Canad. J. Math. Vol. **61** (5), 2009 pp. 1073–1091

# On the 2-Rank of the Hilbert Kernel of Number Fields

Ross Griffiths and Mikaël Lescop

*Abstract.* Let $E/F$ be a quadratic extension of number fields. In this paper, we show that the genus formula for Hilbert kernels, proved by M. Kolster and A. Movahhedi, gives the 2-rank of the Hilbert kernel of $E$ provided that the 2-primary Hilbert kernel of $F$ is trivial. However, since the original genus formula is not explicit enough in a very particular case, we first develop a refinement of this formula in order to employ it in the calculation of the 2-rank of $E$ whenever $F$ is totally real with trivial 2-primary Hilbert kernel. Finally, we apply our results to quadratic, bi-quadratic, and tri-quadratic fields which include a complete 2-rank formula for the family of fields $\mathbb{Q}(\sqrt{2}, \sqrt{\delta})$ where $\delta$ is a squarefree integer.

## Introduction

Let $F$ be a number field with ring of integers $o_F$. Let $F_v$ denote the local field at a finite or real infinite prime $v$. For $K$ a number field or a local field, let $\mu(K)$ be the group of roots of unity of $K$ and, for a finite group $A$, denote by $|A|$ its cardinality, by $A(2)$ its 2-primary part, and by $\operatorname{rk}_2(A)$ its 2-rank. Furthermore, let $K_2$ be the functor of Milnor [Mi]. In other words

$$K_2(F) = F^* \underset{\mathbb{Z}}{\otimes} F^* / \langle x \otimes (1-x); x \neq 0, 1 \rangle,$$

and denote by $\{a, b\}_F$ the class of the element $a \otimes b$ in $K_2(F)$.

To begin with, let us recall briefly the definition of the $m$-th Hilbert symbol on a local field $K$ containing the group $\mu_m$ of $m$-th roots of unity (for more details, see [N]). If $L$ is a finite extension of $K$, then there is an isomorphism

$$r_{L/K} \colon \operatorname{Gal}(L/K)^{ab} \xrightarrow{\sim} K^* / \mathrm{N}_{L/K} L^*$$

given by the reciprocity map of local class field theory. Here $\mathrm{N}_{L/K}$ is the norm map of $L/K$ and $\operatorname{Gal}(L/K)^{ab}$ denotes the maximal abelian factor group of the Galois group of $L/K$, *i.e.,* $\operatorname{Gal}(L/K)$ divided by its commutator subgroup. By inverting $r_{L/K}$, we obtain the local norm residue symbol $(\,\cdot\,, L/K) \colon K^* \to \operatorname{Gal}(L/K)^{ab}$ with kernel $\mathrm{N}_{L/K} L^*$.

For an element $b \in K^*$, the field $K_b := K(\sqrt[m]{b})$ is a Kummer extension (hence abelian) and so $(a, K_b/K) \in \operatorname{Gal}(K_b/K)$ for $a \in K^*$. The $m$-th Hilbert symbol $(a, b)_{K,m}$ is defined to be the $m$-th root of unity satisfying

$$(a, K_b/K)(\sqrt[m]{b}) = (a, b)_{K,m} \sqrt[m]{b}.$$

Received by the editors March 7, 2006.
AMS subject classification: Primary: 11R70; secondary: 19F15.

(Note that this definition is independent of the choice of $\sqrt[m]{b}$.)

Let $\varphi = (\varphi_v)$ denote the homomorphism $K_2(F) \to \bigoplus_v \mu(F_v)$, given by the $|\mu(F_v)|$-th Hilbert symbol at all finite or real infinite primes $v$.

Let $\psi\colon \bigoplus_v \mu(F_v) \to \mu(F)$ be defined by $\psi(\{\zeta_v\}) = \prod_v \zeta_v^{\frac{|\mu(F_v)|}{|\mu(F)|}}$. By definition the Hilbert kernel or wild kernel $WK_2(F)$ of $F$ is the kernel of $\varphi$, and by Moore's reciprocity law [CW] we obtain an exact sequence

$$0 \longrightarrow WK_2(F) \longrightarrow K_2(F) \xrightarrow{\varphi} \bigoplus_v \mu(F_v) \xrightarrow{\psi} \mu(F) \longrightarrow 0,$$

where $v$ runs through all the finite and real infinite primes of $F$.

We also have the tame symbol $\langle a, b\rangle_v$ determined for $a, b \in F^*$ and $v$ a prime of $F$ as the unique element in the multiplicative group of the residue field $k_v$ which modulo the maximal ideal is congruent to

$$(-1)^{\mathrm{ord}_v(a)\,\mathrm{ord}_v(b)} \frac{a^{\mathrm{ord}_v(b)}}{b^{\mathrm{ord}_v(a)}}.$$

For all finite primes $v$ of $F$, the tame symbols define a homomorphism $K_2(F) \to \bigoplus_v k_v^*$ whose kernel is actually the $K$-group $K_2(o_F)$. This kernel is also known as the tame kernel of $F$.

H. Garland proved [Ga] that the tame kernel $K_2(o_F)$ is a finite abelian group and thus the same is true of the Hilbert kernel as a subgroup. In this paper, we compute the 2-rank of the Hilbert kernel for certain number fields, generalizing the formula given by J. Browkin and A. Schinzel (see [BS, Theorem 2, p. 107; Theorem 4, p. 111]) for any quadratic field $\mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is a square-free integer. Note that J.-F. Jaulent and F. Soriano-Gafiuk [JSG] found another method to compute the 2-rank of the Hilbert kernel of quadratic fields, considering the so-called 2-group of positive logarithmic classes.

Here is the general plan of our paper. Let $E/F$ be a quadratic extension of number fields. Our work relies on a genus formula for Hilbert kernels given by [KM] and presented in Section 1.1. Recall that this genus formula for Hilbert kernels is the analogue of the well-known genus formula for ideal class groups proved by Chevalley. We show in Section 1.2 that the genus formula gives the 2-rank of the Hilbert kernel of $E$ provided that the 2-part of the Hilbert kernel of $F$ is trivial. Our first main result, where the formulas to compute the 2-rank are given, is Theorem 1.5. However, since the original genus formula of [KM] is not explicit enough in a very particular case, called case $(*)$ in the sequel, we prove in Section 1.3 a refinement of this formula in order to compute the 2-rank of $E$ in general when it is only assumed that $F$ is a totally real number field with trivial 2-primary Hilbert kernel. Note that this refinement is slightly different from the one proposed in [L2]. Finally Section 2 is devoted to applying our results to quadratic, bi-quadratic and tri-quadratic fields [Gr2].

## 1 Genus Formula and 2-Rank for Hilbert Kernels

In this section we deal with a quadratic extension $E/F$ of number fields with Galois group $G$. Let $F_\infty$ be the cyclotomic $\mathbb{Z}_2$-extension of $F$.

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

### 1.1 The Genus Formula for Hilbert Kernels

Let $N_{E/F}$ denote the norm map of the extension $E/F$ and denote by $D_F$ the Tate kernel of $F$: by definition, $D_F = \{x \in F^*/ \{-1,x\}_F = 1 \in K_2(F)\}$. Clearly $F^{*2} \subset D_F$, and we define $\widetilde{D}_F := D_F/F^{*2}$. We recall (see [T]) that $[D_F:(F^*)^2] = 2^{1+r_2}$ where $r_2$ is the number of pairs of complex embeddings of $F$, in such a way as to have $[F:\mathbb{Q}] = r_1 + 2r_2$ with $r_1$ real embeddings of $F$. Thus, when $F$ is totally real, the group $\widetilde{D}_F$ is cyclic of order 2 and in this case we define $\alpha_F \in D_F$ such that its class modulo $F^{*2}$ is a generator of $\widetilde{D}_F$. In this case, $\alpha_F$ has an explicit description.

***Lemma 1.1*** *Let $F$ be a totally real extension of $\mathbb{Q}$ and $\zeta_{2^n}$ be a primitive $2^n$-th root of unity. Define for $n \geqslant 2$: $\alpha_n = 2 + \zeta_{2^n} + \zeta_{2^n}^{-1}$. Let $n$ be maximal with $\alpha_n \in F$. Then we can take $\alpha_F = \alpha_n$.*

**Proof** First of all, note that $\alpha_n$ is not a square in $F^*$ since this would contradict the maximality of $n$. Indeed we have $\alpha_n = (\alpha_{n+1} - 2)^2$.

Let $L := F(\sqrt{-1}) = F(\zeta_{2^n})$. Then $\alpha_n = (1 + \zeta_{2^n})(1 + \zeta_{2^n}^{-1}) = N_{L/F}(1 + \zeta_{2^n})$. Thus, using the transfer map $\mathrm{Tr}_{L/F}\colon K_2(L) \to K_2(F)$, we get

$$\{-1, \alpha_n\}_F = \mathrm{Tr}_{L/F}\{-1, 1 + \zeta_{2^n}\}_L = 1.$$

The last statement follows from the fact that for $n \geqslant 2$,

$$\{-1, 1 + \zeta_{2^n}\}_L = \{(-\zeta_{2^n})^{2^{n-1}}, 1 + \zeta_{2^n}\}_L = \{-\zeta_{2^n}, 1 + \zeta_{2^n}\}_L^{2^{n-1}} = 1,$$

since $\{x, 1 - x\}_L$ is trivial in $K_2(L)$ for any $x \neq 1$ in $L^*$. Thus $\alpha_n \in D_F$ (and is a norm from $D_L$) and we get the result. ■

We have as a consequence of Lemma 1.1 that if $F$ is a totally real multi-quadratic extension of $\mathbb{Q}$, then $\alpha_F = 2$ if $\sqrt{2} \notin F$, and $\alpha_F = 2 + \sqrt{2}$ otherwise.

Let $T_{E/F}$ denote the set of primes of $F$ consisting of those which are tamely ramified in $E$ and dyadic primes $v$ of $F$, undecomposed in $E$, for which either $\mu(E_w)(2) = \mu(F_v)(2)$, or $E_w$ is not contained in the cyclotomic $\mathbb{Z}_2$-extension of $F_v$, where $w$ is the prime above $v$ in $E$. Actually, the set $T_{E/F}$ consists of all non-complex primes $v$ of $F$ for which the map $j_v\colon \mu(F_v)(2) \to (\bigoplus_{w|v} \mu(E_w)(2))^G$ is not an isomorphism (see [KM, p. 116]). Recall that $j_v$ is defined by $j_v(\zeta_{F_v}) = (N_{E_w/F_v}(\zeta_{E_w}))_{w|v}$ where $\zeta_{E_w}$ is a generator of $\mu(E_w)(2)$ and

$$\zeta_{F_v} := \zeta_{E_w}^{\frac{|\mu(E_w)(2)|}{|\mu(F_v)(2)|}}$$

is a generator of $\mu(F_v)(2)$.

We are now able to state the Genus Formula originally proved by M. Kolster and A. Movahhedi [KM, p. 123].

***Proposition 1.2* (Genus Formula)** *Let $E/F$ be a quadratic extension of number fields with Galois group $G$. Then*

(a) *If $E \subset F_\infty$ and if $|\mu(E)(2)| > |\mu(F)(2)|$, then $WK_2(E)(2)_G \cong WK_2(F)(2)$.*

(b) *If either a real infinite prime of $F$ ramifies in $E$, or $\mu(F_v)(2) = \mu(F)(2)$ for a certain prime $v \in T_{E/F}$, then*

$$\frac{|WK_2(E)(2)_G|}{|WK_2(F)(2)|} = \frac{2^{|T_{E/F}|-r_{E/F}-1}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]},$$

*where $r_{E/F}$ is a non-negative integer which equals 0 if $F$ is totally real.*

(c) *In all other cases,*

$$\frac{|WK_2(E)(2)_G|}{|WK_2(F)(2)|} = \frac{2^{|T_{E/F}|-\rho}}{[D_F : D_F \cap \mathrm{N}_{E/F}(E^*)]},$$

*with $\rho = 0$ or $\rho = 1$.*

The integer $\rho$, sometimes denoted $\rho_{E/F}$, is defined in the following way (see also [KM] and [L1]). Consider the following commutative diagram where the top two rows are exact:

$$\begin{array}{ccccccc}
0 \longrightarrow & WK_2(F)(2) & \longrightarrow & K_2(o_F^S)(2) & \longrightarrow & \bigoplus_{v\in S} \mu(F_v)(2)) \\
 & \downarrow i & & \downarrow & & \downarrow j_S \\
0 \longrightarrow & WK_2(E)(2)^G & \xrightarrow{\gamma} & K_2(o_E^S)(2)^G & \xrightarrow{\alpha} & \bigoplus_{v\in S} \Big(\bigoplus_{w|v} \mu(E_w)(2)\Big)^G \\
 & \downarrow & & \downarrow & & \downarrow \\
 & WK_2(E)(2)^G/\operatorname{im} i & \xrightarrow{\gamma'} & D_F/F^{*2}N_{E/F}(D_E) & \xrightarrow{\alpha'} & \bigoplus_{v\in T_{E/F}} D_{F_v}/F_v^{*2}N_{E_w/F_v}(D_{E_w}) \\
 & \downarrow & & \downarrow & & \downarrow \\
 & 0 & & 0 & & 0
\end{array}$$

Here $S$ is the set of all dyadic primes of $F$, of all finite primes of $F$ which ramify in $E$, and of all real infinite primes of $F$; moreover, $o_F^S$ denotes the ring of $S$-integers of $F$ and $o_E^S$ is the integral closure of $o_F^S$ in $E$. Define $\rho$ by $[\ker\alpha' : \operatorname{im}\gamma'] = 2^\rho$, so that $\rho$ is necessarily either 0 or 1. Note that in the case that $F$ is totally real we have

$$\ker\alpha' = D_F \cap N_{E/F}(E^*)/F^{*2}N_{E/F}(D_E)$$

as a consequence of [KM, Corollary 2.6]. As a result, when $F$ is totally real we have that $\rho = 0$ whenever $\alpha_F$ is not a norm or $E \subset F_\infty$ (in this case $\alpha_F \in N_{E/F}(D_E)$).

## 1.2 Computation of the 2-Rank of the Hilbert Kernel of Number Fields

***Proposition 1.3*** *Let $E/F$ be a quadratic extension of number fields with Galois group $G$, such that $WK_2(F)(2)$ is trivial. Then*

$$|WK_2(E)(2)_G| = 2^{\mathrm{rk}_2(WK_2(E))}.$$

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

**Proof** Since $G$ is cyclic we have $|WK_2(E)(2)_G| = |WK_2(E)(2)^G|$. The result then follows from the fact that the group $WK_2(E)(2)^G$ of $G$-invariants is exactly the group ${}_2WK_2(E)$ of elements of $WK_2(E)$ killed by 2. Indeed, considering the two natural maps $i\colon WK_2(F) \to WK_2(E)$ and the transfer $\mathrm{Tr}\colon WK_2(E) \to WK_2(F)$, we have the following two facts.

- On the one hand, if $y \in WK_2(E)(2)^G$ and $\sigma$ generates $G$, then

$$1 = i \circ \mathrm{Tr}(y) = \prod_{\varphi \in G} y^{\varphi} = yy^{\sigma} = y^2.$$

- On the other hand, if $y \in {}_2WK_2(E)$, then $y^2 = 1$. But we also have

$$1 = i \circ \mathrm{Tr}(y) = \prod_{\varphi \in G} y^{\varphi} = yy^{\sigma}.$$

Hence we obtain $y^{\sigma} = y^{-1} = y$, which gives the result. ∎

***Remark 1.4*** Under the hypotheses of Proposition 1.3, the proof shows that $G$ acts trivially on $WK_2(E)(2)$ if and only if $WK_2(E)(2)$ is an elementary abelian group.

We are now in a position to state the following.

***Theorem 1.5*** *Suppose $E/F$ is a quadratic extension of number fields with $F$ totally real such that $WK_2(F)(2) = 0$. If $\langle[\alpha_F]\rangle = \widetilde{D}_F$, then*

(i) *If $E/F$ is a CM extension (*i.e.*, a totally imaginary quadratic extension of a totally real field) or if $\mu(F_v)(2) = \{\pm 1\}$ for some $v \in T_{E/F}$, then*

$$\mathrm{rk}_2(WK_2(E)) = \begin{cases} |T_{E/F}| - 2 & \text{if } \alpha_F \notin N_{E/F}(E^*), \\ |T_{E/F}| - 1 & \text{if } \alpha_F \in N_{E/F}(E^*). \end{cases}$$

(ii) *Otherwise*

$$\mathrm{rk}_2(WK_2(E)) = \begin{cases} |T_{E/F}| - 1 & \text{if } \alpha_F \notin N_{E/F}(E^*), \\ |T_{E/F}| - \rho & \text{if } \alpha_F \in N_{E/F}(E^*), \end{cases}$$

*where $\rho = 0$ or $\rho = 1$.*

**Proof** First of all, note that case (a) of the Genus Formula does not occur under our hypotheses. We then simply apply Propositions 1.2 and 1.3, the point (i) corresponding to case (b) in the Genus Formula and (ii) to case (c). The only thing in question is the value of $\rho$ in case (ii) when $\alpha_F \notin N_{E/F}(E^*)$. But the result is obvious by the final remark of Section 1.1. ∎

To obtain the 2-rank explicitly, it remains to compute $\rho$ in all cases. For this reason, we focus our attention in the sequel on the interesting special case:

$(*)$ $E/F$ is a quadratic extension of totally real number fields, such that $\alpha_F \in N_{E/F}(E^*)$, $E \not\subset F_\infty$ and $|\mu(F_v)(2)| \geqslant 4$ for all $v \in T_{E/F}$.

### 1.3 A Refinement of the Genus Formula

For the remainder of this section, we assume that the hypotheses of $(*)$ hold. In the sequel we shall refer to quadratic extensions which fall under $(*)$ as *case* $(*)$ *extensions*. We now aim at proving a refinement of the genus formula by computing $\rho$ explicitly in $(*)$.

Consider the diagram in Section 1.1. Recall that the homology at the term $D_F/F^{*2}N_{E/F}(D_E)$ determines $\rho$. Let $[\alpha_F] \in \tilde{D}_F = D_F/F^{*2}$ generate $\tilde{D}_F$. According to condition $(*)$, $\alpha_F$ is a norm in $E/F$ so that there exists $\eta \in E^*$ such that $\alpha_F = N_{E/F}(\eta)$.

Choose $\delta \in F^*$ such that $E = F(\sqrt{\delta})$. Let $\sigma$ be a nontrivial element of $G := \mathrm{Gal}(E/F)$. Then $\{\sqrt{\delta}, \alpha_F\}^\sigma = \{-1, \alpha_F\}\{\sqrt{\delta}, \alpha_F\} = \{\sqrt{\delta}, \alpha_F\}$, the last equality being true as $[\alpha_F] \in \tilde{D}_F$.

Thus, as stated in [KM, p. 120], we see that the symbol $\{\sqrt{\delta}, \alpha_F\}$ lies in $K_2(o_E^S)(2)^G$ and the class of $\{\sqrt{\delta}, \alpha_F\}$ generates the quotient group $K_2(o_E^S)(2)^G \bmod K_2(o_F^S)(2)$. Indeed this comes from [Ka, Théorème 2.3(iv)], taking into account [Ka, Proposition 6.1] which supplies, under our hypothesis, the isomorphism

$$K_2(o_E^S)(2)^G/\operatorname{Im} K_2(o_F^S)(2) \cong K_2(E)^G/\operatorname{Im} K_2(F).$$

Set $\epsilon := \{\sqrt{\delta}, \alpha_F\} \in K_2(o_E^S)(2)^G$. Then its image in $\tilde{D}_F$ is $[\alpha_F] \in \tilde{D}_F$ (see [KM, p. 120]). Now assume that $\alpha'([\alpha_F]) = 0$. From the diagram in Section 1.1 we see that there exists $\omega \in \bigoplus_v \mu(F_v)(2)$ such that $j_s(\omega) = \alpha(\epsilon)$. Let

$$\pi\colon \bigoplus_{v\in S} \mu(F_v)(2) \to \mu(F)(2),$$

given by $\pi((\xi_v)_{v\in S}) = \prod_{v\in S} \xi_v^{n_v/n}$, where $n_v = |\mu(F_v)(2)|$ is the number of $2^s$-torsion (for all $s \in \mathbb{N}$) elements of $F_v^*$ and $n = |\mu(F)(2)|$ is the number of $2^s$-torsion elements in $F^*$.

We claim that $\rho = 0 \Leftrightarrow \pi(\omega) = 1$. Indeed, assume first that $\rho = 0$ and hence the diagram in Section 1.1 is exact in the term $D_F/F^{*2}N_{E/F}D_E$. Then there exist elements $\nu \in WK_2(E)(2)^G$ and $\theta \in K_2(O_F^S)(2)$ such that $\gamma(\nu) + i(\theta) = \epsilon$. Here $i$ is used also to denote the natural map $i\colon K_2(o_F^S)(2) \to K_2(o_E^S)(2)^G$ induced by the inclusion map $F \to E$.

Let $\omega'$ be the image of $\theta$ under the natural map

$$K_2(o_F^S)(2) \longrightarrow \bigoplus_{v\in S} \mu(F_v)(2).$$

Then we see that $j_S(\omega - \omega') = 0$.

Using the exact sequence

$$K_2(O_F^S)(2) \longrightarrow \bigoplus_{v\in s} \mu(F_v)(2) \xrightarrow{\pi} \mu(F)(2) \to 0,$$

we see that $\pi(\omega') = 1$. Also $\omega - \omega'$ belongs to the kernel of $j_S$, which is equal to $\bigoplus_{v\in T_{E/F}} \mu_2$ (for details on the determination of $\ker j_S$ see [KM, p. 116]). Under the condition $(*)$, $n_v \geqslant 4$ for all $v \in T_{E/F}$ so that $n_v/n = n_v/2 \geqslant 2$. Thus coming back to the definition of $\pi$, any element in $\bigoplus_{v\in T_{E/F}} \mu_2$ is necessarily in the kernel of $\pi$. Hence $\pi(\omega - \omega') = 1$ and so $\pi(\omega) = 1$.

Later we will determine $\rho$ by considering it at dyadic places and those in $T_{E/F}$. For this we make the following definition. Let $v$ be a prime in $F$ above the rational prime $q$. If $\omega$ is defined as above, then we define $\rho_v$ (mod 2) by the equation

$$(-1)^{\rho_v} = \pi|_v(\omega_v).$$

Here $\pi|_v$ stands for $\pi|_{\mu(F_v)(2)}$ and $\omega = (\omega_v)_v$ where $\omega_v \in \mu(F_v)(2)$. Note that $\rho_v = 0$ if $v$ is non-dyadic and unramified over $\mathbb{Q}$ since the corresponding tame symbol vanishes. Now define $\rho_q$ by $\rho_q \equiv \sum_{v|q} \rho_v \mod 2$, so that we get $\rho \equiv \sum_q \rho_q \mod 2$, since there is no contribution from the infinite primes (indeed $\alpha_F$ is totally positive).

Before going further with the computation of $\rho$, we fix the following notations for $E/F$, a quadratic extension of number fields:

- $n = |\mu(F)(2)|$,
- $m = |\mu(E)(2)|$,
- $v$ a non complex prime of $F$,
- $w$ is any non complex prime of $E$ above $v$,
- $n_v = |\mu(F_v)(2)|$,
- $m_w = |\mu(E_w)(2)|$,
- $( \,.\, , \,.\, )_{E_w,m_w}$ or $( \,.\, , \,.\, )_{m_w}$ denotes the local Hilbert symbol with values in $\mu(E_w)(2)$.

In the case that $v$ is an odd prime in $T_{E/F}$ we calculate $\rho_v$ using the following.

***Proposition 1.6*** *Let $F$ be totally real with $E = F(\sqrt{\delta})$, $\delta \in \mathbb{Z}$ such that $E/F$ is a case $(*)$ extension with $E$ Galois over $\mathbb{Q}$. Then for an odd prime $v \in T_{E/F}$ we have*

$$\rho_v = 0 \Longleftrightarrow (\delta, \alpha_F)_{F_v,4} = \left(\frac{\alpha_F}{v}\right)_4^{e_q(F/\mathbb{Q})} = 1,$$

i.e., *$\rho_v$ is defined by the formula*

$$\alpha_F^{\frac{Nv-1}{4}\cdot e_q(F/\mathbb{Q})} \equiv (-1)^{\rho_v} \mod v.$$

*Here $e_q(F/\mathbb{Q})$ denotes the ramification index of $q$ in the extension $F/\mathbb{Q}$ and $\left(\frac{\alpha_F}{v}\right)_4$ is the 4-th power-residue symbol.*

***Remark 1.7*** **(About the definition of the power-residue symbol)** Let $s$ be a natural number and $F$ a number field containing the group $\mu_s$ of $s$-th roots of unity. Let $v$ be a non complex prime of $F$. We have already recalled how to define the $s$-th Hilbert symbol $(a, b)_{F_v,s}$ for $a$ and $b$ in $F^*$. We define the $s$-th power-residue symbol by

$$\left(\frac{a}{v}\right)_s := (a, \bar{\pi})_{F_v,s},$$

where $v$ is a prime ideal of $F$ prime to $s$, the element $a$ is a unit in $F_v^*$, and $\bar{\pi}$ is a prime element of $F_v$. We can see that the definition does not depend on the choice of the prime element $\bar{\pi}$, and that

$$\left(\frac{a}{v}\right)_s \equiv 1 \mod v \Longleftrightarrow a \equiv x^s \mod v,$$

(*i.e.*, $a$ is an $s$-th power residue modulo $v$), and more generally

$$\left(\frac{a}{v}\right)_s \equiv a^{\frac{Nv-1}{s}} \mod v.$$

Details can be found in [N, Chapter III, §5; Chapter IV, §9].

**Proof of Proposition 1.6** Note that the Hilbert symbol in the above statement is indeed of order 2 by the assumption on $\alpha_F$. The conditions on the primes in $T_{E/F}$ imply that $|\mu(F_v)(2)| > |\mu(F)(2)| = 2$. Thus, it must be the case that $m_w = n_v$, since otherwise $E_w \subset F_{v,\infty}$ (see for example [KM, Lemma 2.1]). Noting that $(\sqrt{\delta}, \alpha_F)_{m_w} = \zeta^2$ for some $\zeta \in \mu(F_v)(2)$ (again by [KM, Lemma 2.1]), we see that $\rho_v = 0 \Leftrightarrow \zeta^{n_v/2} = 1$. Now

$$\zeta^{n_v/2} = (\zeta^2)^{n_v/4} = (\sqrt{\delta}, \alpha_F)^{n_v/4}_{E_w,m_w} = (\sqrt{\delta}, \alpha_F)_{E_w,4}$$

since $m_w = n_v > 2$. Since $v$ does not split in $E$, we see that the last symbol is equal to

$$(\sqrt{\delta}, \alpha_F)_{E_w,4} = (-\delta, \alpha_F)_{F_v,4} = (\delta, \alpha_F)_{F_v,4}.$$

Thus $\rho_v = 0 \Leftrightarrow (\delta, \alpha_F)_{F_v,4} = 1$. Let $q$ be the rational prime divisor of $\delta$ below $v \in T_{E/F}$. Recall that the norm residue symbols in which we are interested are tame at non-dyadic primes, and so $\rho_v$ is determined by

$$(q, \alpha_F)_{F_v,4} = \left((-1)^{ab}\frac{{\alpha_F}^a}{q^b}\right)^{\frac{Nv-1}{4}} \mod v,$$

where $a = \operatorname{ord}_v(q)$, $b = \operatorname{ord}_v(\alpha_F)$. Thus the formula reduces to

$$(q, \alpha_F)_{F_v,4} = \alpha_F^{\frac{Nv-1}{4}\cdot e_q(F/\mathbb{Q})} \mod v. \qquad \blacksquare$$

The following proposition will be of use in the sequel for calculating $\rho$.

***Proposition 1.8*** *Let $M$ be a totally real Galois extension of $\mathbb{Q}$, not containing $\sqrt{2}$, with trivial 2-Hilbert kernel. Suppose that $L = M(\sqrt{\delta})$ is a non-trivial extension for some square-free integer $\delta$ such that $L/M$ is a case $(*)$ extension. If the rational prime $q$ decomposes in some quadratic subfield of $M$, then $\rho_q = 0$.*

**Proof** Let $G = \operatorname{Gal}(L/\mathbb{Q})$ and let $H = \operatorname{Gal}(L/M)$. In this situation we have

$$\{\sqrt{\delta}, 2\}^{\phi} = \{-\sqrt{\delta}, 2\} = \{\sqrt{\delta}, 2\}$$

where $H = \langle\phi\rangle$. Thus

$$\alpha(\{\sqrt{\delta}, 2\}) \in \Big(\bigoplus_q \bigoplus_{w|q} \mu(L_w)\Big)^G$$

and so $\rho_v$ is independent of $v|q$. The result follows since there is an even number of such $v|q$. $\blacksquare$

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

***Remark 1.9*** In the sequel, we will apply the above proposition to multiple-quadratic fields. Thus, we restrict our attention to quadratic and bi-quadratic fields since Griffiths [Gr1] has shown that totally real number fields with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ have non-trivial 2-Hilbert kernel if $r > 2$.

***Corollary 1.10*** *Let $L/M$ be as in Proposition* 1.8 *with $M$ bi-quadratic over $\mathbb{Q}$.*

(i) *If $q$ is unramified in $M/\mathbb{Q}$, then $\rho_q = 0$.*
(ii) *If $q$ is odd, then $\rho_q = 0$.*

**Proof** (i) Since $q$ is unramified in $M$, the inertia group $I_v$ of $v$ in $M/\mathbb{Q}$ is trivial. Since $\mathrm{Gal}(M_v/\mathbb{Q}_q) \cong D_v/I_v$ is cyclic, where $D_v$ is the decomposition group of $v$ in $M/\mathbb{Q}$, we have $|D_v| = 1$ or 2 which means that $q$ splits in some quadratic subfield of $M$ and the result follows from the above proposition.

The second assertion follows from (i) and Proposition 1.6. ■

The following is Lemma 3.2 of [KM] and will also be of use in Section 2.

***Lemma 1.11*** *Let $M$ be a multiple-quadratic field and let $L$ be a subfield of index* 2. *An undecomposed dyadic prime $v$ of $L$ does not belong to $T_{M/L}$ if and only if $\sqrt{2} \notin L_v$, $M_w = L_v(\sqrt{2})$ and $L_v$ contains $\sqrt{-1}$ or $\sqrt{-2}$.*

# 2 Applications

## 2.1 Quadratic Fields

For this section, let us set $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{d})$ where $d$ is a squarefree integer. We aim at computing the 2-rank of $WK_2(E)$ using the previous section and, as a consequence, recovering the results already proved in [BS] using different techniques. First of all, let us recall the following well-known lemma.

***Lemma 2.1*** *Let $d$ be a squarefree integer.*

(i) $-1$ *is a norm from $\mathbb{Q}(\sqrt{d})$ if and only if $d > 0$ and all odd prime divisors of $d$ are congruent to* 1 *modulo* 4.
(ii) 2 *is a norm from $\mathbb{Q}(\sqrt{d})$ if and only if all odd prime divisors of $d$ are congruent to* $\pm 1$ *modulo* 8.

We now focus our attention on quadratic fields satisfying the assumptions of $(*)$: this means that $E = \mathbb{Q}(\sqrt{d}), d > 0$. Since for $p \in T_{E/\mathbb{Q}}$ we must have $|\mu(\mathbb{Q}_p)(2)| \geqslant 4$, this implies that $2 \notin T_{E/\mathbb{Q}}$ and that $p \equiv 1 \bmod 4$ for all odd $p|d$; hence $d \equiv 1 \bmod 8$. Since 2 is a norm, the prime divisors of $d$ are all $\equiv 1 \bmod 8$. Furthermore $\rho_q = 0$ for all odd $q \nmid d$, since the symbol $\{\sqrt{d}, 2\}$ is tame at $q$. Using the results of the previous section we have

$$(-1)^{\rho_2} = (2, \sqrt{d})_{\mathbb{Q}_2,2} = \prod_{p \in T_{E/\mathbb{Q}}} (2, \sqrt{p})_{\mathbb{Q}_2,2}, \quad (-1)^{\rho_p} = \left(\frac{2}{p}\right)_4, \forall p \in T_{E/\mathbb{Q}}.$$

***Proposition 2.2*** *In the situation above, $(2, \sqrt{p})_{\mathbb{Q}_2,2} = \left(\frac{-1}{p}\right)_8$ for all $p \in T_{E/\mathbb{Q}}$.*

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

**Proof** Indeed, both symbols vanish precisely when $p \equiv 1 \bmod 16$. ■

Hence, $\rho$ is defined by

$$(-1)^{\rho} = \prod_{p \in T_{E/\mathbb{Q}}} (2, \sqrt{p})_{\mathbb{Q}_2,2} \prod_{p \in T_{E/\mathbb{Q}}} \Big(\frac{2}{p}\Big)_4 = \prod_{p \in T_{E/\mathbb{Q}}} \Big(\frac{-1}{p}\Big)_8 \prod_{p \in T_{E/\mathbb{Q}}} \Big(\frac{4}{p}\Big)_8$$
$$= \prod_{p \in T_{E/\mathbb{Q}}} \Big(\frac{-4}{p}\Big)_8$$

since $\zeta_8 \in \mathbb{Q}_p$ for all $p \in T_{E/\mathbb{Q}}$ and so the formula

$$\Big(\frac{2}{p}\Big)_4 = \Big(\frac{2}{p}\Big)_8^2 = \Big(\frac{4}{p}\Big)_8$$

holds for all $p \in T_{E/\mathbb{Q}}$.

We may now state the result for $d > 0$.

***Proposition 2.3*** *Let $d > 0$ be the product of odd rational primes, each $\equiv 1 \bmod 8$. Then $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a case $(*)$ extension and $\rho$ is given by*

$$(-1)^{\rho} = \prod_{p \mid d} \Big(\frac{-4}{p}\Big)_8 .$$

*In other words, $\rho$ is congruent (modulo 2) to the number of prime divisors of $d$ not representable over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

***Remark 2.4*** Note that for primes $p \equiv 1 \bmod 8$, the condition $\big(\frac{-4}{p}\big)_8 = -1$ is equivalent to $p \neq x^2 + 32y^2$ (see [BC]).

As a result of Proposition 2.3 and Theorem 1.5 we get the following.

***Corollary 2.5*** ([**BS**]) *Let $d > 0$ be the product of odd rational primes, each $\equiv 1$* mod 8. *Denote by $t$ the number of prime divisors of $d$, and $s$ the number of prime divisors of $d$ not representable over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$. Then*

$$\mathrm{rk}_2\, WK_2(\mathbb{Q}(\sqrt{d})) = \begin{cases} t & \text{if } s \text{ is even,} \\ t-1 & \text{if } s \text{ is odd.} \end{cases}$$

We now wish to show that our method enables us to compute the 2-rank of the Hilbert kernel of *any* quadratic field. Once again we aim at applying Theorem 1.5. Since, by Lemma 1.11, we have

$$2 \in T_{E/F} \iff 2 \text{ is undecomposed in } \mathbb{Q}(\sqrt{d}),$$
$$\iff d \not\equiv 1 \bmod 8,$$

it is easy to see that case (ii) in Theorem 1.5 holds if and only if $d > 0, d \equiv 1 \bmod 8$ and all prime divisors of $d$ are $\equiv 1 \bmod 4$. It remains to note that $\alpha_F = \alpha_{\mathbb{Q}} = 2$ by Lemma 1.1, which implies that we can draw up (with Theorem 1.5 and Lemma 2.1) the following table where the 2-rank of $WK_2(E)$ is given.

| | | | $2 \in \mathrm{N}_{E/\mathbb{Q}}(E^*)$ | $2 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*)$ |
|---|---|---|---|---|
| $d < 0$ | $d \not\equiv 1 \bmod 8$ | | $t$ | $t-1$ |
| | $d \equiv 1 \bmod 8$ | | $t-1$ | $t-2$ |
| $d > 0$ | $d \not\equiv 1 \bmod 8$ | | $t$ | $t-1$ |
| | $d \equiv 1 \bmod 8$ | $-1 \in \mathrm{N}_{E/\mathbb{Q}}(E^*)$ | $t-\rho$ | $t-1$ |
| | | $-1 \notin \mathrm{N}_{E/\mathbb{Q}}(E^*)$ | $t-1$ | $t-2$ |

In this table $t$ denotes the number of odd prime divisors of $d$, and the value of $\rho$ in $(*)$ (*i.e.*, when $d > 0$, $d \equiv 1 \bmod 8$ and that 2 and $-1$ are both norms from $\mathbb{Q}(\sqrt{d})$) is given by Corollary 2.5.

Using the computation of the 2-rank, we conclude by listing all quadratic fields with trivial 2-primary Hilbert kernel (see also [BS]).

***Corollary 2.6*** *The 2-primary Hilbert kernel exactly vanishes for the following values of the squarefree integer $d$:*

$$
\begin{array}{ll}
d = -1, \pm 2, & \\
d = \pm p, \pm 2p & \textit{with } p \equiv \pm 3 \bmod 8, \\
d = -p & \textit{with } p \equiv 7 \bmod 8, \\
d = p & \textit{with } p \equiv 1 \bmod 8 \textit{ and } p \neq x^2 + 32y^2, \\
d = pq & \textit{with } p \equiv q \equiv 3 \bmod 8, \\
d = -pq & \textit{with } p \equiv -q \equiv 3 \bmod 8,
\end{array}
$$

*where $p$ and $q$ are distinct odd primes.*

## 2.2 Biquadratic Fields

We are now interested in computing the 2-rank of a bi-quadratic field $E$ having a totally real quadratic subfield $F$ such that $WK_2(F)(2) = 0$ (in order to apply Theorem 1.5). As before, we will focus our attention on case $(*)$ extensions $E$ since the computation of $\rho$ shows up in this case. For the remainder of this section let $F = \mathbb{Q}(\sqrt{d})$ and $E = \mathbb{Q}(\sqrt{d}, \sqrt{\delta})$ be totally real with $WK_2(F)(2) = 0$. We may assume that $d, \delta \in \mathbb{Z}$ are squarefree and positive with $d \nmid \delta$. In fact, Corollary 2.6 implies that $d$ is one of the following:

$$
\begin{array}{ll}
2, & \\
p, 2p & p \text{ a prime with } p \equiv \pm 3 \bmod 8, \\
p & p \text{ a prime with } p \equiv 1 \bmod 8,\ p \neq x^2 + 32y^2, \\
pq & p, q \text{ primes with } p \equiv q \equiv 3 \bmod 8.
\end{array}
$$

As a result we may also assume that the gcd of $d$ and $\delta$ is 1 or 2 in the cases where $d \not\equiv 1 \bmod 8$, and that this gcd is 1 or $q$ for some prime $q \equiv 3 \bmod 8$ otherwise. In addition we have the following.

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

***Proposition 2.7*** *For $d$ in the previous list, the set $T_{E/F}$ contains all undecomposed dyadic primes. Thus, a dyadic prime of $F$ is in the set $T_{E/F}$ if and only if it does not split in $E$.*

**Proof** By Lemma 1.11, if an undecomposed dyadic prime lies outside of $T_{E/F}$, then necessarily $E_w = F_v(\sqrt{2})$, and $F_v$ contains either $\sqrt{-1}$ or $\sqrt{-2}$. Thus we can assume that $d \equiv -1$ or $-2 \mod 8$. We see however that this is impossible (*e.g.* by Corollary 2.6). ■

***Remark 2.8*** (i) Note that we are only in $(*)$ when the dyadic primes of $F$ split in $E$. Indeed, in all cases involving the $d$'s of the above list, we have $|\mu(F_v)(2)| = 2$ for all dyadic primes $v$ in $F$, so that necessarily $v \notin T_{E/F}$ under the assumptions of $(*)$.

(ii) For an odd rational prime $q$ lying below the prime $v \in T_{E/F}$ we have $q \nmid d$ and so thus $e_q(F/\mathbb{Q}) = 1$.

Before we move on to the explicit calculations, it will be convenient to record the following observation.

***Lemma 2.9*** *Suppose that $E/F$ (as defined above) is a case $(*)$ extension and let $q$ be a rational prime lying below the prime $v \in T_{E/F}$. Then $q \equiv 1 \mod 4$ or $\left(\frac{d}{q}\right) = -1$. If $\sqrt{2} \notin F$, then $q \equiv 1 \mod 8$ or $\left(\frac{d}{q}\right) = -1$.*

**Proof** Note that $q \nmid d$ by Remark 2.8. The first statement is a reformulation of the fact that $|\mu(F_v)(2)| > |\mu(F)(2)|$, which means that either $\sqrt{-1} \in \mathbb{Q}_q$ or else $q$ must be inert in $F = \mathbb{Q}(\sqrt{d})$. The second statement incorporates the requirement that $2 \in F$ is a norm from $F(\sqrt{\delta})$. Indeed, if $\left(\frac{d}{q}\right) = 1$, then $q$ decomposes in $F$ and $q \equiv 1 \mod 4$. Since 2 is a norm, we must have $(2, q)_{F_{\mathfrak{q}_1},2} = (2, q)_{\mathbb{Q}_q,2} = 1$ which implies that $q \equiv 1 \mod 8$. ■

### 2.2.1 $d \neq 2$

We move on now to the determination of $\rho_{E/F}$ for $d \neq 2$ appearing in the list.

***Proposition 2.10*** *Let $q$ be a rational prime sitting below a prime $v \in T_{E/F}$. Then we have $\rho_q = 1 \Leftrightarrow q \equiv -3 \mod 8$.*

**Proof** We first consider the case where $q \equiv 3 \mod 4$ (*i.e.*, $q \equiv 3, -1 \mod 8$). For such a prime we noted in Lemma 2.9 that $(\frac{d}{q}) = -1$ and so $Nv = q^2$ and $v(q) = 1$. Since $2 \in \mathbb{Z}$, we have $(2 \mod v) \in \mathbb{Z}/q\mathbb{Z} \subset o_{F_v}/v$. We also have $4|(q+1)$ and so

$$2^{\frac{q^2-1}{4}} = 2^{(q-1)\frac{q+1}{4}} = 1 \mod q$$

which yields the result in this case by Proposition 1.6.

Now suppose $q \equiv 5 \mod 8$. Again Lemma 2.9 implies that $\left(\frac{d}{q}\right) = -1$ so that $Nq = q^2$. Now $q+1 \equiv 6 \mod 8$ and so $\frac{q+1}{2}$ is an odd integer. Thus

$$2^{\frac{q^2-1}{4}} \equiv 2^{\frac{q-1}{2}\frac{q+1}{2}} \equiv \left(\frac{2}{q}\right)^{\frac{q+1}{2}} \equiv -1 \mod q$$

and the result follows in this case.

Recall that there are no restrictions placed on primes $q \equiv 1 \bmod 8$ dividing $\delta$ so we must consider two cases. If $(\frac{d}{q}) = -1$, then the calculation is identical to the last considered except that in this case $(\frac{2}{q}) = 1$ and the result follows. We are left with the case where $q \equiv 1 \bmod 8$ and $(\frac{d}{q}) = 1$ which is settled by Proposition 1.8. ■

For $m \in \mathbb{Z}$ define $\theta^+(m)$ to be the number (mod 2) of primes dividing $m$ which are $\equiv +3 \bmod 8$. Similarly, let $\theta^-(m)$ be the number (mod 2) of primes dividing $m$ which are $\equiv -3 \bmod 8$. Then we have the following.

***Corollary 2.11*** *Recall that $d \nmid \delta$. For $d \not\equiv 1 \bmod 8$ we have $\rho_{E/F} \equiv \theta^+(\delta) \bmod 2$; if $d \equiv 1 \bmod 8$, then $\rho_{E/F} \equiv \theta^-(\delta) \bmod 2$.*

**Proof** To determine $\rho$, it remains to calculate $\rho_2$ in the various cases. If $d \not\equiv 1 \bmod 8$, then $\gcd(d, \delta) = 1$ or 2, so that the odd primes ramifying in $E/F$ are precisely those which divide $\delta$. Thus

$$\sum_{v \in T_{E/F}} \rho_v \equiv \sum_{\substack{q|\delta \\ q \text{ odd}}} \rho_q \equiv \theta^-(\delta) \mod 2$$

by the previous proposition. Also, 2 does not split in $F$ and so

$$(\sqrt{\delta}, 2)_{E_w,2} = (N_{E/F_1}(\sqrt{\delta}), 2)_{F_{1,v},2} = (-\delta, 2)_2.$$

Thus $\rho_2 \equiv \theta^+(\delta) + \theta^-(\delta) \bmod 2$ where $F_1$ is the dyadic decomposition field in the extension $E/\mathbb{Q}$. Therefore $\rho_{E/F} \equiv \theta^+(\delta) + 2\theta^-(\delta) \equiv \theta^+(\delta) \bmod 2$.

If $d \equiv 1 \bmod 8$, then $\rho_2 = 0$ by Proposition 1.8 and either $\gcd(d, \delta) = 1$ or $\gcd(d, \delta) = q$ for some prime $q \equiv 3 \bmod 8$ (not lying below a prime in $T_{E/F}$ by Remark 2.8). In both situations we see that the equality $\sum_{v \in T_{E/F}} \rho_v \equiv \theta^-(\delta) \bmod 2$ still holds, as required. ■

***Example 2.12*** Let $d = 3$ and $\delta = 17 \cdot 43 \cdot 53 \cdot 101 = 3913043$. The prime divisors $q$ of $\delta$ satisfy:

| $q$ | 17 | 43 | 53 | 101 |
|---|---|---|---|---|
| $q \bmod 8$ | 1 | 3 | $-3$ | $-3$ |
| $(\frac{3}{q})$ | $-1$ | $-1$ | $-1$ | $-1$ |

Thus the set $T_{E/F}$ consists of the unique primes of $F = \mathbb{Q}(\sqrt{3})$ above 17, 43, 53, and 101. Indeed since $\delta \equiv 3 \bmod 8$, the prime 2 is decomposed in $\mathbb{Q}(\sqrt{3\delta})$ so that the dyadic prime of $F$ is decomposed in $E/F$ and does not belong to $T_{E/F}$. As a consequence (here $d = 3 \not\equiv 1 \bmod 8$), we get $\theta^+(\delta) = 1$, $\rho = 1$, and finally,

$$\operatorname{rk}_2 WK_2(\mathbb{Q}(\sqrt{3}, \sqrt{\delta})) = 3.$$

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

***Example 2.13*** Let $d = 3$ and

$$\delta = 7 \cdot 29 \cdot 31 \cdot 67 \cdot 73 \cdot 139 \cdot 149 = 637465173793.$$

The prime divisors $q$ of $\delta$ satisfy

| $q$ | 7 | 29 | 31 | 67 | 73 | 139 | 149 |
|---|---|---|---|---|---|---|---|
| $q$ mod 8 | $-1$ | $-3$ | $-1$ | 3 | 1 | 3 | $-3$ |
| $\left(\frac{3}{q}\right)$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ |

Thus the set $T_{E/F}$ consists of the unique primes of $F = \mathbb{Q}(\sqrt{3})$ above 7, 29, 31, 67, 139, 149 and the two primes of $F$ above 73. Indeed, since $\delta \equiv 1 \bmod 8$, the prime 2 is decomposed in $\mathbb{Q}(\sqrt{\delta})$ so that the dyadic prime of $F$ is decomposed in $E/F$. As a consequence (here $d = 3 \not\equiv 1 \bmod 8$), we get $\theta^{+}(\delta) = 2$, $\rho = 0$, and finally,

$$\mathrm{rk}_2\, WK_2(\mathbb{Q}(\sqrt{3}, \sqrt{\delta})) = 8.$$

***Example 2.14*** Let $d = 17$ and $\delta = 23 \cdot 29 \cdot 107 = 71369$. The prime divisors $q$ of $\delta$ satisfy

| $q$ | 23 | 29 | 107 |
|---|---|---|---|
| $q$ mod 8 | $-1$ | $-3$ | 3 |
| $\left(\frac{17}{q}\right)$ | $-1$ | $-1$ | $-1$ |

Thus the set $T_{E/F}$ consists of the unique primes of $F = \mathbb{Q}(\sqrt{17})$ above 23, 29, and 107. Indeed since $\delta \equiv 1 \bmod 8$, the prime 2 is decomposed in $\mathbb{Q}(\sqrt{\delta})$ so that the dyadic prime of $F$ is decomposed in $E/F$ and does not belong to $T_{E/F}$. As a consequence (here $d = 17 \equiv 1 \bmod 8$), we get $\theta^{-}(\delta) = 1$, $\rho = 1$, and finally,

$$\mathrm{rk}_2\, WK_2(\mathbb{Q}(\sqrt{17}, \sqrt{\delta})) = 2.$$

***Example 2.15*** Let $d = 17$ and $\delta = 5 \cdot 11 \cdot 37 \cdot 89 \cdot 131 = 23726065$. The prime divisors $q$ of $\delta$ satisfy

| $q$ | 5 | 11 | 37 | 89 | 131 |
|---|---|---|---|---|---|
| $q$ mod 8 | $-3$ | 3 | $-3$ | 1 | 3 |
| $\left(\frac{17}{q}\right)$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ |

Thus the set $T_{E/F}$ consists of the unique primes of $F = \mathbb{Q}(\sqrt{17})$ above 5, 11, 37, 131, and the two primes of $F$ above 89. Indeed since $\delta \equiv 1 \bmod 8$, the prime 2 is decomposed in $\mathbb{Q}(\sqrt{\delta})$ so that the dyadic prime of $F$ is decomposed in $E/F$. As a consequence (here $d = 17 \equiv 1 \bmod 8$), we get $\theta^{-}(\delta) = 2$, $\rho = 0$, and finally,

$$\mathrm{rk}_2\, WK_2(\mathbb{Q}(\sqrt{17}, \sqrt{\delta})) = 6.$$

### 2.2.2 $d = 2$

We note that in this situation $F = \mathbb{Q}(\sqrt{2})$ and $\alpha_F = 2 + \sqrt{2}$. The next proposition gives a criterion for case $(*)$ extensions.

***Proposition 2.16*** *Let $\delta$ be a squarefree integer. Then the extension $F(\sqrt{\delta})/F$ is a case $(*)$ extension if and only if each odd prime divisor of $\delta$ is $\equiv 1 \bmod 16$.*

**Proof** Recall that $\alpha_F$ must be a norm to be in $(*)$. We calculate the symbol $(2+\sqrt{2}, \delta)_2$ over the global field $F$ by using the Hasse principle: suppose that $2+\sqrt{2}$ is a norm from $E$, and let $q$ be a rational prime divisor of $\delta$ congruent to $\pm 3 \bmod 8$. Since $q$ is inert in $F$, let $v$ denote the prime of $F$ above $q$ and we have

$$(2+\sqrt{2}, \delta)_{F_v,2} = (2+\sqrt{2}, q)_{F_v,2} = (2, q)_{\mathbb{Q}_v,2} = -1,$$

which contradicts our assumption that $2+\sqrt{2}$ is a norm. Note also that for $q \equiv -1 \bmod 8$, $q|\delta$ we require that $q$ is inert in $F$ (so that we are adjoining roots of unity locally), which is impossible.

Assume then that $q \equiv 1 \bmod 8$. Let $v$ be one of the two primes above $q$ and note that

$$(2+\sqrt{2}, q)_{F_v,2} = (2+\sqrt{2})^{\frac{q-1}{2}} \mod q,$$

which is clearly trivial if and only if $\zeta_{16} \in \mathbb{F}_q$ (since $\sqrt{-1} \in \mathbb{F}_q$), *i.e.*, if and only if $q \equiv 1 \mod 16$. The result follows by reciprocity since there is only one dyadic prime in $F$. ■

For the remainder of this section we assume that $\delta$ is the product of distinct odd rational primes, each $\equiv 1 \bmod 16$.

We now calculate $\rho_2$. Since $\delta \equiv 1 \bmod 8$, it is a 2-adic square and since $\delta \equiv 1 \bmod 16$ we know that its 2-adic square roots are $\equiv \pm 1 \bmod 8$. Thus

$$(\sqrt{\delta}, 2+\sqrt{2})_{F_2,2} = (\sqrt{\delta}, 2)_{\mathbb{Q}_2,2} = 1$$

and so $\rho_2 = 0$.

Now let $q|\delta$ be odd and let $v_1, v_2$ be the primes in $F$ above $q$. Then $\rho_q = \rho_{v_1} + \rho_{v_2} \bmod 2$ and we calculate

$$(\delta, 2+\sqrt{2})_{F_{v_1},4} \cdot (\delta, 2+\sqrt{2})_{F_{v_2},4}$$

as in the previous section. This product is equal to

$$(2.1) \qquad (\delta, 2+\sqrt{2})_{\mathbb{Q}_q,4} \cdot (\delta, 2-\sqrt{2})_{\mathbb{Q}_q,4} = (\delta, 2)_{\mathbb{Q}_q,4} \equiv 2^{\frac{q-1}{4}} \mod q.$$

***Lemma 2.17*** *The symbol in (2.1) is equal to $\left(\frac{-4}{q}\right)_8$.*

**Proof** Since $\zeta_{16} \in \mathbb{Q}_q$, we have $\left(\frac{-1}{q}\right)_8 = 1$. Now the symbol in (2.1) is equal to $\left(\frac{2}{q}\right)_4$, and we have

$$\left(\frac{2}{q}\right)_4 = \left(\frac{2}{q}\right)_8^2 = \left(\frac{4}{q}\right)_8 = \left(\frac{-4}{q}\right)_8$$

as required. ■

We arrive at the following proposition which, surprisingly, looks like Proposition 2.3.

***Proposition 2.18*** *Suppose $\delta > 0$ is the product of distinct odd rational primes, each congruent to* 1 mod 16*. Then $\rho_{E/F}$ is congruent (modulo 2) to the number of prime divisors of $\delta$ not representable over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

**Proof** This follows from the calculation of $\rho$ above and from Remark 2.4. ■

As an application of the previous calculation of $\rho$, we give a family of bi-quadratic fields for which we are able to compute the 2-rank of the Hilbert kernel in general. Note that similar applications to other families of bi-quadratic fields should be possible.

***Corollary 2.19*** *Let $F = \mathbb{Q}(\sqrt{2})$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{\delta})$ where $\delta$ is any squarefree odd integer. We denote by $t_0$ the number of prime divisors of $\delta$ which are congruent to $\pm 1$ modulo* 8 *and by $t_1$ the number of prime divisors of $\delta$ which are congruent to $\pm 3$ modulo* 8*. Then the* 2*-rank of the Hilbert kernel of $E = \mathbb{Q}(\sqrt{2}, \sqrt{\delta})$ is given in the following table:*

<table>
<tr><td colspan="3"></td><td>$\forall q \vert \delta, q \equiv \pm 1$ mod16</td><td>$\exists q \vert \delta, q \not\equiv \pm 1$ mod1</td></tr>
<tr><td rowspan="2">$\delta < 0$</td><td colspan="2">$\delta \not\equiv 1$ mod 8</td><td>$2t_0$</td><td>$2t_0 + t_1 - 1$</td></tr>
<tr><td colspan="2">$\delta \equiv 1$ mod 8</td><td>$2t_0 - 1$</td><td>$2t_0 + t_1 - 2$</td></tr>
<tr><td rowspan="3">$\delta > 0$</td><td colspan="2">$\delta \not\equiv 1$ mod 8</td><td>$2t_0$</td><td>$2t_0 + t_1 - 1$</td></tr>
<tr><td rowspan="2">$\delta \equiv 1$ mod 8</td><td>$\forall p \vert \delta, p \equiv 1, 3, 4$ mod 8</td><td>$2t_0 - \rho$</td><td>$2t_0 + t_1 - 1$</td></tr>
<tr><td>$\exists p \vert \delta, p \equiv -1$ mod 8</td><td>$2t_0 - 1$</td><td>$2t_0 + t_1 - 2$</td></tr>
</table>

*The above value of $\rho$ in the case where $\delta > 0, \delta \equiv 1$ mod $8, \forall p \vert \delta, p \equiv 1, 3, 5$ mod 8 and $\forall q \vert \delta, q \equiv \pm 1$ mod 16, which simply means that $\delta > 0$ and $\forall q \vert \delta, q \equiv 1$ mod 16, is given (by the previous proposition) in the following way: $\rho$ is congruent (modulo 2) to the number of prime divisors of $\delta$ not representable over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

**Proof** We aim at applying Theorem 1.5. Here we have $F = \mathbb{Q}(\sqrt{2}), E = \mathbb{Q}(\sqrt{2}, \sqrt{\delta})$, $\alpha_F = 2 + \sqrt{2}$. Moreover, the number of prime divisors of $\delta$ which are decomposed (resp. undecomposed) in $F$ is $t_0$ (resp. $t_1$). To complete the table we need the following facts.

***Lemma 2.20*** *Let $F = \mathbb{Q}(\sqrt{2})$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{\delta})$ where $\delta$ is any squarefree odd integer. Then*

(i) $\alpha_F = 2 + \sqrt{2}$ *is a norm in $E/F$ if and only if $\forall q|\delta, q \equiv \pm 1 \bmod 16$.*

(ii) *If $v$ is the dyadic prime of $F$, then $v \in T_{E/F}$ if and only if $\delta \not\equiv 1 \bmod 8$.*

(iii) *If $v$ is a prime of $F$ lying above a prime divisor $q$ of $\delta$, then $v \in T_{E/F}$ and*

$$\mu(F_v)(2) = \{\pm 1\} \Leftrightarrow q \equiv -1 \bmod 8.$$

**Proof** (i) It comes from arguments already seen in the proof of our Proposition 2.16 and in the proof of [KM, Proposition 3.5].

(ii) We have $v \in T_{E/F}$ if and only if $v$ is undecomposed in $E$ and if $\mu(F_v)(2) = \{\pm 1\}$. So $v \in T_{E/F}$ if and only if $v$ is undecomposed in $E$, namely if and only if 2 is undecomposed in $\mathbb{Q}(\sqrt{\delta})$, whence the result.

(iii) Since $v$ is tamely ramified in $E$, we have $v \in T_{E/F}$. Moreover if $\mu(F_v)(2) = \mu(\mathbb{Q}_q(\sqrt{2}))(2) = \{\pm 1\}$, then $q \equiv 3 \bmod 4$. Now, on the one hand, if $q \equiv 3 \bmod 8$, $q$ is inert in $F = \mathbb{Q}(\sqrt{2})$ and $\mu_4$ is contained in the residue field $\mathbb{F}_{q^2}$ of $F_v$. On the other hand, if $q \equiv -1 \bmod 8$, $q$ is decomposed in $F = \mathbb{Q}(\sqrt{2})$ and $\mu(F_v)(2) = \mu(\mathbb{Q}_q)(2) = \{\pm 1\}$. ■

Putting all these facts together, it is easy to apply Theorem 1.5. Note that in the first column where $\forall q|\delta, q \equiv \pm 1 \bmod 16$, the number $t_1$ never shows up since $t_1 = 0$ in this case. ■

***Example 2.21*** Let $\delta = 17 \cdot 257 = 4369$. We first note that 17 is not representable over $\mathbb{Z}$ by $x^2 + 32y^2$, whereas $257 = 15^2 + 32 \times 1^2$. The previous corollary gives $\rho = 1$ and so $\operatorname{rk}_2 WK_2(\mathbb{Q}(\sqrt{2}, \sqrt{\delta})) = 3$.

***Example 2.22*** Let $\delta = 97 \cdot 113 \cdot 241 = 2641601$. Now 97 and 241 are not representable over $\mathbb{Z}$ by $x^2 + 32y^2$, whereas $113 = 9^2 + 32 \times 1^2$. The previous corollary gives $\rho = 0$ and thus $\operatorname{rk}_2 WK_2(\mathbb{Q}(\sqrt{2}, \sqrt{\delta})) = 6$.

## 2.3 Tri-Quadratic Fields

In this section we let $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a totally real bi-quadratic field with trivial 2-Hilbert kernel. Such fields were completely determined (using $\zeta$-functions) in [KM] as those appearing in the following list:

$$\begin{array}{ll} \mathbb{Q}(\sqrt{2}, \sqrt{p}) & \text{with } p \equiv \pm 3 \bmod 8, \\ \mathbb{Q}(\sqrt{p}, \sqrt{q}) & \text{with } p \equiv q \equiv 3 \bmod 8, \\ \mathbb{Q}(\sqrt{2p}, \sqrt{2q}) & \text{with } p \equiv q \equiv 3 \bmod 8, \\ \mathbb{Q}(\sqrt{pq}, \sqrt{qr}) & \text{with } p \equiv q \equiv r \equiv 3 \bmod 8, \end{array}$$

where $p, q$ and $r$ are distinct odd primes. Note that the vanishing of the 2-Hilbert kernel for these fields can be verified by the 2-rank formula of the previous section.

Let $E = F(\sqrt{\delta})$ be a quadratic extension of $F$ for some square-free rational integer $\delta$ and for a rational prime $q$ we will always use $v$ to denote a prime of $F$ above $q$ and use $w$ to denote a prime of $E$ above $v$. We are again interested in case $(*)$ extensions $E/F$ and we show the following.

***Proposition 2.23*** *With the notations defined above,* $\rho_{E/F} = 0$.

**Proof** First assume that $\sqrt{2} \notin F$. By Corollary 1.10 we have $\rho_{\text{odd}} = 0$. Moreover, by Proposition 1.8 and Corollary 1.10, if 2 is either unramified in $F$ or splits in a quadratic subfield of $F$, then $\rho_2 = 0$ and the result follows in this case.

Suppose now that $F = \mathbb{Q}(\sqrt{2}, \sqrt{p})$, $p \equiv \pm 3 \bmod 8$. Again, we assume that $\alpha_F = 2 + \sqrt{2}$ is a norm from $E = F(\sqrt{\delta})$ where $\delta$ is a squarefree integer and is prime to 2 and to $p$.

By taking norms twice we may calculate $\rho_2$ as follows:

$$\begin{aligned}(-1)^{\rho_2} &= (2+\sqrt{2}, \sqrt{\delta})_{\mathbb{Q}_2(\sqrt{2},\sqrt{p})}\\ &= (2+\sqrt{2}, \pm\delta)_{\mathbb{Q}_2(\sqrt{2})}\\ &= (2, \delta)_{\mathbb{Q}_2}.\end{aligned}$$

Suppose that $\delta$ has an odd prime divisor $q \equiv \pm 3 \bmod 8$. Recall that to be a case $(*)$ extension $\alpha_F = 2 + \sqrt{2}$ must be a norm from $E$ and so, in particular, the symbol $(2+\sqrt{2}, q)_{\mathbb{Q}_q(\sqrt{2},\sqrt{p}),2}$ must vanish. Now the primes above $q$ must split in the extension $\mathbb{Q}(\sqrt{2}, \sqrt{p})/\mathbb{Q}(\sqrt{2})$ by the proof of Corollary 1.10 and so the last symbol is equal to $(2+\sqrt{2}, q)_{\mathbb{Q}_q(\sqrt{2}),2} = (2, q)_{\mathbb{Q}_q,2}$ since $q$ is inert in $\mathbb{Q}(\sqrt{2})$. Thus $\alpha_F$ cannot be a norm in this situation, which means that the prime divisors of $\delta$ are $\equiv \pm 1 \bmod 8$ and so $\rho_2 = 0$.

We now calculate $\rho_{\text{odd}}$. Let $q$ be an odd prime lying below a prime in $T_{E/F}$. Let $K = \mathbb{Q}(\sqrt{2})$. If the primes in $K$ lying above $q$ split in $F$, the same argument to the one in Proposition 1.8 (with $G = \mathrm{Gal}(E/K)$, $H = \mathrm{Gal}(E/F)$ and 2 replaced with $2 + \sqrt{2}$) shows that $\rho_q = 0$.

It therefore remains to analyze the case where $q$ splits in $K$ and is inert in $F/K$. In this situation we need to calculate the product $(\delta, 2+\sqrt{2})_{F_{v_1},4} \cdot (\delta, 2+\sqrt{2})_{F_{v_2},4}$, which is equal to

$$(\delta, 2+\sqrt{2})_{\mathbb{Q}_q(\sqrt{p}),4} \cdot (\delta, 2-\sqrt{2})_{\mathbb{Q}_q(\sqrt{p}),4} = (\delta, 2)_{\mathbb{Q}_q(\sqrt{p}),4}.$$

By norming this symbol down to $\mathbb{Q}_q$ we obtain the symbol

$$(\delta^2, 2)_{\mathbb{Q}_q,4} = (\delta, 2)_{\mathbb{Q}_q,2} = \left(\frac{2}{q}\right) = 1$$

where the last equality is given by the condition that $q$ splits in $K$. ∎

***Example 2.24*** Let $\delta = 17 \cdot 97 = 1649$ such that $F = \mathbb{Q}(\sqrt{2}, \sqrt{13})$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{13}, \sqrt{1649})$. We start by checking that $E/F$ is a case $(*)$ extension. Since 17 and 97 are primes $\equiv 1 \bmod 16$, we know by Proposition 2.16 that $2+\sqrt{2}$ is a norm from the extension $\mathbb{Q}(\sqrt{2}, \sqrt{1649})/\mathbb{Q}(\sqrt{2})$ and so is a norm from $E/F$. Moreover, for any prime $v$ of $F$ above 17 or 97, it is obvious that $v \in T_{E/F}$ and that $|\mu(F_v)(2)| \geqslant 4$. Since $\delta \equiv 1 \bmod 8$, the dyadic prime of $F$ is decomposed in $E/F$ and then does not

https://doi.org/10.4153/CJM-2009-051-3 Published online by Cambridge University Press

belong to $T_{E/F}$. As a result, $E/F$ is indeed a case $(*)$ extension. We then get $\rho = 0$ and there remains to determine $|T_{E/F}|$: the computation of some Legendre symbols gives

$$\left(\frac{2}{17}\right) = 1, \left(\frac{13}{17}\right) = 1; \left(\frac{2}{97}\right) = 1, \left(\frac{13}{97}\right) = -1,$$

and implies that 17 is totally decomposed in $F/\mathbb{Q}$, and there are two primes of $F$ above 97. Hence $|T_{E/F}| = 6$ and $\mathrm{rk}_2\, WK_2(\mathbb{Q}(\sqrt{2}, \sqrt{13}, \sqrt{1649})) = 6$.

**Acknowledgements** The authors would like to thank M. Kolster and A. Movahhedi for their helpful suggestions throughout the development of this work. They also want to thank McMaster University (Canada) and Université de Limoges (France) where part of this research was done.

## References

[BC] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity.* J. Reine Angew. Math. **238**(1969), 67–70.

[BS] J. Browkin and A. Schinzel, *On Sylow-2 subgroups of $K_2(O_F)$ for quadratic number fields F.* J. Reine Angew. Math. **331**(1982), 104–113.

[CW] S. U. Chase and W. C. Waterhouse, *Moore's theorem on uniqueness of reciprocity laws.* Invent. Math. **16**(1972), 267–270.

[Ga] H. Garland, *A finiteness theorem for $K_2$ of a number field.* Ann. of Math. **94**(1971), 534–548.

[Gr1] R. Griffiths, *Multi-Quadratic Extensions of $\mathbb{Q}$ with Trivial 2-Primary Hilbert Kernel.* Master's thesis, McMaster University, 2000.

[Gr2] ———, *A genus formula for étale Hilbert kernels in a cyclic p-power extension.* Ph.D. thesis, McMaster University, 2005.

[JSG] J.-F. Jaulent and F. Soriano-Gafiuk, *2-Groupe des classes positives d'un corps de nombres et noyau sauvage de la $K_2$-théorie.* J. Number Theory **108**(2004), no 2, 187–208.

[Ka] B. Kahn, *Descente galoisienne et $K_2$ des corps de nombres.* K-theory **7**(1993), 55–100.

[Ke] F. Keune, *On the structure of the $K_2$ of the ring of integers in a number field.* K-Theory **2**(1989), no. 5, 625–645.

[KM] M. Kolster and A. Movahhedi, *Bi-quadratic number fields with trivial 2-primary Hilbert kernel.* Proc. London Math. Soc. **87**(2003), no. 1, 109–136.

[L1] M. Lescop, *Sur les 2-extensions de $\mathbb{Q}$ dont la 2-partie du noyau sauvage est triviale.* Thèse, Université de Limoges, 2003.

[L2] ———, *2-extensions of $\mathbb{Q}$ with trivial 2-primary Hilbert kernel.* Acta Arith. **112**(2004), no. 2, 345–366.

[Mi] J. Milnor, *Introduction to Algebraic K-Theory.* Annals of Mathematics Studies 72, Princeton University Press, Princeton, NJ, 1971.

[N] J. Neukirch, *Class Field Theory.* Grundlehren der Mathematischen Wissenschaften 280, Springer-Verlag, Berlin, 1986.

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

*Department of Mathematics and Statistics, McMaster University, 1280 Main Street West, Hamilton, Ontario L8S 4K1*
*e-mail*: ross.griffiths@gmail.com

*IUT de Brest, Départment GMP, Rue de Kergoat, 29200 Brest, France*
*e-mail*: mikael_lescop@hotmail.com