb{Z}/2$	$\mathbb{Z}/6$	$\mathbb{Z}/10$	
q_F	5	5	4	5	5	5	5	5	
d	-120	-127	-131	-132	-136	-139	-143	-151	
The class group	$(\mathbb{Z}/2)^2$	$\mathbb{Z}/5$	$\mathbb{Z}/5$	$(\mathbb{Z}/2)^2$	$\mathbb{Z}/4$	$\mathbb{Z}/3$	$\mathbb{Z}/10$	$\mathbb{Z}/7$	
q_F	5	4	5	6	5	5	6	5	

Proof. We apply the fact that all quadratic imaginary fields with small class numbers are known (see [A1], [A2], [W] and references given there).

(i) Obvious.

(ii) If $q_F = 2$, then by (i) we have $h_F > 1$, and to every nontrivial class of ideals belongs an ideal of norm 2. Consequently 2 is not inert, i.e., $(\frac{d}{2}) \neq -1$, $(2) = \mathfrak{p}_2\mathfrak{p}_2'$. Therefore there are at most two nontrivial classes, i.e., $h_F \leq 3$.

Conversely, if $h_F = 2$ or 3 and $(\frac{d}{2}) \neq -1$, then $|d| \geq 15$ and there is a prime ideal $\mathfrak{p}_2$ of norm 2. Since there is no element of norm 2, $\mathfrak{p}_2$ is not principal.

If $h_F = 2$, then $Q = \{(1), \mathfrak{p}_2\}$, if $h_F = 3$, then $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ and $\mathfrak{p}_2, \mathfrak{p}_2'$ belong to distinct ideal classes since the class number is odd. Hence $Q = \{(1), \mathfrak{p}_2, \mathfrak{p}_2'\}$. Thus in both cases $q_F = 2$.

(iii) Now the prime 2 is inert, but there is a prime ideal $\mathfrak{p}_3$ of norm 3. Since $|d| \geq 15$, the ideal $\mathfrak{p}_3$ is not principal, and we proceed similarly as in (ii).

(iv) It is an easy exercise on the ideals in quadratic number fields (see e.g., [C], Table III—some of the ideals given there can be replaced by ideals with smaller norms). □

One can characterize similarly quadratic imaginary fields F such that $q_F = 3$, $q_F = 4$, etc.

For example, $q_F = 3$ iff one of the following conditions holds:

(i) $(\frac{d}{2}) = -1$, $(\frac{d}{3}) \neq -1$ and $h_F = 2$ or 3;

(ii) $(\frac{d}{2}) \neq -1$, $(\frac{d}{3}) \neq -1$, $(\frac{d}{6}) = 0$ and $h_F = 4$ with cyclic class group;

(iii) $(\frac{d}{2}) = 1$, $(\frac{d}{3}) = 1$ and $h_F = 5$.

We leave the proof to the reader as an amusing exercise.

3.2. **The set W of generators of U.** We say that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ is earlier than v if the valuation corresponding to $\mathfrak{p}$ appears before v in the sequence (1).

We assume that $d < -4$ and that every ideal belonging to Q is a product of prime ideals earlier than v. This condition is obviously satisfied if $Nv > q_F$.

Let W be the set consisting of -1 and of generators $a \neq 1$ of principal ideals of $\mathcal{O}_F$ of the following forms:

(i) $(a) = \mathfrak{p}\mathfrak{q}$,

(ii) $(a) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$,

where $\mathfrak{p}$ is a prime ideal earlier than v, and $\mathfrak{q}, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3 \in Q$.

It follows that the set W is finite and $W \subset U \cap \mathcal{O}_F$.

Let us remark that if $h_F = 1$, then $Q = \{(1)\}$, thus we can omit the ideals (ii). Similarly, if $h_F = 2$, then we can assume in (ii) that $\mathfrak{q}_3 = (1)$.

Denote by $\langle W \rangle$ the group generated by W.

Lemma 2. $\langle W \rangle = U$.

Proof. 1) First we prove by induction on r that if a principal ideal

$$(a) = \mathfrak{q}_1 \cdots \mathfrak{q}_r,$$

where all $\mathfrak{q}_j \in Q$, then a belongs to $\langle W \rangle$.

If $r \leq 3$, then the claim follows from the definitions of W and Q.

If $r > 3$, then let $\mathfrak{q} \in Q$ represent the class containing the ideal $\mathfrak{q}_1\mathfrak{q}_2$, and let $\mathfrak{q}' \in Q$ represent the opposite class.

We have

$$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}' = (b), \quad \mathfrak{q}\mathfrak{q}' = (c),$$

where $b, c \in \langle W \rangle$ by the definition of W.

Consequently $b|ac$ and

$$(a)(c) = (b)\mathfrak{q}\mathfrak{q}_3 \cdots \mathfrak{q}_r.$$

From the inductive assumption it follows that

$$\mathfrak{q}\mathfrak{q}_3 \cdots \mathfrak{q}_r = (d),$$

where $d \in \langle W \rangle$. Hence $a = \pm bd/c \in \langle W \rangle$.

2) Let $u \in U$, and consider the prime ideal decomposition

$$(u) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)(\mathfrak{p}_{r+1} \cdots \mathfrak{p}_{r+s})^{-1}. \tag{2}$$

For $j = 1, \ldots, r+s$, we have $\mathfrak{p}_j$ is earlier than v and

$$\mathfrak{p}_j\mathfrak{q}_j = (a_j), \quad \text{for some } \mathfrak{q}_j \in Q.$$

Hence $a_j \in W$. Moreover, for an appropriate $\mathfrak{q} \in Q$, we have

$$\mathfrak{q}\mathfrak{q}_1 \cdots \mathfrak{q}_r = (b), \quad \text{where } b \in \mathcal{O}_F.$$

Hence b belongs to $\langle W\rangle$ by the first part of the proof.

Multiplying both sides of (2) by the ideal

$$(b)(a_{r+1})\cdots(a_{r+s}) = \mathfrak{q}\,\mathfrak{q}_1\cdots\mathfrak{q}_r\mathfrak{p}_{r+1}\cdots\mathfrak{p}_{r+s}\cdot\mathfrak{q}_{r+1}\cdots\mathfrak{q}_{r+s}$$

we get

$$(u)(b)(a_{r+1})\cdots(a_{r+s}) = \mathfrak{q}\,\mathfrak{q}_{r+1}\cdots\mathfrak{q}_{r+s}(a_1)\cdots(a_r).$$

Consequently the ideal $\mathfrak{q}\,\mathfrak{q}_{r+1}\cdots\mathfrak{q}_{r+s}$ is principal, and its generator, say t, belongs to $\langle W\rangle$ by the first part of the proof.

Therefore the element

$$u = \pm ta_1\cdots a_r/ba_{r+1}\cdots a_{r+s}$$

belongs to the group generated by W. □

Let us remark that if the set W satisfies condition (1) of Theorem 1, and some proper subset generates U, then obviously this subset also satisfies the condition (1). Thus in general we can replace the set W defined above by a smaller one.

Lemma 3. *For every $w \in W$, we have $Nw \le q_F Nv$, provided*

(i) $h_F \le 2$, *and* $q_F \le Nv$, *or*

(ii) $h_F > 2$ *and* $q_F^2 \le Nv$.

Proof. From the definition of W it follows that for every $w \in W$,

$$Nw \le \max(N\mathfrak{p}N\mathfrak{q}, N\mathfrak{q}_1N\mathfrak{q}_2N\mathfrak{q}_3) \le \max(q_FNv, q_F^3) \le q_FNv,$$

under the assumption (ii).

If $h_F \le 2$, we can assume that $\mathfrak{q}_3 = (1)$ in view of the remark before Lemma 2. Hence

$$Nw \le \max(N\mathfrak{p}N\mathfrak{q}, N\mathfrak{q}_1N\mathfrak{q}_2) \le \max(q_FNv, q_F^2) \le q_FNv$$

under the assumption (i). □

We shall frequently use the following lemma.

Lemma 4 ([T], Lemma 1). *If $a, b \in U \cap \mathcal{O}_F$, $\beta(a) = \beta(b)$ and $|a| + |b| < Nv$, then $a \in bU_1$.* □

3.3. **The set C of representatives modulo v.** First we make the following remark (see [T], proof of Propositon 1).

Remark 1. Condition (2) of Theorem 1 implies that $\beta(C) = k^*$.

Proof. From (2) it follows that $\beta(C)\beta(G) \subset \beta(C)$, and hence by induction on t we get $\beta(C)\beta(G)^t \subset \beta(C)$, for $t = 1, 2, \dots$.

For every $a \in k^*$ and $c \in C$ we have $a = \beta(c)a'$, for some $a' \in k^*$. Moreover a' is a product of generators of k^*:

$$a' = \beta(g_1)\cdots\beta(g_r), \quad \text{for some} \quad g_1, \dots, g_r \in G.$$

Hence $a = \beta(c)\beta(g_1)\cdots\beta(g_r) \in \beta(C)$, i.e., $\beta(C) = k^*$. □

We need the following version of the theorem of Thue generalized by Skałba.

Theorem 2. ([S], GTT and Lemma 3.2) *Let $Nv > M_d^2$, where $M_d := \frac{2}{\pi}\sqrt{|d|}$, and let real positive numbers h, h' satisfy*

(i) $\quad hh' = M_d\sqrt{Nv}$,

(ii) $\max(h, h') < \sqrt{Nv}$,

then for every $c \in F$, $v(c) = 0$, *there exist* $x_c, y_c \in \mathcal{O}_F$ *such that*

$$|x_c| \leq h,\ |y_c| \leq h',\ v(x_c) = v(y_c) = 0,\ \textit{and}\ \frac{x_c}{y_c} \equiv c \pmod{v}.$$

□

From now on we assume that $\sqrt{Nv} > 2M_d$, so Theorem 2 can be applied. For the fields with $|d| \geq 15$ we have $M_d = \frac{2}{\pi}\sqrt{|d|} \geq \frac{2}{\pi}\sqrt{15} > 2.4656\dots$. The open interval

$$I = \left(\sqrt{2}M_d,\ \frac{1}{\sqrt{2}}\sqrt{Nv}\right)$$

is not empty. Let h run over all numbers in I, and define $h' = \frac{M_d\sqrt{Nv}}{h}$. Then h' also runs over I. Evidently h and h' satisfy conditions (i) and (ii) of Theorem 2. From the theorem it follows that, for every $c \in F$, $v(c) = 0$, there exist $x_c, y_c \in \mathcal{O}_F$ such that

$$|x_c| \leq h,\ |y_c| \leq h',\ \text{ and } \beta(c) = \beta\left(\frac{x_c}{y_c}\right).$$

We define C to be the set of all these quotients:

$$C = \left\{\frac{x}{y}\ :\ x, y \in \mathcal{O}_F,\ 0 < |x| \leq h,\ 0 < |y| \leq \frac{M_d\sqrt{Nv}}{h},\ \text{ for some } h \in I\right\}.$$

Let us observe that from $0 < |x| \leq h < \frac{1}{\sqrt{2}}\sqrt{Nv}$ it follows that $0 < Nx = |x|^2 < Nv$, i.e., $v(x) = 0$, and similarly $v(y) = 0$.

Lemma 5. *If* $a, b \in C$ *and* $\beta(a) = \beta(b)$, *then* $a \in b\,U_1$.

Proof. Let $a = \frac{x_a}{y_a}$, $b = \frac{x_b}{y_b}$ where $x_a, y_a, x_b, y_b \in \mathcal{O}_F$, and $0 < |x_a| \leq h$, $0 < |y_a| \leq h'$, $0 < |x_b| \leq h_1$, $0 < |y_b| \leq h_1{}'$ for some $h, h', h_1, h_1{}' \in I$ satisfying $hh' = h_1h_1{}' = M_d\sqrt{Nv}$.

From $\beta(a) = \beta(b)$ we get $\beta(x_ay_b) = \beta(x_by_a)$.

Moreover

$$|x_ay_b| + |x_by_a| \leq hh_1{}' + h'h_1 < \frac{1}{2}Nv + \frac{1}{2}Nv = Nv.$$

Therefore from Lemma 4 we get $x_ay_b \in x_by_aU_1$, i.e., $a \in b\,U_1$. □

Lemma 6. $1 \in C \cap \ker\beta \subset U_1$.

Proof. From $1 < \sqrt{2}M_d$, it follows that $1 \in C$.

Let $c \in C \cap \ker\beta$. Then $\beta(c) = \beta(1)$, and from Lemma 5 we get $c \in U_1$. □

Lemma 7. *If*

$$\sqrt{Nv} > \max(2M_d, \sqrt{2q_F}M_d + \frac{1}{\sqrt{2}}), \tag{3}$$

then $W \subset CU_1$.

Proof. From (3) it follows that

$$\sqrt{Nv} > q\sqrt{2q_F}\,M_d + \frac{1}{q\sqrt{2}}, \tag{4}$$

for every $q > 1$ sufficiently near to 1.

Take $h = \frac{1}{q\sqrt{2}}\sqrt{Nv}$, $h' = q\sqrt{2}M_d$, then $h, h' \in I$, provided $q > 1$ is sufficiently near to 1.

For $w \in W$ we choose $c = \frac{x}{y} \in C$ such that $\beta(w) = \beta(c)$ and $x, y \in \mathcal{O}_F$ satisfy $0 < |x| \leq h$, $0 < |y| \leq h'$.

Since $q_F \leq \sqrt{|d|/3}$, then $M_d = \frac{2}{\pi}\sqrt{|d|} \geq \frac{2\sqrt{3}}{\pi}q_F > q_F$. Consequently (3) implies that $\sqrt{Nv} > q_F$ and we can apply Lemma 3. Hence $|w|^2 = Nw \leq q_F Nv$. Moreover $\beta(wy) = \beta(x)$ and

$$|wy| + |x| \leq \sqrt{q_F Nv}h' + h = \sqrt{Nv}\,q\,\sqrt{2q_F}\,M_d + \frac{1}{q\sqrt{2}}\sqrt{Nv} < Nv$$

in view of (3). Therefore from Lemma 4 we get $wy \in xU_1$, i.e., $w \in cU_1$. □

Lemma 8. *$Cg \subset CU_1$, provided $g \in \mathcal{O}_F, v(g) = 0$ and $1 \leq |g| < \frac{Nv}{4M_d^2}$.*

Proof. If $|g| = 1$, then $g = \pm 1 \in C$, and the lemma holds. Therefore we can assume that $|g| > 1$.

For $a = \frac{x_a}{y_a} \in C$ take $b = \frac{x_b}{y_b} \in C$ such that $\beta(ga) = \beta(b)$, where $x_a, y_a, x_b, y_b \in \mathcal{O}_F$ and

$$0 < |x_a| \leq h,\ 0 < |y_a| \leq h',\ 0 < |x_b| \leq h_1,\ 0 < |y_b| \leq h_1{}',$$

where $h, h', h_1, h_1{}' \in I$, $hh' = h_1h_1{}' = M_d\sqrt{Nv}$.

If we choose different a', $b' \in C$ (corresponding to different values of h and h_1) such that $\beta(a') = \beta(a)$ and $\beta(b') = \beta(b)$ then in view of Lemma 5 we have $a' \in aU_1$ and $b' \in bU_1$. Therefore if $ag \in bU_1$, then also $a'g \in b'U_1$, i.e., the claim of the lemma does not depend on the values of h, h_1 chosen. Thus we can choose h, $h_1 \in I$ arbitrarily. Put $h = q\sqrt{2}M_d$, $h_1 = \frac{1}{q}\sqrt{|g|}h$, where $q > 1$ is sufficiently near to 1, to be fixed later. Then $h_1 = \sqrt{2|g|}M_d \in I$, since $1 < \sqrt{|g|} < \frac{\sqrt{Nv}}{2M_d}$ by the assumption of the lemma. We can prove similarly that $h \in I$.

We have $\beta(gx_ay_b) = \beta(x_by_a)$ and

$$|gx_ay_b| + |x_by_a| \leq |g|hh_1{}' + h'h_1 = \sqrt{|g|}M_d\sqrt{Nv}\left(q + \frac{1}{q}\right).$$

Since $2\sqrt{|g|} < \frac{\sqrt{Nv}}{M_d}$ by the assumption, then also

$$\left(q + \frac{1}{q}\right)\sqrt{|g|} < \frac{\sqrt{Nv}}{M_d}$$

holds, for every $q > 1$ sufficiently near to 1. Consequently we get $|gx_ay_b| + |x_by_a| < Nv$.

Therefore from Lemma 4 it follows that $gx_ay_b \in x_by_aU_1$, i.e., $ga \in bU_1$. □

3.4. **The set $G \subset \mathcal{O}_F$ such that $\beta(G)$ generates k^*.** Now we define the set G:

$$G = \left\{ x \in \mathcal{O}_F \, : \, 0 < |x_c| \le M_d^{\frac{1}{2}} Nv^{\frac{1}{4}} \right\}.$$

Lemma 9. *If $\sqrt{Nv} > M_d$, then $\beta(G)$ generates k^*.*

Proof. The numbers $h = h' = M_d^{\frac{1}{2}} Nv^{\frac{1}{4}}$ satisfy the assumptions of Theorem 2. Therefore for every $a \in k^*$ there exist $x, y \in \mathcal{O}_F$ such that $0 < |x|, \, |y| \le h$ and $\beta(a) = \frac{\beta(x)}{\beta(y)}$. It follows that $x, y \in G$ and hence $\beta(G)$ generates k^*. □

3.5. **Main result.**

Theorem 3. *If $Nv > 2^{8/3} M_d^{10/3}$ and $|d| \ge 15$, then ∂_v is an isomorphism.*

Proof. We have proved above (Lemmas 2, 6 and 7) that there exist sets C and W satisfying conditions (1) and (3) of Theorem 1, provided

$$\sqrt{Nv} > \max\left(2M_d, \sqrt{2q_F}\, M_d + \frac{1}{\sqrt{2}} \right).$$

Moreover $M_d > q_F$. From Lemmas 8 and 9 it follows that there exists a set G satisfying condition (2) of Theorem 1 if

$$M_d^{1/2} Nv^{1/4} < \frac{Nv}{4M_d^2}, \text{ i.e., if } \sqrt{Nv} > 2^{4/3} M_d^{5/3}.$$

Since

$$2^{4/3} M_d^{5/3} > \max\left(2M_d, \sqrt{2}\, M_d^{3/2} + \frac{1}{\sqrt{2}} \right)$$

for $M_d \ge M_{-15} = 2.4656\ldots$, the inequality $\sqrt{Nv} > 2^{4/3} M_d^{5/3}$ implies that there exist sets C, G, W satisfying the assumptions of Theorem 1. Therefore ∂_v is an isomorphism. □

In the table below, for every discriminant $d, -151 \le d \le -15$, we give the estimation of Nv from Theorem 3.

−15	−19	−20	−23	−24	−31	−35	−39	−40
128.57	190.66	207.68	262.15	281.42	431.13	527.78	632.10	659.34
−43	−47	−51	−52	−55	−56	−59	−67	
743.80	862.66	988.47	1020.98	1121.03	1155.20	1260.18	1557.65	
−68	−71	−79	−83	−84	−87	−88	−91	−95
1596.59	1715.71	2049.86	2225.75	2270.62	2407.38	2453.68	2594.67	2787.53
−103	−104	−107	−111	−115	−116	−119	−120	
3189.64	3241.42	3398.75	3613.14	3832.74	3888.45	4057.50	4114.48	
−123	−127	−131	−132	−136	−139	−143	−148	−151
4287.34	4522.23	4762.10	4822.84	5068.87	5256.60	5511.12	5836.01	6034.51

4. Applications

The bound for Nv given in Theorem 3 is small enough to use computers. For a given discriminant $d < 0$ every ∂_v is an isomorphism, with a finite number of exceptions. These exceptional v's should be considered separately.

We describe below the main steps of the computations, and we illustrate them in the example $d = -23$. We have used the package GP/PARI Calculator [BBCO]. Further examples are given in the Appendix.

For a fixed $d < 0$ it is possible in general to improve the constructions of sets C, G, W given above. It enables us to reduce the number of exceptional v's considerably. We discuss these improvements below.

4.1. **A better set G.** It is sufficient to consider valuations v of the field $\mathbb{Q}(\sqrt{d})$ such that Nv does not exceed the bound given in Theorem 3.

Assume that

$$\sqrt{Nv} > \max\left(2M_d, \sqrt{2q_F}\, M_d + \frac{1}{\sqrt{2}}\right). \tag{5}$$

Then the sets C and W defined above satisfy the assumptions of Theorem 1. We shall define a better set G, provided $Nv = p$ is a prime number.

Namely, let G be a set of generators of the group $(\mathbb{Z}/p)^*$ with the minimal value of $m(G) := \max_{g \in G} |g|$. It is an easy exercise in programming in GP to find this set G. The results are as follows.

Let $w(k)$, for $k = 3, 5, 7, 11$, be the set of all odd primes $p < 1010$ such that there exists a set G of generators of the group $(\mathbb{Z}/p)^*$ satisfying $m(G) = k$, and there does not exist a set of generators with a smaller value of $m(G)$.

Then we have the following table: $w(3) = \{17, 31, 41, 43, 89, 109, 113, 127, 137, 151, 157, 223, 229, 233, 251, 257, 277, 281, 283, 331, 353, 397, 401, 449, 521, 569, 571, 593, 617, 631, 641, 683, 691, 733, 739, 761, 809, 811, 857, 881, 911, 929, 953, 971, 977\}$

$w(5) = \{73, 97, 193, 307, 313, 337, 431, 433, 439, 457, 499, 577, 673, 727, 919, 937\}$
$w(7) = \{241, 409, 601, 643, 769, 997\}$
$w(11) = \{1009\}$,
and $w(2)$ contains all odd primes $p < 1010$ not appearing in the above sets. Therefore $p \in w(2)$ iff the group $(\mathbb{Z}/p)^*$ is generated by the set $G = \{-1, 2\}$.

Now, to apply Lemma 8, it is sufficient to verify if

$$m(G) < \frac{Nv}{4M_d^2} \tag{6}$$

holds. Then ∂_v is an isomorphism provided also (5) is satisfied.

For $d = -23$, we have $q_F = 2$ in view of Lemma 1. Moreover $M_{-23} = \frac{2}{\pi}\sqrt{23} = 3.053\ldots$; therefore, (5) takes the form $Nv > 6.8133\ldots$.

The bound in Theorem 3 is $Nv > 262$. Using the table above it is easy to verify that (6) holds for all noninert v satisfying $73 < p < 262$, where $Nv = p$. Therefore the corresponding ∂_v's are isomorphisms.

4.2. **The best set C.** If, for a noninert prime $p = Nv$, (6) does not hold, we consider the set W defined above, but we look for a better set C. Using a computer we can determine a set $C \subset U \cap \mathcal{O}_F$ of representatives of all nonzero residues modulo v such that $m(C) := \max_{c \in C} |c|$ takes the minimal value. The procedure is as follows. Let

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2}, & \text{if } d \text{ is odd,} \\ \frac{\sqrt{d}}{2}, & \text{if } d \text{ is even.} \end{cases}$$

We compute all values $|x + y\omega|$, where $x, y \in \mathbb{Z}$, $|x| \le m$, $|y| \le m$ for some m, and determine the corresponding residues

$$x + y\omega \pmod{v} \in \mathcal{O}_F/v \cong \mathbb{Z}/p.$$

If m is sufficiently large, we get all residues in this way.

Then, for every nonzero residue $r \pmod{p}$, we choose among the numbers $x+y\omega$ a number $x_r + y_r\omega \equiv r \pmod{p}$ with the smallest absolute value, say c_r.

If $c_r < p$, then evidently $x_r + y_r\omega \in U$, and we get in this way the best set C. Moreover $m(C) = \max_r c_r$.

Then using the table above we determine the least value $m(G)$ of a set G of generators of the group $(\mathcal{O}_F/v)^* \cong (\mathbb{Z}/p)^*$.

Denote $m(W) := \max_{w \in W} |w|$.

Now, from Lemma 4 it follows that if

$$m(W) + m(C) < Nv, \tag{7}$$

then assumption (1) of Theorem 1 holds, and if

$$(m(G) + 1)m(C) < Nv, \tag{8}$$

then assumption (2) of Theorem 1 holds.

Assumption (3) of Theorem 1 is satisfied, since $C \cap \ker\beta = \{1\}$, for the set C defined above.

Thus, if (7) and (8) hold, then ∂_v is an isomorphism.

For example, if $d = -23$, then $q_F = 2$. For all noninert primes p, $3 < p \leq 73$, the values of $m(C)$ have been determined by a computer, the values of $m(G)$ we get from the table above, and the values of $m(W)$ are estimated by $\sqrt{2Nv}$.

The results are as follows.

p	$m(G)$	$m(W) \leq$	$m(C)$
13	2	5.099	2.828
23	2	6.782	6.928
29	2	7.616	5.099
31	3	7.874	5.196
41	3	9.055	6.000
47	2	9.695	6.928
59	2	10.863	9.591
71	2	11.916	7.874
73	5	12.083	8.485

It is easy to see that in all cases the inequalities (7) and (8) are satisfied. Thus ∂_v is an isomorphism, for all v such that $p = Nv$, $3 < p \leq 73$.

4.3. **The inert primes.**

We shall consider the inert primes separately. In every case we construct the sets G and C with small values of $m(G)$ and $m(C)$. Then either inequalities (7) and (8) hold, or we should apply Lemma 4 directly to verify assumptions (1) and (2) of Theorem 1.

For $d = -23$, there are only three inert primes $p = 5, 7, 11$ satisfying the inequality $Nv = p^2 < 262$ of Theorem 3. In each case we give the sets G and C explicitly. Denote $\omega = \frac{1}{2}(1 + \sqrt{-23})$.

For $p = v = 5, 7$ and 11 in view of Lemma 3 we have

$$m(W) \leq \sqrt{q_F Nv} = \sqrt{2}p.$$

Put

$$C = \left\{ a + b\,\omega \ : \ a, b \in \mathbb{Z},\ |a| \leq \frac{p-1}{2},\ |b| \leq \frac{p-1}{2},\ (a,b) \neq (0,0) \right\}.$$

Evidently C represents all nonzero residues in $\mathcal{O}_F/v \cong \mathbb{F}_{p^2}$, Moreover, for $c = a + b\omega \in C$ we have

$$|c|^2 = N(c) = a^2 + ab + 6b^2 \leq \left(\frac{p-1}{2}\right)^2 \cdot 8 = 2(p-1)^2 < 2p^2.$$

Hence $m(C) \leq \sqrt{2}(p-1)$.

To prove that $C \subset U$, it is sufficient to verify that for every $c = a + b\omega \in C$ all prime divisors of $N(c) = a^2 + ab + 6b^2$ are less than $Nv = p^2$. Since $N(c) < 2p^2$, it is sufficient to prove that $N(c)$ is not a prime number greater than p^2.

Suppose that $q = a^2 + ab + 6b^2$ is a prime number $> p^2$. Then a is odd, b is even and $3 \nmid a(a+b)$, $ab \neq 0$, and e.g., $b > 0$. Moreover, $\max(|a|, |b|) \leq \frac{p-1}{2}$.

For $p = 5$ and $p = 7$ the only pair (a, b) satisfying the above conditions is $(-1, 2)$, then $q = 23 < p^2$.

For $p = 11$ we have to consider the pairs $(a, b) = (1, 4), (-5, 4), (5, 2), (-1, 2)$. The corresponding values of q are $101, 101, 59, 23$, and they are less than $p^2 = 121$.

Thus in all cases we get a contradiction, hence $C \subset U$.

Of course, we can also verify that $C \subset U$ using a computer.

Since $Nv = p^2$, it is evident that the inequality (7) is satisfied.

Now we look for a set $G \subset \mathcal{O}_F$ such that $\beta(G)$ generates $\mathbb{F}_{p^2}^*$ and $m(G)$ is small.

For every p in question we define the set G separately.

If $p = 5$, take $G = \{\omega - 2\}$.
Here $\operatorname{ord}(\omega - 2) = 24$ in $\mathbb{F}_{25}^*$ and $|\omega - 2| = \sqrt{10}$, hence $m(G) = \sqrt{10}$.

If $p = 7$, take $G = \{2, \omega\}$.
Here $\operatorname{ord}(2) = 3$ and $\operatorname{ord}(\beta(\omega)) = 16$ in $\mathbb{F}_{49}^*$, and $|2| = 2$, $|\omega| = \sqrt{6}$, hence $m(G) = \sqrt{6}$.

If $p = 11$, take $G = \{\omega + 1\}$.
Here $\operatorname{ord}(\beta(\omega + 1)) = 120$ in $\mathbb{F}_{121}^*$, and $|\omega + 1| = \sqrt{8}$, hence $m(G) = \sqrt{8}$.

It is easy to verify that in all these cases inequality (8) holds, and hence ∂_v is an isomorphism for $v = 5, 7$ and 11.

4.4. **Small primes.** Thus there remained four prime ideals $\mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3, \mathfrak{p}_3'$ corresponding to the splitting primes 2 and 3.

We shall prove that also for $v = \mathfrak{p}_3'$ the mapping ∂_v is an isomorphism.

We can take $W = \{-1, 1 + \omega, 2, \omega\}$, since $(1 + \omega) = \mathfrak{p}_2^3$, $(2) = \mathfrak{p}_2\mathfrak{p}_2'$, $(\omega) = \mathfrak{p}_2'\mathfrak{p}_3$, and $\mathfrak{p}_2'^3 = (2^3 \cdot (1 + \omega)^{-1})$.

Put $G = \{-1\}$ and $C = \{1, -1\}$. Since $(1 - \omega) = \mathfrak{p}_2\mathfrak{p}_3'$ we can take $\pi = 1 - \omega$. Then the following elements belong to U_1 : 1, $1 + \frac{4}{1+\omega}\pi = -1 - \omega$, $1 + (-\frac{\omega}{2})\pi = -2$, $1 - \pi = \omega$. Consequently $W \subset CU_1$. Moreover $CG = C \subset CU_1$.

Therefore from Theorem 1 it follows that ∂_v is an isomorphism for $v = \mathfrak{p}_3'$.

4.5. **The generators of $K_2\mathcal{O}_F$.** Thus we have proved that, for $d = -23$, the group $K_2\mathcal{O}_F$ is contained in the group $\langle\langle W \rangle\rangle$ generated by symbols $\{a, b\}$, where $a, b \in W = \{-1, 1 + \omega, 2, \omega\}$. It is known (see [BS]) that a Sylow 2-subgroup of $K_2\mathcal{O}_F$ has order 2 and is generated by $\{-1, -1\}$. Hence $K_2\mathcal{O}_F \cong \mathbb{Z}/2 \oplus 2K_2\mathcal{O}_F$. We shall prove that the group $2K_2\mathcal{O}_F$ of odd order is trivial.

It is sufficient to prove that $4\langle\langle W \rangle\rangle = 1$, since $2K_2\mathcal{O}_F = 4K_2\mathcal{O}_F \subset 4\langle\langle W \rangle\rangle$.

The group $4\langle\langle W \rangle\rangle$ is generated by elements $\{a, b\}^4$, where $a, b \in W$. Since $\{a, a\}^2 = \{-1, a\}^2 = 1$, for every $a \in W$, and $\{\omega, 1 + \omega\}^2 = \{-\omega, 1 + \omega\}^2 = 1$, there remain two generators, $\{\omega, 2\}^4$ and $\{1 + \omega, 2\}^4$. We look for relations which they satisfy.

From the equality

$$1-\frac{\omega}{2}=\frac{4}{1+\omega}$$

we get

$$1=\left\{\frac{\omega}{2},1-\frac{\omega}{2}\right\}^2=\left\{\frac{\omega}{2},\frac{4}{1+\omega}\right\}^2=\{\omega,2\}^4\cdot\{1+\omega,2\}^{-2},$$

i.e., $\{\omega,2\}^4=\{1+\omega,2\}^2$.

From the equalities

$$1-\frac{3}{\omega}=\frac{1+\omega}{2}\quad\text{and}\quad-\left(2-\frac{3}{\omega}\right)=\left(1-\frac{3}{\omega}\right)\cdot\frac{\omega^2}{4}$$

we get

$$\begin{aligned}1&=\left\{2-\frac{3}{\omega},-\left(1-\frac{3}{\omega}\right)\right\}^2=\left\{\left(1-\frac{3}{\omega}\right)\cdot\frac{\omega^2}{4},-\left(1-\frac{3}{\omega}\right)\right\}^2=\left\{\frac{\omega^2}{4},\frac{1+\omega}{2}\right\}^2\\&=\{\omega,2\}^{-4}\{1+\omega,2\}^4=\{\omega,2\}^4.\end{aligned}$$

Hence $\{1+\omega,2\}^2=1$.

4.6. **The group $K_2\mathcal{O}_F$ for $d=-31$.** Let us remark that for larger values of $|d|$ the last step of the proof cannot be performed so automatically. We should look for relations between a finite number of symbols. If we know some nontrivial elements of $K_2\mathcal{O}_F$ (like $\{-1,-1\}$ for $d=-23$) and we can show that all other symbols in question are trivial or are equal to known elements, then the determination of $K_2\mathcal{O}_F$ is complete. Nevertheless, it may happen that we cannot prove the triviality of some symbols (and we suspect that they in fact are nontrivial!), but the reason may be that we did not use a sufficient number of relations between symbols. There is an example of this kind given by K. Belabas and H. Gangl: For $d=-303$ we expect that the symbol $\{2,37-3\sqrt{-303}\}$ has order 11 in $K_2\mathcal{O}_F$, but we cannot prove that it is nontrivial.

As a curiosity, we give below the last step of the proof that for $d=-31$ the group $K_2\mathcal{O}_F$ has order 2 (and is generated by $\{-1,-1\}$).

Suppose that we have proved that ∂_v is an isomorphism, if $Nv \gtrless 7$ (see the Appendix).

Let $F=\mathbb{Q}(\sqrt{-31})$, $\omega=\frac{1+\sqrt{-31}}{2}$ and let $v=3, Nv=9$. Then we can take

$$W=\{-1,\ \omega,\ 2,\ 1+\omega,\ 1+\bar{\omega},\ 2+\omega,\ 2+\bar{\omega}\},$$

and the group $\langle W\rangle$ generated by W is equal to U.

Let $\langle\langle W\rangle\rangle$ be the subgroup of K_2F generated by symbols $\{a\,,\,b\}$, where $a,b\in W$. Thus $K_2\mathcal{O}_F\subset\langle\langle W\rangle\rangle$.

It is known that a Sylow 2-subgroup of $K_2\mathcal{O}_F$ has order 2 and is generated by $\{-1,-1\}$, and a Sylow 3-subgroup of $K_2\mathcal{O}_F$ is trivial (see e.g., [BG]). Hence $K_2\mathcal{O}_F=\mathbb{Z}/2\oplus 2K_2\mathcal{O}_F$, and the order of $2K_2\mathcal{O}_F$ is prime to 6.

We shall prove that the group $2K_2\mathcal{O}_F$ is trivial.

Denote by X the subgroup of $\langle\langle W\rangle\rangle$ generated by its Sylow p-subgroups, where $p=2$ and 3.

We shall use below the following easy observations:

(i) *If $x \in \langle\langle W\rangle\rangle$ satisfies $x^2 \in X$ or $x^3 \in X$, then $x \in X$.*

(ii) *If $a, b, c \in \langle W\rangle$ satisfy $a+b=c$ and $\{b\,,\,c\} \in X$, then*

$$\{a\,,\,b\} \equiv \{a\,,\,c\} \pmod X.$$

In fact, from $\frac{a}{c}+\frac{b}{c}=1$ we get

$$1=\left\{\frac{a}{c}\,,\,\frac{b}{c}\right\}=\{a\,,\,b\}\{a\,,\,c\}^{-1}\{b\,,\,c\}\{c\,,\,c\}\equiv\{a\,,\,b\}\{a\,,\,c\}^{-1}\pmod X.$$

From $\omega\bar{\omega}=8$ it follows that $\bar{\omega}\in\langle W\rangle$. Consequently the groups $\langle W\rangle$, $\langle\langle W\rangle\rangle$ and X are closed under complex conjugation.

Lemma 10. $\langle\langle W\rangle\rangle = X$.

Proof. We shall prove that

1. $\{\omega\,,\,\bar{\omega}\}\,,\ \{\omega\,,\,2\}\in X$.

2. $\{1+\omega\,,\,\omega\}\,,\ \{1+\omega\,,\,\bar{\omega}\}\,,\ \{1+\omega\,,\,2\}\in X$.

3. $\{3\,,\,\omega\}\,,\ \{3\,,\,1+\omega\}\,,\ \{1+\omega\,,\,1+\bar{\omega}\}\in X$.

4. $\{2+\omega\,,\,a\}\in X$ for $a=2,\ \omega,\ \bar{\omega},\ 1+\omega,\ 1+\bar{\omega},\ 3,\ 2+\bar{\omega}$.

Then from the above remark the lemma follows.

All congruences below are modulo X.

Proof of **1**. From $\omega+\bar{\omega}=1$ and $\omega\bar{\omega}=8$ it follows that $\{\omega\,,\,\bar{\omega}\}=1$ and

$$\{\omega\,,\,2\}^3=\{\omega\,,\,\omega\bar{\omega}\}\equiv\{\omega\,,\,\bar{\omega}\}=1\pmod X,$$

since $\{\omega\,,\,\omega\}\in X$. Hence $\{\omega\,,\,2\}\in X$ by (i).

Proof of **2**. From $(1+\omega)-\omega=1$, and $(1+\omega)+\bar{\omega}=2$ in view of Step **1.** and (ii) we get

$$\{1+\omega\,,\,\omega\}\equiv 1\pmod X,$$
$$\{1+\omega\,,\,\bar{\omega}\}\equiv\{1+\omega\,,\,2\}\pmod X.$$

Hence

$$\{1+\omega\,,\,\bar{\omega}\}^3\equiv\{1+\omega\,,\,2\}^3=\{1+\omega\,,\,\omega\bar{\omega}\}=\{1+\omega\,,\,\bar{\omega}\}.$$

Consequently

$$\{1+\omega\,,\,\bar{\omega}\}\in X\quad\text{and}\quad\{1+\omega\,,\,2\}\in X.$$

Proof of **3**. The equalities

$$\begin{aligned}&1)\ \ 9-\omega\bar{\omega}=1,\\&2)\ \ 9+\omega^2=1+\omega,\\&3)\ \ 6+2\bar{\omega}=-\omega(1+\omega),\end{aligned}$$

in view of (ii) imply, respectively,

$$\begin{aligned}&1)\quad \{3\,,\,\omega\}\{3\,,\,\bar{\omega}\}\in X,\\&2)\quad \{3\,,\,\omega\}^4\equiv\{3\,,\,1+\omega\}^2\pmod X,\\&3)\quad \{6\,,\,2\bar{\omega}\}\equiv\{6\,,\,\omega(1+\omega)\}\pmod X,\end{aligned}$$

and hence in view of Steps **1.** and **2.**

$$3')\quad\{3\,,\,\bar{\omega}\}\equiv\{3\,,\,\omega(1+\omega)\}\,.$$

Consequently by 2), 3′) and 1) we get

$$\{3\,,\,\omega\}^4 \equiv \{3\,,\,1+\omega\}^2 \equiv \{3\,,\,\bar{\omega}\}^2\,\{3\,,\,\omega\}^{-2} \equiv \{3\,,\,\omega\}^{-4},$$

i.e., $\{3\,,\,\omega\}^8 \in X$ and hence $\{3\,,\,\omega\} \in X$. Then $\{3\,,\,1+\omega\} \in X$ by 2).

Finally, from the equality

$$4)\quad (1+\omega)+(1+\bar{\omega}) = 3,$$

applying (ii) and complex conjugation we get $\{1+\omega\,,\,1+\bar{\omega}\} \equiv \{1+\bar{\omega}\,,\,3\} \in X$.

Proof of **4**. From the equalities

$$\begin{array}{ll} 1) & (2+\omega)-(1+\omega) = 1,\\ 2) & (2+\omega)-\omega = 2,\\ 3) & (2+\omega)+\bar{\omega} = 3,\\ 4) & (2+\omega)+(1+\bar{\omega}) = 4, \end{array}$$

we get

$$\begin{array}{lll} 1) & \{2+\omega\,,\,1+\omega\} & \equiv 1,\\ 2) & \{2+\omega\,,\,\omega\} & \equiv \{2+\omega\,,\,2\},\\ 3) & \{2+\omega\,,\,\bar{\omega}\} & \equiv \{2+\omega\,,\,3\},\\ 4) & \{2+\omega\,,\,1+\bar{\omega}\} & \equiv \{2+\omega\,,\,2\}^2. \end{array}$$

Now we apply the equalities

$$5)\qquad 3+\omega = \frac{(1+\bar{\omega})\bar{\omega}}{-2} \quad \text{and} \quad (3+\omega)-(2+\omega) = 1.$$

Hence

$$\begin{aligned} 1 &\equiv \{2+\omega\,,\,3+\omega\} \equiv \{2+\omega\,,\,1+\bar{\omega}\}\,\{2+\omega\,,\,\bar{\omega}\}\,\{2+\omega\,,\,2\}^{-1}\\ &\equiv \left\{2+\omega\,,\,2^2\cdot 3\cdot 2^{-1}\right\} \equiv \{2+\omega\,,\,\omega\bar{\omega}\} = \{2+\omega\,,\,2\}^3, \end{aligned}$$

and consequently $\{2+\omega\,,\,2\} \in X$.

From 1) − 5) we get that all symbols in question but the last belong to X. Finally, from

$$6)\qquad \bar{\omega}(2+\omega)+\omega(2+\bar{\omega}) = 2\cdot 9$$

we get $\{\bar{\omega}(2+\omega)\,,\,\omega(2+\bar{\omega})\} \equiv \{\bar{\omega}(2+\omega)\,,\,2\cdot 9\} \in X$, i.e., $\{2+\omega\,,\,2+\bar{\omega}\} \in X$. □

Lemma 11. *The group $K_2\mathcal{O}_F$ has order* 2 *and is generated by* $\{-1,-1\}$.

Proof. From the above it follows that $K_2\mathcal{O}_F \subset \langle\langle W\rangle\rangle = X$, i.e., no prime greater than 3 divides $\#K_2\mathcal{O}_F$. The Sylow p-subgroups of $K_2\mathcal{O}_F$, for $p=2$ and $p=3$ are known (see e.g., [BG]). □

Let us remark that in the proof of Lemma 10 we have also used symbols $\{a\,,\,b\}$, where a did not belong to $\langle W\rangle = U$, e.g., $\{3\,,\,\omega\}$ with $3 \notin U$. Our attempts to eliminate such external symbols from the proof was without success.

APPENDIX: DETERMINING $K_2O_{\mathbb{Q}(\sqrt{d})}$ FOR $0 > d \geq -151$

1. Using the constructions given in this paper (see Theorem 3 and subsections 4.1–4.3), we can first determine the bad primes and subsequently, using additional considerations, reduce the number of primes which can possibly contribute to the generation of the tame kernel. This has been performed successfully for the discriminants $d \geq -151$ and the results are displayed in Table 1: the first column gives $-d$, the second one shows a bound on the norm of the prime ideals involved which is deduced directly using the techniques described in the above. As an example, we give the full set of norms of "bad primes" for $d = -107$:

$$[3, 4, 11, 13, 19, 23, 25, 29, 37, 41, 47, 49, 53, 83, 193, 241, 643, 1801].$$

2. The third column of the table displays a bound which was obtained after subsequent improvements of the algorithm, still using Tate's criterion, by constructing suitable sets C for each bad prime separately. For details, we refer to our paper in preparation [KH].

3. The program not only finds (small) bounds for the primes v for which the map ∂_v is possibly not an isomorphism, it actually produces generators for the corresponding K-group and relations coming from trivial symbols $\{z, 1-z\}$ where both z and $1-z$ involve only primes below some bound (essentially the one given in the third column). In order to (considerably) simplify the program, the results are determined only up to 2-torsion. (This is not a serious restriction in view of the work of Browkin and Schinzel [BS] who have determined the maximal elementary Abelian 2-subgroup ${}_2K_2\mathcal{O}_F$ of $K_2\mathcal{O}_F$ for quadratic F, and in particular the generators of this subgroup.) Again, details are given in [KH]. The generators are stated in the fourth column of the table, where x is put in place of $\sqrt{-d}$. If the group $K_2\mathcal{O}_F/{}_2K_2\mathcal{O}_F$ is trivial, the corresponding slot is left empty.

4. Finally, the fifth column gives (in the nontrivial case) the order of the generators modulo ${}_2K_2\mathcal{O}_F$, for which we have a priori only obtained an upper bound in the process. On the other hand, lower bounds for the q-part of $K_2\mathcal{O}_F$ for $q = 2, 3, 4$ have been established by Browkin, Schinzel, Qin and others, and the two bounds coincide in almost all cases. The only lower bound which seems not yet covered in the published literature is the 8-rank for $d = -68$, but see [Q3], Theorem 4.1. All the results agree with the conjectural ones in [BG]. They are reproduced here in the last column.

5. Summarizing, the computer program (written in GP-PARI) covers many more cases than have been known so far, although the complexity of the computations tends to increase rapidly with the size of the discriminant. Moreover, for larger discriminants, one can at least conjecturally give generators and their orders (cf. [KH]).

TABLE 1. The group $K_2\mathcal{O}_F$

$-d$	bound for bad primes	refined bound	generator mod ${}_2K_2\mathcal{O}_F$	order mod ${}_2K_2\mathcal{O}_F$	$K_2\mathcal{O}_F$
31	31	5			2
39	41	3	$\{2, x+5\}$	3	(2,3)
40	41	11			1
43	97	17			1
47	25	3			2
51	49	11			2
52	47	11			1
55	17	7			2
56	23	3			2
59	17	3			1
67	193	23			1
68	25	3	$\{2, x+2\}$	4	8
71	73	3			2
79	241	5			2
83	41	7			1
84	37	7	$\{2, x-6\}$	3	(2,3)
87	241	7			2
88	307	23			1
91	241	7	$\{3, x+3\}$	3	2
95	97	3			2
103	409	13			2
104	121	5			1
107	1801	11	$\{2, x-1\}$	3	3
111	307	5	$\{-\frac{3}{2}x+\frac{5}{2}, -\frac{1}{2}x-\frac{9}{2}\}$	3	(2,3)
115	1129	23	$\{2, x-5\}$	2	2
116	289	5			1
119	241	5			(2,2)
120	1801	13	$\{2, x-12\}$	3	(2,3)
123	1009	17			2
127	127	13			2
131	409	3			1
132	433	17	$\{2, x+6\}$	2	4
136	431	19	$\{2, x+8\}$	2	4
139	409	11			1
143	409	3	$\{2, 3x-53\}$	2	2
148	2689	43			1
151	1009	5			2

ACKNOWLEDGMENTS

I express my gratitude to the I.C.T.P. in Trieste for the invitation and hospitality during my stay there, when the present paper was written. I also thank H. Gangl and K. Belabas for their cooperation, and the anonymous referee for many valuable suggestions to the earlier version of the paper.

REFERENCES

[A1] S. Arno, *The imaginary quadratic fields of class number* 4, Acta Arith. **60** (1992), 321–334. MR **93b:**11144

[A2] S. Arno, M.L. Robinson, F.S. Wheeler, *The imaginary quadratic fields with small odd class number*, Acta Arith. **83** (1998), 295–330. MR **99a:**11123

[BBCO] C. Batut, D. Bernardi, H. Cohen, M. Olivier, *GP/PARI Calculator*, version 1.39.

[KH] K. Belabas, H. Gangl, *Generators and relations for $K_2\mathcal{O}_F$, F imaginary quadratic*, in preparation.

[BG] J. Browkin, H. Gangl, *Tame and wild kernels of quadratic imaginary number fields*, Math. Comp. **68** (1999) 291–305. MR **99c:**11144

[BS] J. Browkin, A. Schinzel, *On Sylow* 2*-subgroups of $K_2\mathcal{O}_F$ for quadratic number fields F*, J. Reine Angew. Math. **331** (1982), 104–113. MR **83g:**12011

[C] Harvey Cohn, *Advanced Number Theory*, Dover Publications, New York, 1962. MR **82b:**12001

[Q1] H. Qin, *Computation of* $K_2\mathbb{Z}[\sqrt{-6}]$, J. Pure Appl. Algebra **96** (1994), 133–146. MR **95i:**11135

[Q2] ———, *Computation of* $K_2\mathbb{Z}[\frac{1+\sqrt{-35}}{2}]$, Chin. Ann. Math. **17B** (1) (1996), 63–72. MR **97a:**19004

[Q3] ———, *Tame kernels and Tate kernels of quadratic number fields*, preprint, 1998.

[S] M. Skałba, *Generalization of Thue's theorem and computation of the group $K_2\mathcal{O}_F$*, J. Number Theory **46** (1994), 303–322. MR **95d:**19001

[T] J. Tate, *Appendix*, Lecture Notes in Math., Vol. 342, Springer Verlag, New York/Berlin, 1973, pp. 429–446. MR **48:**3656b

[W] C. Wagner, *Class number* 5, 6 *and* 7, Math. Comp. **65** (1996), 785–800. MR **96g:**11135

INSTITUTE OF MATHEMATICS, UNIVERSITY OF WARSAW, UL. BANACHA 2, PL-02-097 WARSAW, POLAND

E-mail address: bro@mimuw.edu.pl

DEPT. DE MATHÉMATIQUES, BÂT. 425, UNIVERSITÉ PARIS-SUD, F-91405 ORSAY, FRANCE

E-mail address: Karim.Belabas@math.u-psud.fr

MAX-PLANCK INSTITUT FÜR MATHEMATIK, VIVATSGASSE 7, D-53111, BONN, GERMANY

E-mail address: herbert@mpim-bonn.mpg.de