SEPARABLE FREE QUADRATIC ALGEBRAS OVER QUADRATIC INTEGERS

J. Browkin, J. Brzeziński

Abstract. The aim of the paper is to determine all free separable quadratic algebras over the rings of integers of quadratic fields in terms of the properties of the fundamental unit in the real case. The paper corrects some earlier published results on the subject.

1. INTRODUCTION

Let K be a real quadratic field extension of the rational numbers and let R denote the integers in K. In [T], Thérond gives a description of all separable quadratic extensions $S \supset R$ such that S is free as an R-module. His result is reproduced in [H] (see pp.40 – 41). According to [T], the number of such extensions depends on the residue modulo 4 of the discriminant d of K and on the residues modulo 4 of $u, v \in \mathbb{Z}$, where $\varepsilon = \frac{u}{2} + \frac{v}{2}\sqrt{d}$ is the fundamental unit of K. Unfortunately, when $d = 21$ or 29, the residues of d modulo 4 are the same, and the fundamental units are $\varepsilon = \frac{5+\sqrt{d}}{2}$, so they can not be differentiated in the given way. However, for $d = 21$ there is a separable free quadratic extension of R, while for $d = 29$ such an extension of the corresponding ring R does not exist (see Theorem 8).

The aim of the present paper is to give a correct version of the result and to determine all free separable quadratic algebras over the rings of integers of quadratic number fields. All separable quadratic algebras over the integers of quadratic fields were studied in many papers (see e.g. [He], [GL] and [SW]), in particular, because of their relevance to Gauss theory of genera of integral binary quadratic forms. This relation was pointed out by Hasse (see [Ha]). The contents of the paper is the following. In Section 2, we recall necessary notions concerning separable algebras. In Section 3, we discuss the notion of quadratic defect, which we use in the proofs in Section 4. Using this notion, we get easy alternative proofs of the results in [T] and the new results concerning the most involved case when the discriminant of the real quadratic field is congruent to 1 modulo 4. An interesting point is a relation between the existence of free unramified extensions over the real quadratic integers and the norm of the fundamental unit, which is a theme of several results of the present paper.

1991 *Mathematics Subject Classification.* [2000] Primary 11R11, Secondary 11R04, 11R27, 11S15.

Key words and phrases. Quadratic separable algebra, quadratic defect, fundamental unit.

Typeset by $\mathcal{AMS}$-TEX

2. SEPARABLE QUADRATIC ALGEBRAS

Let now R denote the ring of integers in a global or a local field K and S an R-algebra finitely generated and projective as an R-module. Recall that S is called separable (or étale) over R if for every maximal ideal $\mathfrak{m}$ in R, the algebra $S/\mathfrak{m}$ is separable over the field $R/\mathfrak{m}$ (for a thorough treatment of separability see [KO], Chap. III). It is clear that S is separable over R if and only if for each maximal ideal $\mathfrak{m}$ in R, the completion $S_{\mathfrak{m}}$ is separable over the completion $R_{\mathfrak{m}}$ with respect to the $\mathfrak{m}$-adic topology. If $L = K \otimes_R S$ is a field, then S is separable over R if and only if L is an unramified extension of K (at all finite primes of K).

Assume now that S is a quadratic separable R-algebra, that is, the rank of S as a projective R-module equals 2. Then $L = K \otimes_R S$ is either a quadratic unramified field extension of K or $L \cong K \times K$. In the last case, $S \cong R \times R$, since S is the maximal commutative R-order in L (see [KO], Chap. III, §4). In both cases, S is the integral closure of R in L, that is, the ring of all elements of L integral over R.

Let now $S = R + Re$ be a free quadratic R-algebra. This means that $e^2 = pe + q$, for suitable $p, q \in R$, so that $S = R[X]/(X^2 - pX - q)$. For more details concerning (free) quadratic algebras see [H], Chap.1–3. Let $\Delta(S/R) = p^2 + 4q$ be the discriminant of S with respect to R.

Theorem 1. *$S = R + Re$, where $e^2 = pe + q$, $p, q \in R$ is separable over R if and only if $\Delta(S/R) \in R^*$, where R^* denotes the group of units in R. Moreover, two free quadratic algebras $S = R + Re$ and $S' = R + Re'$ are R-isomorphic if and only if their discriminants differ by a square of a unit in R, that is, $\Delta(S'/R) = \eta^2 \Delta(S/R)$, where $\eta \in R^*$.*

Proof. See [H], (2.2), p.23, for the first part, and (1.3), p.7 for the second one. □

This result shows that all R-isomorphism classes of the free separable quadratic algebras S over R are classified by those units $\varepsilon \in R^*$, which can be represented in the form $\varepsilon = p^2 + 4q$, where $p, q \in R$, modulo squares of the units in R. It is clear that the product of two units of this form (two discriminants of free separable quadratic algebras) is again such a discriminant.

Definition. By the group of separable free quadratic R-algebras, we mean the group of all units in R of the form $p^2 + 4q$, where $p, q \in R$, modulo the squares of the units. Following [H], p.31, we denote this group by $\mathrm{Qu_f}(R)$.

Remark 1. The group $\mathrm{Qu_f}(R)$ may be defined in a more natural way. If S and S' are separable quadratic R-algebras, then they have canonical non-trivial R-involutions σ and σ'. The fixed subring for the natural action of the tensor product $\sigma \otimes \sigma'$ on the R-algebra $S \otimes_R S'$ gives the (isomorphism class of) separable quadratic R-algebra, which corresponds to $\Delta(S/R)\Delta(S'/R)$ if the two algebras S and S' are free. See [H], p.174. □

In Section 4, we compute the group $\mathrm{Qu_f}(R)$ for the rings of integers in quadratic number fields, but in order to limit the computations, we discuss shortly a very useful notion of the quadratic defect.

3. QUADRATIC DEFECTS

In this section, we refer to [O'M], §63A. If $x \in K$ and K is a discrete local field with the ring of integers R, then the quadratic defect of x is the intersection of all the ideals bR, where $x = a^2 + b$ for elements $a \in K$. We denote the quadratic defect of x by $\mathfrak{d}(x)$ and note that x is a square in K if and only if its quadratic defect is (0). If π is any generator of the maximal ideal $\mathfrak{m}$ in R and the quadratic defect of a non-square x is $\mathfrak{m}^r$, then we shall also say that x has quadratic defect π^r. Similarly, we say that squares in K have quadratic defect 0.

We note some important facts concerning the quadratic defect, which are proved in [O'M]. If 2 is a unit in R (non-dyadic case), then the quadratic defects of the units in R are (0) (squares) or R (non-squares). If 2 is not a unit in R (dyadic case) and $(2) = (\pi^t)$, then (see [O'M], 63:2) the quadratic defects of the units in R are the ideals in the chain:

$$(0) \subset (\pi^{2t}) \subset (\pi^{2t-1}) \subset (\pi^{2t-3}) \subset \cdots \subset (\pi^3) \subset (\pi).$$

We shall repeatedly use the following result (see [O'M], 63:5 and 63:3):

Theorem 2. *Let K be a discrete local field with the integers R whose maximal ideal $\mathfrak{m}$ has a generator π. Then:*
(a) If $\varepsilon = \eta^2 + \pi^r\delta$, where $\eta, \delta \in R^*$ and $1 \leq r \leq 2t-1$ is odd, then $\mathfrak{d}(\varepsilon) = \pi^r R$. In any of these cases, $K[\sqrt{\varepsilon}] = K(\sqrt{\varepsilon})$ is a ramified field extension of K, that is, the integral closure S of R in this field is not separable over R.
(b) If $\varepsilon = \eta^2 + 4\alpha$, where $\eta \in R^*, \alpha \in R$, then $\mathfrak{d}(\varepsilon) = 4R$ when α is a unit and (0) when α is not a unit. Moreover, in the first case $K[\sqrt{\varepsilon}] = K(\sqrt{\varepsilon})$ is an unramified field extension of K, and in the second one, $K[\sqrt{\varepsilon}] = K \times K$, so in both cases the integral closure S of R in $K[\sqrt{\varepsilon}]$ is a quadratic (free) separable R-algebra.

4. QUADRATIC INTEGERS

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field over the rationals $\mathbb{Q}$, where d is a square free integer. As before, we denote by R the ring of integers in K. If $\mathfrak{p}$ is a non-zero prime ideal in R, we denote by $|x|_{\mathfrak{p}}$ or simply by $|x|$, when there is no danger of confusion, the value of $x \in K_{\mathfrak{p}}$ with respect to the (normalized) valuation corresponding to $\mathfrak{p}$.

Very often we shall use the following easy observation: Let $L = K[\sqrt{\eta}]$, where η is any unit in R. Then for all prime ideals $\mathfrak{p}$ in R not containing 2 (non-dyadic fields $K_{\mathfrak{p}}$), $L_{\mathfrak{p}} = K_{\mathfrak{p}}[\sqrt{\eta}]$ is an unramified field extension of $K_{\mathfrak{p}}$ or $L_{\mathfrak{p}} = K_{\mathfrak{p}} \times K_{\mathfrak{p}}$. This means that in order to check whether the integers S in L form a separable quadratic R-algebra, it is sufficient to check this property locally for the dyadic completions of K. The proofs of Theorems 3 – 5 and a part of Theorem 6 below can be found in [T] (see also [H], pp.39–40). For completeness, we give proofs using a method based on the notion of quadratic defect.

Theorem 3. *Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a square-free integer and let R denote the integers in K. Then $-1 \in \mathrm{Qu_f}(R)$ if and only if $d \equiv 3 \pmod 4$.*

Proof. We have to decide when $L = K(\sqrt{-1})$ is an unramified extension of K. Let $d \equiv 3 \pmod 4$, and let $\mathfrak{p}$ be the prime ideal containing 2. We have $-1 =$

$(\sqrt{d})^2 - 4\frac{d+1}{4}$, which shows that the quadratic defect $\mathfrak{d}_{\mathfrak{p}}(-1) = (0)$ or $4R_{\mathfrak{p}}$. Thus L is unramified over K.

If $d \equiv 1 \pmod 4$, then the equality $-1 = 1 - 2$ shows that $\mathfrak{d}_{\mathfrak{p}}(-1) = \mathfrak{p}R_{\mathfrak{p}}$, where $\mathfrak{p}$ is any prime ideal containing 2 (see Theorem 2 (a)). In fact, the ideal (2) in R is either inert or splits into product of two different ideals, so $|2|_{\mathfrak{p}} = 1$. Hence L is ramified over K.

If $d \equiv 2 \pmod 4$, then the the equality

$$-1 = (1 + \sqrt{d})^2 - [2\sqrt{d} + (d + 2)]$$

shows that $\mathfrak{d}_{\mathfrak{p}}(-1) = \mathfrak{p}^3 R_{\mathfrak{p}}$, where $\mathfrak{p}$ is the only prime ideal in R containing 2. In fact, $|2\sqrt{d} + d + 2|_{\mathfrak{p}} = 3$, since $|2\sqrt{d}|_{\mathfrak{p}} = 3$ and $|d + 2|_{\mathfrak{p}} \geq 4$. Thus L is ramified over K. □

The description of the group $\mathrm{Qu_f}(R)$ for non-real quadratic number fields is very easy. If $d < 0$ and $d \neq -1, -3$ then the group $\mathrm{Qu_f}(R)$ may contain at most two elements represented by ± 1, and according to Theorem 1, it has 2 elements if and only if $d \equiv 3 \pmod 4$. Since for $d = -3 \equiv 1 \pmod 4$, $R^*/R^{*2} = \{1, -1\}$, so the group $\mathrm{Qu_f}(R)$ is trivial in this case. If $d = -1$, then $R^*/R^{*2} = \{1, i\}$ and $i = 1^2 + (i - 1)$, which says that the quadratic defect $\mathfrak{d}_{\mathfrak{p}}(i) = \mathfrak{p}$, where $\mathfrak{p} = (1 - i)$. Hence $\mathrm{Qu_f}(R)$ is also trivial when $d = -1$. Thus we have:

Theorem 4. *Let $d < 0$ be a square-free integer and let R be the ring of integers in $\mathbb{Q}(\sqrt{d})$. Then*

$$\mathrm{Qu_f}(R) = \begin{cases} \mathbb{Z}/2 = \langle\, -1 \,\rangle & \text{if } d \equiv 3 \pmod 4, d \neq -1, \\ 1 & \text{otherwise.} \end{cases}$$

□

Assume now that $d > 0$ and let ε denote the fundamental unit in K. The group $\mathrm{Qu_f}(R)$ may contain at most four elements represented by $\pm 1, \pm\varepsilon$. For simplicity, we consider these numbers as the possible elements of $\mathrm{Qu_f}(R)$. We shall study this group in three cases depending on the residue of d modulo 4 beginning with $d \equiv 3 \pmod 4$, then $d \equiv 2 \pmod 4$ and finally, $d \equiv 1 \pmod 4$, which was the starting motivation for this paper.

Theorem 5. *Let $K = \mathbb{Q}(\sqrt{d})$, where $d \equiv 3 \pmod 4$ and let $\varepsilon = u + v\sqrt{d}$ be the fundamental unit in R. Then $\mathrm{Nr}(\varepsilon) = 1$ and*

$$\mathrm{Qu_f}(R) = \begin{cases} \mathbb{Z}/2 \times \mathbb{Z}/2 = \langle\, -1 \,\rangle \times \langle\, \varepsilon \,\rangle & \text{if } 2 \mid v, \\ \mathbb{Z}/2 = \langle\, -1 \,\rangle & \text{if } 2 \nmid v. \end{cases}$$

Proof. Since $\mathrm{Nr}(\varepsilon) = u^2 - dv^2 = \pm 1$, u and v have different parities. Considering u odd and v even or vice versa, we get $\pm 1 = u^2 - dv^2 \equiv 1 \pmod 4$, so $u^2 - dv^2 = 1$.

Let $\mathfrak{p} = (2, \sqrt{d} + 1)$ be the prime ideal in R containing 2. As we already know, $-1 \in \mathrm{Qu_f}(R)$. If $2 \nmid v$, then $u^2 - dv^2 = 1$, says that u must be even. Hence $\varepsilon = 1 + (u - v - 1) + v(\sqrt{d} + 1)$ gives $|u - v - 1|_{\mathfrak{p}} \geq 2$ and $|v(\sqrt{d} + 1)|_{\mathfrak{p}} = 1$, so

$|u-v-1+v(\sqrt{d}+1)|_{\mathfrak{p}}=1$, that is, $\mathfrak{d}_{\mathfrak{p}}(\varepsilon)=\mathfrak{p}$. Thus $\varepsilon\notin \mathrm{Qu}_{\mathrm{f}}(R)$. Since -1 is in this group, $-\varepsilon$ can not be its element either.

If $2\mid v$, then u must be odd, so $u^2\equiv 1 \pmod 8$. Hence $u^2=dv^2+1$, implies that $4\mid v$. If now $u\equiv 1 \pmod 4$, then $\varepsilon=1+(u-1)+v\sqrt{d}$ gives $\mathfrak{d}_{\mathfrak{p}}(\varepsilon)=4R_{\mathfrak{p}}$ or (0). If $u\equiv -1 \pmod 4$, then $\varepsilon=(2+\sqrt{d})^2+(u-d-4)+v\sqrt{d}$ and again $\mathfrak{d}_{\mathfrak{p}}(\varepsilon)=4R_{\mathfrak{p}}$ or (0). Thus $\varepsilon\in \mathrm{Qu}_{\mathrm{f}}(R)$. Also $-\varepsilon\in \mathrm{Qu}_{\mathrm{f}}(R)$, since -1 belongs to this group. □

Remark 2. Notice that according to the proof above, $2\mid v$ implies $4\mid v$.

Theorem 6. *Let $K=\mathbb{Q}(\sqrt{d})$, where $d\equiv 2 \pmod 4$ and let $\varepsilon=u+v\sqrt{d}$ be the fundamental unit in R. Then*

$$\mathrm{Qu}_{\mathrm{f}}(R)=\begin{cases}\mathbb{Z}/2 & \textit{if } \mathrm{Nr}(\varepsilon)=1,\\ 1 & \textit{if } \mathrm{Nr}(\varepsilon)=-1.\end{cases}$$

Moreover, $\mathrm{Nr}(\varepsilon)=1$ *iff* $2|v$, *and in this case either ε or $-\varepsilon$ is in* $\mathrm{Qu}_{\mathrm{f}}(R)$. *More precisely,* $\varepsilon\in\mathrm{Qu}_{\mathrm{f}}(R)$ *iff* $(u,v)\equiv(1,0),(3,2) \pmod 4$ *and* $-\varepsilon\in\mathrm{Qu}_{\mathrm{f}}(R)$ *iff* $(u,v)\equiv (1,2),(3,0) \pmod 4$.

Proof. According to Theorem 3, $-1\notin \mathrm{Qu}_{\mathrm{f}}(R)$, so this group may consist of one or two elements. Since $u^2-dv^2=\pm 1$, u is odd. We have $(2)=\mathfrak{p}^2$, where $\mathfrak{p}=(2,\sqrt{d})$.

If $2\nmid v$, then the equality $\varepsilon=1+[(u-1)+v\sqrt{d}]$ says that the quadratic defect $\mathfrak{d}_{\mathfrak{p}}(\varepsilon)=\mathfrak{p}$, since $|u-1|_{\mathfrak{p}}\geq 2$ and $|v\sqrt{d}|_{\mathfrak{p}}=1$. Thus the extension $K_{\mathfrak{p}}(\sqrt{\varepsilon})$ of $K_{\mathfrak{p}}$ is ramified and the group $\mathrm{Qu}_{\mathrm{f}}(R)$ is trivial.

Assume now that $2\mid v$. We consider four cases corresponding to $u\equiv\pm1 \pmod 4$ and $v\equiv 0,2 \pmod 4$.

If $u\equiv 1 \pmod 4$ and $4|v$, then $\varepsilon=1+(u-1)+v\sqrt{d}$ gives $|u-1+v\sqrt{d}|_{\mathfrak{p}}\geq 4$, so the quadratic defect $\mathfrak{d}_{\mathfrak{p}}(\varepsilon)=4R_{\mathfrak{p}}$ or (0), while $u\equiv 1 \pmod 4$, $v\equiv 2 \pmod 4$ and $-\varepsilon=(1+\sqrt{d})^2-(d+u+1)-(v+2)\sqrt{d}$ show that $\mathfrak{d}_{\mathfrak{p}}(-\varepsilon)=4R_{\mathfrak{p}}$ or (0).

If $u\equiv -1 \pmod 4$ and $4\mid v$, then $-\varepsilon=1-(u+1)-v\sqrt{d}$ gives $\mathfrak{d}_{\mathfrak{p}}(-\varepsilon)=4R_{\mathfrak{p}}$ or (0), while $u\equiv -1 \pmod 4$, $v\equiv 2 \pmod 4$ and the equality $\varepsilon=(1+\sqrt{d})^2+u-1-d+(v-2)\sqrt{d}$ show that $\mathfrak{d}_{\mathfrak{p}}(\varepsilon)=4R_{\mathfrak{p}}$ or (0).

Finally notice that considering the equality $u^2-dv^2=\pm1$ modulo 4 shows that if $2\mid v$, then $u^2-dv^2=1$, while $2\nmid v$ implies $u^2-dv^2=-1$. □

Assume now that $d\equiv 1 \pmod 4$ and let $\varepsilon=u+v\frac{1+\sqrt{d}}{2}$ be the fundamental unit in $K=\mathbb{Q}(\sqrt{d})$ with the ring of integers R.

Theorem 7. *Let $K=\mathbb{Q}(\sqrt{d})$, where $d\equiv 1 \pmod 4$ and let ε be the fundamental unit in R. Then*

$$\mathrm{Qu}_{\mathrm{f}}(R)=\begin{cases}\mathbb{Z}/2 & \textit{if } \mathrm{Nr}(\varepsilon)=1,\\ 1 & \textit{if } \mathrm{Nr}(\varepsilon)=-1.\end{cases}$$

Moreover, in the first case either ε or $-\varepsilon$ is in $\mathrm{Qu}_{\mathrm{f}}(R)$.

Proof. By the definition of $\mathrm{Qu}_{\mathrm{f}}(R)$, ε or $-\varepsilon$ belongs to this group if and only if $\varepsilon\equiv\pm p^2 \pmod{4R}$, where $p\in R$. Let $H=\{\pm p^2 : p\in (R/4R)^*\}$. We consider two cases.

Case 1: $d \equiv 5 \pmod 8$. Then 2 is inert in K, and the residue field $R/2R$ is $\mathbb{F}_4$. Therefore every element of $(R/4R)^*$ can be written in the form $\alpha_0 + \alpha_1 \cdot 2 \pmod 4$, where $\alpha_0, \alpha_1 \in R$ represent elements of $\mathbb{F}_4^*$ and $\mathbb{F}_4$, respectively. Hence $\#(R/4R)^* = 12$. Consequently

$$(R/4R)^* = \langle -1 \rangle \times \langle \sqrt{d} \rangle \times \langle \xi \rangle,$$

where ξ is an element of order 3. Here we used the fact that $(\sqrt{d} \pmod 4)^2 = d \pmod 4 = 1$, and $\sqrt{d} \not\equiv \pm 1 \pmod 4$. It follows that $H = \langle -1, \xi \rangle$ is a subgroup of index 2. Representatives of the cosets modulo H are 1 and $\sqrt{d}$.

If $\varepsilon \in H$, then $\varepsilon \equiv \pm p^2 \pmod 4$, $p \in R$. Consequently $\sigma(\varepsilon) \equiv \pm\sigma(p)^2 \pmod 4$, where σ is the nontrivial automorphism of K. Then

$$\mathrm{Nr}(\varepsilon) = \varepsilon \cdot \sigma(\varepsilon) \equiv (\pm p^2)(\pm\sigma(p)^2) = \mathrm{Nr}(p)^2 \equiv 1 \pmod 4,$$

since $\mathrm{Nr}(p)$ is an odd integer. From $\mathrm{Nr}(\varepsilon) = \pm 1$ and the above congruence, it follows that $\mathrm{Nr}(\varepsilon) = 1$.

If $\varepsilon \in \sqrt{d}\,H$, then proceeding similarly as above we get $\varepsilon \equiv \pm p^2\sqrt{d} \pmod 4$, $\sigma(\varepsilon) \equiv \pm\sigma(a)^2 \cdot \sigma(\sqrt{d}) = \pm\sigma(p)^2 \cdot (-\sqrt{d}) \pmod 4$. Hence

$$\mathrm{Nr}(\varepsilon) = \varepsilon \cdot \sigma(\varepsilon) \equiv -\mathrm{Nr}(p)^2 \cdot d \equiv -1 \pmod 4,$$

which implies $\mathrm{Nr}(\varepsilon) = -1$.

Case 2: $d \equiv 1 \pmod 8$. Then 2 splits in K, $(2) = \mathfrak{p}_1\mathfrak{p}_2$. Consequently

$$R/4R = R/\mathfrak{p}_1^2\mathfrak{p}_2^2 = R/\mathfrak{p}_1^2 \times R/\mathfrak{p}_2^2 = \mathbb{Z}/4 \times \mathbb{Z}/4.$$

The group of units of this ring

$$(\mathbb{Z}/4)^* \times (\mathbb{Z}/4)^* = \mathbb{Z}/2 \times \mathbb{Z}/2$$

is generated by -1 and $\sqrt{d}$, by an argument similar to the above. Consequently, $H = \langle -1 \rangle$, and cosets modulo H are represented by 1 and $\sqrt{d}$. The same argument as in the previous case leads to the same result. □

Now we can characterize the non-triviality of $\mathrm{Qu_f}(R)$ when $d \equiv 1 \pmod 4$ in terms of the fundamental unit in R:

Theorem 8. *Let $d \equiv 1 \pmod 4$ and let $\varepsilon = u + v\omega$, where $\omega = \frac{1+\sqrt{d}}{2}$, be the fundamental unit in R. Assume that $\mathrm{Qu_f}(R) \neq 1$.*
(a) If v is even, then

$$\mathrm{Qu_f}(R) = \langle \varepsilon \rangle \quad \textit{iff} \quad (u,v) \equiv (1,0) \pmod 4,$$

$$\mathrm{Qu_f}(R) = \langle -\varepsilon \rangle \quad \textit{iff} \quad (u,v) \equiv (-1,0) \pmod 4.$$

(b) If v is odd, then

$$\begin{aligned}\mathrm{Qu_f}(R) = \langle \varepsilon \rangle \quad & \textit{iff} \quad d \equiv 5 \pmod{16},\ (u,v) \equiv (1,1) \textit{ or } (2,3) \pmod 4,\\ & \textit{or} \quad d \equiv 13 \pmod{16},\ (u,v) \equiv (0,3) \textit{ or } (3,1) \pmod 4.\end{aligned}$$

$$\begin{aligned}\mathrm{Qu_f}(R) = \langle -\varepsilon \rangle \quad & \textit{iff} \quad d \equiv 5 \pmod{16},\ (u,v) \equiv (3,3) \ \textit{or}\ (2,1) \pmod 4, \\ & \textit{or} \quad d \equiv 13 \pmod{16},\ (u,v) \equiv (0,1) \ \textit{or}\ (1,3) \pmod 4.\end{aligned}$$

Proof. By the assumption $\mathrm{Qu_f}(R) \neq 1$, from Theorem 7 it follows that

$$\mathrm{Nr}(\varepsilon) = u^2 + uv + \frac{1-d}{4}v^2 = 1. \tag{1}$$

(a) If $2 \mid v$, this equality is possible only if u is odd. Hence $u^2 \equiv 1 \pmod 4$, so $4 \mid v$, since otherwise, $uv \equiv 2 \pmod 4$ and we get a contradiction.

If now $u \equiv 1 \pmod 4$, then $\varepsilon = 1 + (u-1) + v\omega$ implies that the quadratic defect $\mathfrak{d}_\mathfrak{p}(\varepsilon)$ at any $\mathfrak{p}$ containing 2 is equal to $4R_\mathfrak{p}$ or (0).

If $u \equiv -1 \pmod 4$, then by the above $-\varepsilon$ represents the non-trivial element of $\mathrm{Qu_f}(R)$.

(b) Assume now that v is odd. Since (1) is equivalent to $(2u+v)^2 - dv^2 = 4$ and $(2u+v)^2 \equiv v^2 \equiv 1 \pmod 8$, we get $1 - d \equiv 4 \pmod 8$, that is, $d \equiv 5 \pmod 8$.

We have two cases.

If $d \equiv 5 \pmod{16}$, then the equality (1) modulo 4 is equivalent to $u^2+uv-v^2 = 1$. We have $\omega^2 \equiv \omega + 1 \pmod 4$. If now $v \equiv 1 \pmod 4$, then we easily get $u \equiv 1$ or $2 \pmod 4$. Similarly $v \equiv 3 \pmod 4$, gives $u \equiv 2$ or $3 \pmod 4$. Notice now that if $(u,v) \equiv (1,1) \pmod 4$, then

$$\varepsilon = u + v\omega \equiv 1 + \omega \equiv \omega^2 \pmod 4,$$

so the quadratic defect $\mathfrak{d}_\mathfrak{p}(\varepsilon) = 4R_\mathfrak{p}$ or (0) for the only dyadic prime ideal $\mathfrak{p} = (2)$ in R. Similarly, $(u,v) \equiv (2,3) \pmod 4$, gives

$$\varepsilon = u + v\omega \equiv 2 + 3\omega \equiv (\omega+1)^2 \pmod 4,$$

with the same result as regards $\mathfrak{d}_\mathfrak{p}(\varepsilon)$. Observe now that the remaining pairs $(3,3)$ and $(2,1)$ give the quadratic defect $\mathfrak{d}_\mathfrak{p}(-\varepsilon) = 4R_\mathfrak{p}$ or (0).

If $d \equiv 13 \pmod{16}$, then the equality (1) modulo 4 is equivalent to $u^2+uv+v^2 = 1$. We have $\omega^2 \equiv \omega + 3 \pmod 4$. This time $v \equiv 1 \pmod 4$, implies $u \equiv 0$ or $3 \pmod 4$, and $v \equiv 3 \pmod 4$, gives $u \equiv 0$ or $1 \pmod 4$. Notice now that if $(u,v) \equiv (0,3) \pmod 4$, then

$$\varepsilon = u + v\omega \equiv 3\omega \equiv (\omega+1)^2 \pmod 4,$$

while $(u,v) \equiv (3,1) \pmod 4$, gives

$$\varepsilon = u + v\omega \equiv 3 + \omega \equiv \omega^2 \pmod 4.$$

In both cases, the quadratic defect $\mathfrak{d}_\mathfrak{p}(\varepsilon) = 4R_\mathfrak{p}$ or (0) for both prime ideals $\mathfrak{p}$ in R containing 2. Finally observe that the remaining pairs $(0,1)$ and $(1,3)$ give the quadratic defect $\mathfrak{d}_\mathfrak{p}(-\varepsilon) = 4R_\mathfrak{p}$ or (0). □

The table below shows that all the possibilities for $(u, v) \pmod 4$ mentioned in Theorem 8 (b) really occur.

TABLE

d	$d \pmod{16}$	$u \pmod 4$	$v \pmod 4$	ε
21	5	2	1	$2+\omega$
69	5	3	3	$11+3\omega$
357	5	1	1	$9+\omega$
805	5	2	3	$698+51\omega$
77	13	0	1	$4+\omega$
93	13	1	3	$13+3\omega$
205	13	0	3	$20+3\omega$
221	13	3	1	$7+\omega$

Taking into account Theorems 5, 6, 7, we get the following result:

Corollary 1. *Let $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is squarefree. Then there exists an unramified quadratic extension of K, whose ring of integers is a free module over the integers of K if and only if the fundamental unit in K has norm 1.*

An interesting consequence of Theorems 6 and 7 is a relation between the norm of the unit and its residue in the finite group $(R/4R)^*$.

Corollary 2. *Let ε be any unit in $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is squarefree and $d \not\equiv 3 \pmod 4$. Then $\mathrm{Nr}(\varepsilon) = 1$ if and only if $\varepsilon \in H = \{\pm p^2 : p \in (R/4R)^*\}$.*

Proof. It follows directly from Theorems 6 and 7 noting that in the actual cases, $\mathrm{Nr}(\varepsilon) = 1$ if and only if the group $\mathrm{Qu_f}(R)$ is non-trivial and contains either ε or $-\varepsilon$, which is equivalent to $\varepsilon \in H$. Since these statements were proved by different methods for $d \equiv 1 \pmod 4$ (in Theorem 7) and $d \equiv 2 \pmod 4$ (in Theorem 6), we present also a proof in the second case, which is parallel to the argument given in the first case, since the result seems to be interesting on its own rights.

Let $d \equiv 2 \pmod 4$. Then $1, \sqrt{d}$ is the integral basis of R and 2 ramifies in this ring, so

$$(R/4R)^* = \{a + b\sqrt{d} \pmod 4 \ : \ a = \pm 1,\ b = 0, \pm 1, 2\}$$

$$= \{\pm 1,\ \pm 1 \pm \sqrt{d}, \pm 1 + 2\sqrt{d} \pmod 4\}.$$

Moreover $1 + \sqrt{d} \pmod 4$ has order 4. Consequently

$$(R/4R)^* = \mathbb{Z}/2 \times \mathbb{Z}/4 = \langle -1 \rangle \times \langle 1 + \sqrt{d} \rangle.$$

Therefore $H = \langle -1, (1+\sqrt{d})^2 \rangle = \langle -1, 1+2\sqrt{d} \rangle$, and representatives of cosets modulo H are 1 and $1+\sqrt{d}$.

If $\varepsilon \in H$, then $\varepsilon \equiv \pm p^2 \pmod 4$, $\sigma(\varepsilon) \equiv \pm\sigma(p)^2 \pmod 4$. Hence $\mathrm{Nr}(\varepsilon) \equiv \mathrm{Nr}(p)^2 \equiv 1 \pmod 4$, so $\mathrm{Nr}(\varepsilon) = 1$.

If $\varepsilon \in (1+\sqrt{d})\, H$, we proceed analogously to the above taking into account that $\mathrm{Nr}(1+\sqrt{d}) = 1-d \equiv -1 \pmod 4$, and get $\mathrm{Nr}(\varepsilon) \equiv \mathrm{Nr}(p)^2\, \mathrm{Nr}(1+\sqrt{d}) \equiv -1 \pmod 4$, hence $\mathrm{Nr}(\varepsilon) = -1$. □

Along the same lines one can prove

Corollary 3. *Let ε be any unit in $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is squarefree. Then $Nr(\varepsilon) = 1$ if and only if $\varepsilon \in \{\pm p^2 : p \in (R/3R)^*\}$.*

□

Remark 3. Let us observe that in the case $d \equiv 3 \pmod 4$, we have

$$(R/4R)^* = \{\pm 1, \pm\sqrt{d}, \pm 1 + 2\sqrt{d}, 2 \pm \sqrt{d} \pmod 4\},$$

and $(\sqrt{d})^2 = d \equiv -1 \pmod 4$. Hence $\sqrt{d} \pmod 4$ has order 4 and -1 is a square. Consequently

$$(R/4R)^* = \mathbb{Z}/4 \times \mathbb{Z}/2 = \langle \sqrt{d} \rangle \times \langle 1+2\sqrt{d} \rangle,$$

and $H = \langle -1 \rangle$. Therefore there are four cosets modulo H, and in general $\varepsilon \pmod 4$ does not belong to H. E.g. for $d = 7$, and $\varepsilon = 8+3\sqrt{7} \equiv -\sqrt{7} \pmod 4$, we have $\varepsilon \pmod 4 \notin H$. □

Finally note that each quadratic unramified extension L of $K = \mathbb{Q}(\sqrt{d})$ (if such exists) must be biquadratic over the rational numbers according to the well-known result of Hasse about the genus fields of the quadratic number fields (see [Ha] and compare [He], Theorem 1, p.VII-6 and [SW]). In fact, in our case, let $\varepsilon = u + v\omega$, where $\omega = \sqrt{d}$ if $d \equiv 2$ or $3 \pmod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ be a unit with $\mathrm{Nr}(\varepsilon) = 1$ such that $L = K(\sqrt{\varepsilon})$. Then $L = \mathbb{Q}\left(\sqrt{d}, \sqrt{\frac{u-1}{2}}\right) = \mathbb{Q}\left(\sqrt{d}, \sqrt{\frac{u+1}{2}}\right)$, when $d \equiv 2$ or $3 \pmod 4$, while $L = \mathbb{Q}\left(\sqrt{d}, \sqrt{\frac{2u+v-2}{2}}\right) = \mathbb{Q}\left(\sqrt{d}, \sqrt{\frac{2u+v+2}{2}}\right)$, when $d \equiv 1 \pmod 4$. These equalities follow easily from the identity:

$$\sqrt{a+\sqrt{b}} = \sqrt{\frac{a+c}{2}} + \sqrt{\frac{a-c}{2}},$$

where $a^2 - b = c^2$ (here $c = 1$, $a = u$ when $d \equiv 2$ or $3 \pmod 4$ and $a = (2u+v)/2$ when $d \equiv 1 \pmod 4$).

Acknowledgments

The second author expresses his gratitude for the invitation and hospitality to the organizers of the Workshop in Warsaw on the occasion of 60-th birthday of Professor H.C. Williams. The idea of the present paper emerged in discussions during this workshop.

References

[GL] S.K. Gogia, I.S. Luthar, *Quadratic unramified extensions of* $\mathbb{Q}(\sqrt{d})$, J. reine angew. Math. **298** (1978), 108–111.

[H] A.J. Hahn, *Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups*, Universitext, Springer-Verlag, 1994.

[Ha] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, Journal of the Math. Soc. of Japan **3** (1951), 45–51.

[He] C.S. Herz, *Construction of class fields, in Seminar on Complex Multiplication*, Lecture Notes in Mathematics vol. 21, Springer-Verlag, 1966.

[KO] M.–A. Knus, M. Ojanguren, *Théorie de la Descente et Algébres d'Azumaya*, Lecture Notes in Mathematics vol. 389, Springer-Verlag, 1974.

[O'M] O.T. O'Meara, *Introduction to Quadratic Forms*, Die Grundlehren der mathematischen Wissenschaften 117, Springer-Verlag, 1973.

[SW] B.K. Spearman, K.S. Williams, *Unramified quadratic extensions of a quadratic field*, Rocky Mountain Math. Journ. **25** (1995), 783–788.

[T] J.–D. Thérond, *Le groupe des extensions quadratiques séparables libres de l'anneau des entiers de* $\mathbb{Q}(\sqrt{d})$, C.R. Acad. Sc. Paris **281A** (1975), 939–942.

Institute of Mathematics, University of Warsaw,
ul. Banacha 2, PL–02–097 Warsaw, Poland
E-mail address: bro@mimuw.edu.pl

Department of Mathematics, Chalmers University of Technology
and Goteborg University, S–41296 Goteborg, Sweden
E-mail address: jub@math.chalmers.se