ACTA ARITHMETICA
119.3 (2005)

Relative norms of units and 4-rank of class groups

by

Tommy Bülow (Copenhagen)

1. Introduction. In this paper, we use the following notation, for K being a number field:

- $\mathcal{O}_K$ is the ring of integers of K;
- $\mathcal{O}_K^*$ is the group of units in $\mathcal{O}_K$;
- $\mathrm{Cl}(K)$ is the class group;
- $h(K)$ is the class number;
- for a fractional ideal $\mathfrak{a}$ of K, $[\mathfrak{a}]_K$ is the ideal class in $\mathrm{Cl}(K)$ containing $\mathfrak{a}$;
- $e_4(K)$ is the number of invariants of K divisible by 4, i.e. the number of cyclic factors of the 2-class group of K whose order is divisible by 4 ($e_4(K)$ will also be called the 4-rank of K);
- for an extension L/K of number fields, $N_{L/K}$ is the relative norm map;
- $\mathbb{Z}$ is the set of rational integers and $\mathbb{N}$ resp. $\mathbb{N}_0$ is the set of positive resp. non-negative integers;
- $\|$ means "divides exactly" (for prime powers);
- $\mathbb{F}_q$ is the finite field with q elements where q is a prime power.

The problem of the solvability of the negative Pell equation, $x^2 - dy^2 = -1$ with $d > 1$ square-free can, as is well known, be formulated as a question of whether the fundamental unit ε_d of $\mathbb{Q}(\sqrt{d})$ has norm -1. In other words, we ask whether the relative norm map between unit groups,

$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} : \mathcal{O}^*_{\mathbb{Q}(\sqrt{d})} \to \mathcal{O}^*_{\mathbb{Q}} = \{\pm 1\},$$

is surjective.

In general, we could ask the following natural question. Let L/K be an extension of number fields. What can be said about the relative norm map

$$N_{L/K} : \mathcal{O}_L^* \to \mathcal{O}_K^*$$

between unit groups? (Clearly, units of L are mapped to units of K.) In particular, can we decide whether this map is surjective?

2000 *Mathematics Subject Classification*: 11R11, 11R20, 11R27, 11R29.

In this paper, we investigate this problem for certain cyclic extensions of prime degree, mostly quadratic.

Apart from the classical case, not much is known about the general question. Hilbert (see [5]) gave a *reformulation* (in terms of the ramified primes of L/K) of the problem only in the special case of $K = \mathbb{Q}(i)$ the Gaussian field and $L = K(\sqrt{d})$, d an integer. We shall have more to say about this case later and we shall use it to illustrate some of the results.

See also [3] where this problem about surjectivity is considered for certain quadratic extensions of totally real number fields.

We mention two classical results.

Definition 1. Let D be the discriminant of the quadratic number field K. Consider factorizations $D = D_1 D_2$ of D where each of D_1 and D_2 is a product of prime discriminants or equal to 1. The factorizations $D = D_1 D_2$ and $D = D_2 D_1$ are considered the same. The factorization $D = D_1 D_2$ is *of the second kind* (German: "von zweiter Art") if

$$\left(\frac{D_2}{p}\right) = 1 \text{ for all primes } p \mid D_1 \quad \text{and} \quad \left(\frac{D_1}{p}\right) = 1 \text{ for all primes } p \mid D_2.$$

Here $\left(\frac{D_i}{\cdot}\right)$ is the Kronecker symbol.

Definition 2. For a finite abelian group G, the number of cyclic factors of the 2-Sylow subgroup of G whose order is divisible by 4 is called the 4-*rank* of G.

In 1934, Rédei and Reichardt (see [12] and [13]) proved the following theorem:

Theorem 1. *Let the quadratic number field K have discriminant D. If the number of factorizations $D = D_1 D_2$ of D of the second kind is 2^u, then u is the* 4-*rank of the strict class group of K.*

They also proved the following

Theorem 2. *Let $d > 1$ be a square-free integer. Assume that d is not divisible by a prime congruent to* 3 *modulo* 4. *If only the trivial factorization of the discriminant of $\mathbb{Q}(\sqrt{d})$ is of the second kind* (*which*, *by Theorem* 1, *means that the strict* 2-*class group of $\mathbb{Q}(\sqrt{d})$ is elementary abelian*), *then $N(\varepsilon_d) = -1$.*

The main results of this paper are the following two theorems (see Definition 4 for the definition of a (right) Rédei matrix and factorizations of the second kind):

Theorem 3. *Let l be a prime number. Let K be a number field that contains the lth roots of unity and assume that $l \nmid h(K)$; let $\pi_1, \ldots, \pi_t \in \mathcal{O}_K$,*

$t \geq 2$, be such that $(\pi_1), \ldots, (\pi_t)$ are powers of distinct prime ideals. Let $\beta_1, \ldots, \beta_t \in \{1, \ldots, l-1\}$; put $\alpha := \pi_1^{\beta_1} \cdots \pi_t^{\beta_t}$ and $L := K(\sqrt[l]{\alpha})$. Assume that the prime ideal in K dividing (π_i) is the unique prime ramified in $K(\sqrt[l]{\pi_i})$. Consider the Rédei matrix $M = M_{L/K}$. Define $u \geq 0$ by $\mathrm{rank}_{\mathbb{F}_l}(M) = t - 1 - u$. Then the index $[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]$ divides l^u. In particular, if M has maximal rank, $t-1$, then $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$.

We shall use $e_4(L)$ to denote the 4-rank of the class group of the number field L (cf. Definition 2).

Theorem 4. *Let K be a number field and assume that $2 \nmid h(K)$; let $\pi_1, \ldots, \pi_t \in \mathcal{O}_K$, $t \geq 2$, be such that $(\pi_1), \ldots, (\pi_t)$ are distinct prime ideals. Put $\alpha := \pi_1 \cdots \pi_t$ and $L := K(\sqrt{\alpha})$. Assume that (π_i) is the unique prime ramified in $K(\sqrt{\pi_i})$. Assume that $\mathcal{O}_K^* \subseteq N_{L/K}(L)$, so the 2-rank of $\mathrm{Cl}(L)$ is $t-1$ (cf. Lemmas 1 and 2). Let the right Rédei matrix $M_{L/K}$ have $\mathbb{F}_2$-rank $t-1-u$, $u \geq 0$. We can write $[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)] = l^w$, $w \geq 0$. Then*

$$u - w \leq e_4(L) \leq u.$$

In particular, if M has maximal rank, $t-1$ (i.e. if only the trivial factorization of α is of the second kind), then the 2-class group of L is elementary abelian.

2. General observations. In this section, we will see that the problem about surjectivity of the relative norm map between unit groups for certain cyclic extensions of prime degree is related to the ambiguous ideals of the extension.

Definition 3. Let L/K be a cyclic extension of number fields with Galois group $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. An ideal $\mathfrak{a}$ of L is called *ambiguous* (with respect to K) if it is fixed by σ: $\sigma(\mathfrak{a}) = \mathfrak{a}$.

An ideal class $[\mathfrak{a}]$ of L is called *ambiguous* (with respect to K) if it is fixed by σ: $\sigma([\mathfrak{a}]) = [\mathfrak{a}]$. The group of ambiguous ideal classes is denoted by $\mathrm{Am}(L/K)$. An ideal class $[\mathfrak{a}]$ of L is called *strongly ambiguous* (with respect to K) if it contains an ambiguous ideal. The group of strongly ambiguous ideal classes is denoted by $\mathrm{Am}_{\mathrm{s}}(L/K)$. Clearly, $\mathrm{Am}_{\mathrm{s}}(L/K) \subseteq \mathrm{Am}(L/K)$.

From [8, §13, Lemma 4.1] and [6, p. 115] we have:

Lemma 1. *Let L/K be a cyclic extension of number fields of prime degree l. Let t' be the number of ramified primes in L/K. For l odd, assume that no infinite prime ramifies in L/K. Then*

$$|\mathrm{Am}(L/K)| = \frac{h(K) l^{t'-1}}{[\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*]},$$

$$|\mathrm{Am}_{\mathrm{s}}(L/K)| = \frac{h(K) l^{t'-1}}{[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]}.$$

The following lemma is well known and easily proved.

LEMMA 2. *Let L/K be a quadratic extension of algebraic number fields. Suppose that $2 \nmid h(K)$. Then the 2-Sylow subgroup $\mathrm{Am}_2(L/K)$ of the group of ambiguous ideal classes is given by*

$$\mathrm{Am}_2(L/K) = \{[\mathfrak{a}]_L \in \mathrm{Cl}(L) \mid [\mathfrak{a}]_L^2 = [(1)]_L\};$$

and hence

$$|\mathrm{Am}_2(L/K)| = [\mathrm{Cl}(L) : \mathrm{Cl}(L)^2] = 2^{\mathrm{rank}_2(\mathrm{Cl}(L))}.$$

In particular,

$$2 \mid h(L) \;\Leftrightarrow\; 2 \mid |\mathrm{Am}_2(L/K)|.$$

PROPOSITION 1. *Let L/K be a cyclic extension of number fields of prime degree l. Assume that $l \nmid h(K)$ and that L/K is unramified at infinity. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t \subseteq \mathcal{O}_L$ be the ramified prime ideals in L/K. Put $\mathrm{Cl}_0(L) = \{[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_L \mid 0 \le a_i \le l-1\}$. Then*

$$|\mathrm{Cl}_0(L)| = \frac{l^{t-1}}{[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]}.$$

In particular, the index $[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]$ is a power of l.

Proof. Using the ambiguous class number formula (cf. Lemma 1),

$$|\mathrm{Am}(L/K)| = \frac{h(K) l^{t-1}}{[\mathcal{O}_K^* : N_{L/K}(L^*) \cap \mathcal{O}_K^*]},$$

and the fact that the map $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$, $[\mathfrak{a}]_K \mapsto [\mathfrak{a}]_L$, is injective (since $l \nmid h(K)$, cf. [10, Corollary, p. 190]) it is not hard to see that the group $\mathrm{Am}_{\mathrm{s}}(L/K)$ of strongly ambiguous ideal classes of L/K is the product of the subgroups

$$\mathrm{Cl}_0(L) \quad \text{and} \quad \{[\mathfrak{a}]_L \mid \mathfrak{a} \text{ fractional ideal in } K\},$$

where $\mathrm{Cl}_0(L)$ is an l-group (possibly trivial) and the second factor has order $h(K)$. It follows from Lemma 1 that

$$|\mathrm{Cl}_0(L)| = \frac{|\mathrm{Am}_{\mathrm{s}}(L/K)|}{h(K)} = \frac{l^{t-1}}{[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]}. \ \blacksquare$$

3. A sufficient condition for surjectivity. Let l be a prime number. Let K be an algebraic number field that contains the lth roots of unity and assume that $l \nmid h(K)$; let $\pi_1, \ldots, \pi_t \in \mathcal{O}_K$, $t \ge 2$, be such that $(\pi_1), \ldots, (\pi_t)$ are powers of distinct prime ideals. Assume that no prime different from the prime in K dividing (π_i) is ramified in the extension $K(\sqrt[l]{\pi_i})/K$. Let $\beta_1, \ldots, \beta_t \in \{1, \ldots, l-1\}$; put $\alpha := \pi_1^{\beta_1} \cdots \pi_t^{\beta_t}$. Let $\mathfrak{p}_i \subseteq \mathcal{O}_{K(\sqrt[l]{\alpha})}$ be the prime ideal above (π_i). Put $L := K(\sqrt[l]{\alpha})$ and $L' := K(\sqrt[l]{\pi_1}, \ldots, \sqrt[l]{\pi_t})$.

Definition 4. Let the notation be as above.

(i) We use the Artin symbol to define the $t \times t$ *Rédei matrix* $M = [M_{uv}] = M_{L/K}$ with coefficients in $\mathbb{F}_l$ (the field with l elements) corresponding to the extension L/K in the following way:

For $u, v \in \{1, \ldots, t\}$, we let $M_{uv} := k$ if

$$\left(\frac{L'/L}{\mathfrak{p}_u}\right)(\sqrt[l]{\pi_v})\Big/\sqrt[l]{\pi_v} = e^{\frac{2\pi i}{l}\cdot k}.$$

(ii) Let $l = 2$ (and hence $\beta_1 = \cdots = \beta_t = 1$), and let $(\pi_1), \ldots, (\pi_t)$ be prime ideals. We say that the Rédei matrix M is a *right* Rédei matrix if it satisfies the matrix relation

$$M \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

(iii) Let the assumptions be as in (ii). Consider a factorization $\alpha = \alpha_1\alpha_2$ where $\alpha_1 = \prod_{u\in A_1} \pi_u$ and $\alpha_2 = \prod_{u\in A_2} \pi_u$ with disjoint A_1 and A_2 whose union is $\{1, \ldots, t\}$. We think of $\alpha = \alpha_1\alpha_2$ and $\alpha = \alpha_2\alpha_1$ as the same factorization of α; hence there are 2^{t-1} distinct factorizations of α. We say that $\alpha = \alpha_1\alpha_2$ is a factorization of α *of the second kind* if the right Rédei matrix $M = M_{L/K}$ satisfies

$$\sum_{v\in A_2} M_{uv} = 0 \text{ for all } u \in A_1 \quad\text{and}\quad \sum_{v\in A_1} M_{uv} = 0 \text{ for all } u \in A_2.$$

Remark 1. (1) If $\mathfrak{p}_1^{\gamma_1} \cdots \mathfrak{p}_t^{\gamma_t}$, $\gamma_u \geq 0$, is a principal ideal, then

$$\left(\frac{L'/L}{\mathfrak{p}_1}\right)^{\gamma_1} \cdots \left(\frac{L'/L}{\mathfrak{p}_t}\right)^{\gamma_t} = 1,$$

i.e. the matrix relation $[\gamma_1 \cdots \gamma_t]M = [0 \cdots 0]$ holds. It follows that

$$\operatorname{rank}_{\mathbb{F}_l}(M) \leq \dim_{\mathbb{F}_l}(\mathrm{Cl}_0(L))$$

where $\mathrm{Cl}_0(L) = \{[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_L \mid 0 \leq a_i \leq l-1\}$.

In particular, if (π_i) is the n_ith power of a prime ideal in K, we have $\mathfrak{p}_1^{n_1\beta_1} \cdots \mathfrak{p}_t^{n_t\beta_t} = (\sqrt[l]{\alpha})$, which implies that a Rédei matrix has rank at most $t-1$ over $\mathbb{F}_l$.

Also, under the assumptions in (ii), a symmetric Rédei matrix is clearly a right Rédei matrix.

(2) Our definition (iii) is a generalization of the concepts in [13]. It is easily seen that

the $\mathbb{F}_2$-rank of $M_{L/K}$ is $t-1-u$

$\Leftrightarrow$ the number of factorizations of α of the second kind is 2^u.

We can now prove Theorem 3. Put $L := K(\sqrt[l]{\alpha})$ and let $\mathrm{Cl}_0(L) = \{[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_L \mid 0 \le a_i \le l-1\}$. Then Remark 1 and Proposition 1 imply that

$$l^{t-1-u} = l^{\mathrm{rank}_{\mathbb{F}_l}(M)} \le |\mathrm{Cl}_0(L)| = \frac{l^{t-1}}{[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]}.$$

Therefore, the index $[\mathcal{O}_K^* : N_{L/K}(\mathcal{O}_L^*)]$ divides l^u. If, in particular, $u = 0$, then $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$. This completes the proof of Theorem 3.

We shall illustrate the quadratic case in Section 5; here we give one example for $l = 3$:

PROPOSITION 2. *Let p be a prime number congruent to 1 modulo 9; so we can write $p = a^2+3b^2$ with $a, b \in \mathbb{Z}$. Assume that $3 \,\|\, b$. Then the following two relative norm maps are surjective*:

$$N_{K(\sqrt[3]{3p})/K} : \mathcal{O}^*_{K(\sqrt[3]{3p})} \to \mathcal{O}^*_K, \qquad N_{K(\sqrt[3]{3p^2})/K} : \mathcal{O}^*_{K(\sqrt[3]{3p^2})} \to \mathcal{O}^*_K,$$

where $K = \mathbb{Q}(\sqrt{-3})$.

Proof. Write $p = \pi\overline{\pi}$, $\pi = a + b\sqrt{-3}$, $\overline{\pi} = a - b\sqrt{-3}$; we can assume that $a \equiv 1 \pmod 9$. Since also $3 \mid b$, it is easy to see that $\left(\frac{\pi}{\overline{\pi}}\right)_3 = \left(\frac{\overline{\pi}}{\pi}\right)_3 = 1$. The fact that $3 \,\|\, b$ implies that $(\sqrt{-3})$ is inert in each of $K(\sqrt[3]{\pi})/K$ and $K(\sqrt[3]{\overline{\pi}})/K$.

If we let $\alpha_1 := \sqrt{-3} \cdot \pi \cdot \overline{\pi}$ and $\alpha_2 := \sqrt{-3} \cdot \pi^2 \cdot \overline{\pi}^2$, we see that the Rédei matrices $M_1 = M_{K(\sqrt[3]{\alpha_1})/K}$ and $M_2 = M_{K(\sqrt[3]{\alpha_2})/K}$ have the forms

$$M_1 = \begin{bmatrix} * & x & y \\ * & -x & 0 \\ * & 0 & -y \end{bmatrix}, \qquad M_2 = \begin{bmatrix} * & x & y \\ * & x & 0 \\ * & 0 & y \end{bmatrix},$$

where x and y are non-zero. Hence M_1 and M_2 have rank $2 = 3-1$ over $\mathbb{F}_3$. By Theorem 3 it is enough to note that $K(\sqrt[3]{\alpha_1}) = K(\sqrt[3]{3p^2})$ and $K(\sqrt[3]{\alpha_2}) = K(\sqrt[3]{3p})$. ■

4. 4-rank of class groups. From now on, we shall only consider quadratic extensions.

In this section, we prove Theorem 4. We shall use the following lemma whose proof is elementary:

LEMMA 3. *Let G be a finite abelian 2-group of 2-rank $n \in \mathbb{N}$. Let H be a subgroup of index 2 in G. Then it is possible to choose a basis $b_1, \ldots, b_n \in G$ for G such that $H = \langle b_1, \ldots, b_{n-1}, b_n^2 \rangle$.*

We can now prove Theorem 4. First, note that, by Proposition 1, we have

$$\dim_{\mathbb{F}_2}(\{[\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_L \mid a_i \in \{0,1\}\}) = t-1-w, \qquad w \in \{0,1,\ldots,t-1\},$$

where $\mathfrak{p}_i$ is the prime ideal in L above (π_i).

The idea of the proof is the same as in Reichardt [13], with a few adjustments. Class field theory will be used.

Note first that for a non-trivial factorization $\alpha = \alpha_1\alpha_2$ of α,

$$\begin{aligned} &\alpha = \alpha_1\alpha_2 \text{ is of the second kind}\\ &\Leftrightarrow \text{ each prime in } L \text{ dividing } (\alpha) \text{ splits completely in } K(\sqrt{\alpha_1},\sqrt{\alpha_2}). \end{aligned}$$

Put $A :=$ the group of fractional ideals of L and $S :=$ the group of fractional principal ideals of L.

As the 2-rank of $\mathrm{Cl}(L)$ is $t-1 \geq 1$, there is (by class field theory) at least one ideal group H_1 (modulo S) in L of index 2 in A. The corresponding class field L_1 is a quadratic and unramified extension of L and hence has the form $L_1 = K(\sqrt{\alpha_1},\sqrt{\alpha_2})$ where $\alpha = \alpha_1\alpha_2$ is a non-trivial factorization of α. Conversely, for every such non-trivial factorization of α the field $K(\sqrt{\alpha_1},\sqrt{\alpha_2})$ is a quadratic and unramified extension of L and is, therefore, the class field for an ideal group (modulo S) in L of index 2 in A.

By class field theory, $e_4(L) \geq 1$ if and only if there exists an unramified $\mathbb{Z}/4$-extension L_2 of L. If this is the case, there is exactly one field L_1 between L and L_2 such that L_1/L is a quadratic and unramified extension; L_1 must have the form $L_1 = K(\sqrt{\alpha_1},\sqrt{\alpha_2})$; the unique non-trivial factorization $\alpha = \alpha_1\alpha_2$ of α will be called the factorization of α *attached to* L_2.

We now prove some claims:

(a) *If the non-trivial factorization $\alpha = \alpha_1\alpha_2$ is attached to L_2 where L_2 is unramified and $\mathbb{Z}/4$ over L, then $\alpha = \alpha_1\alpha_2$ is of the second kind.*

Let H_2 be the ideal group (modulo S) in L corresponding to L_2. Let cH_2 be a generator of A/H_2 ($\simeq \mathbb{Z}/4$). Fix an $i \in \{1,\ldots,t\}$. Since, in L, $(\pi_i) = \mathfrak{p}_i^2$ and $(\pi_i) \in H_2$, we have $\mathfrak{p}_i \in \langle (cH_2)^2\rangle =: H_1$. As the class field L_1 corresponding to H_1 is unramified and quadratic over L and contained in L_2, it follows that $\mathfrak{p}_i$ splits completely in $L_1 = K(\sqrt{\alpha_1},\sqrt{\alpha_2})$. Hence $\alpha = \alpha_1\alpha_2$ is of the second kind. This proves (a).

(b) *Let the non-trivial factorization $\alpha = \alpha_1\alpha_2$ be of the second kind. Let H_1 be the ideal group (modulo S) in L corresponding to $K(\sqrt{\alpha_1},\sqrt{\alpha_2})$. Then*

$$\begin{aligned} &K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \textit{ is contained in an unramified } \mathbb{Z}/4\textit{-extension}\\ &\qquad\qquad\qquad\qquad \Leftrightarrow \mathrm{rank}_2(H_1/S) = t-1, \end{aligned}$$

and we have $\mathfrak{p}_1,\ldots,\mathfrak{p}_t \in H_1$.

$G := A/S$ has 2-rank $t-1$; and $G_1 := H_1/S$ has index 2 in G. By Lemma 3 (applied to 2-Sylow groups) we can write

$$G = \langle g_1 S, \ldots, g_{t-1} S\rangle \overline{H}/S, \qquad g_i \in A,$$

and

$$G_1 = \langle g_1 S, \ldots, g_{t-2} S, (g_{t-1} S)^2\rangle \overline{H}/S,$$

where $[\overline{H} : S]$ is odd. We see that

$$H_1 = \langle g_1, \ldots, g_{t-2}, g_{t-1}^2\rangle \overline{H}.$$

Assume that G_1 has 2-rank $t-1$. Then we must have $g_{t-1}^2 \notin S$. Put $H_2 := \langle g_1, \ldots, g_{t-2}, g_{t-1}^4\rangle \overline{H}$. Then $A/H_2 \simeq \mathbb{Z}/4$.

Now let $\mathrm{rank}_2(G_1) < t-1$. Then

$$H_1 = \langle g_1, \ldots, g_{t-2}\rangle \overline{H}.$$

From this we see that if $H_1 \supseteq N \supseteq S$ and $[H_1 : N] = 2$, then $A/N \not\simeq \mathbb{Z}/4$. (For $A = H_1 \cup g_{t-1} H_1$.) This proves the first part of (b). The second part is clear since each $\mathfrak{p}_i$ splits completely in $K(\sqrt{\alpha_1}, \sqrt{\alpha_2})$.

(c) *Let the non-trivial factorization $\alpha = \alpha_1\alpha_2$ be of the second kind. If $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$, then $K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/L$ is contained in an unramified $\mathbb{Z}/4$-extension.*

This follows from (b) and Proposition 1.

(d) *Assume that $N_{L/K}(\mathcal{O}_L^*) \neq \mathcal{O}_K^*$ and that (cf. Proposition 1)*

$$\dim_{\mathbb{F}_2}(\{[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_L \mid a_i \in \{0,1\}\}) = t - 1 - w, \qquad w \geq 1.$$

If prime ideals $\widetilde{\mathfrak{p}}_1, \ldots, \widetilde{\mathfrak{p}}_w$ in L not dividing (2α) are chosen such that

$$\dim_{\mathbb{F}_2}(\{[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t} \widetilde{\mathfrak{p}}_1^{\widetilde{a}_1} \cdots \widetilde{\mathfrak{p}}_w^{\widetilde{a}_w}]_L \mid a_i, \widetilde{a}_j \in \{0,1\}\}) = t - 1,$$

then, for a non-trivial factorization $\alpha = \alpha_1\alpha_2$ of the second kind,

$K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/L$ is contained in an unramified $\mathbb{Z}/4$-extension

$$\Leftrightarrow \left(\frac{\alpha_1}{\widetilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\widetilde{\mathfrak{p}}_j}\right) = 1 \textit{ for all } j \in \{1, \ldots, w\}.$$

Let H_1 be as in (b). Then (d) follows from:

$K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/L$ is contained in an unramified $\mathbb{Z}/4$-extension

$$\Leftrightarrow \mathfrak{p}_j \in H_1 \text{ for all } j \in \{1, \ldots, w\}$$

$$\Leftrightarrow \mathfrak{p}_j \text{ splits completely in } K(\sqrt{\alpha_1}, \sqrt{\alpha_2}) \text{ for all } j \in \{1, \ldots, w\}$$

$$\Leftrightarrow \left(\frac{\alpha_1}{\widetilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\widetilde{\mathfrak{p}}_j}\right) = 1 \text{ for all } j \in \{1, \ldots, w\}.$$

The proof of the theorem can now be finished as follows. Put

$$\begin{aligned} n :=\ & \text{the number of non-trivial factorizations } \alpha=\alpha_1\alpha_2 \text{ of the second kind}\\ & \quad \text{where } K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4\text{-extension}\\ =\ & \text{the number of non-trivial factorizations } \alpha=\alpha_1\alpha_2 \text{ where}\\ & K(\sqrt{\alpha_1},\sqrt{\alpha_2})/L \text{ is contained in an unramified } \mathbb{Z}/4\text{-extension}\\ =\ & \text{the number of subgroups of } G:=A/S \text{ of index } 2\\ & \text{containing a subgroup in } G \text{ with factor group } \mathbb{Z}/4\\ =\ & 2^{e_4(G)}-1 = 2^{e_4(L)}-1, \end{aligned}$$

where $e_4(G)$ is the 4-rank of the group G; here the third equality follows from class field theory and the fourth is group theory of finite abelian groups.

From (a) we get

$$n \le 2^u - 1.$$

For a given $j \in \{1,\dots,w\}$ we have

$$x_j := \left|\left\{\alpha=\alpha_1\alpha_2 \text{ of the second kind} \;\middle|\; \left(\frac{\alpha_1}{\widetilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\widetilde{\mathfrak{p}}_j}\right) = 1\right\}\right| \in \{2^{u-1}, 2^u\};$$

in particular, $x_j = 2^u$ if $N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*$. Since

$$n+1 = \left|\left\{\alpha=\alpha_1\alpha_2 \text{ of the second kind} \;\middle|\; \left(\frac{\alpha_1}{\widetilde{\mathfrak{p}}_j}\right) = \left(\frac{\alpha_2}{\widetilde{\mathfrak{p}}_j}\right) = 1 \text{ for all } j \in \{1,\dots,w\}\right\}\right|,$$

we conclude that

$$n+1 \ge 2^{u-y} \ge 2^{u-w}$$

where y is the number of j with $x_j = 2^{u-1}$.

Note also that for $u = t-1$,

$$n+1 = 2^u \;\Leftrightarrow\; x_1 = \dots = x_w = 2^u.$$

This completes the proof of Theorem 4.

Remark 2. (1) As the proof shows, information (in concrete examples) about (some of) the prime ideals $\widetilde{\mathfrak{p}}_1,\dots,\widetilde{\mathfrak{p}}_w$ could give a more precise lower bound on the 4-rank of L.

(2) For cyclic extensions $L = K(\sqrt[l]{\alpha})$ of K (l odd prime) with $\mathrm{Gal}(L/K) = \langle\sigma\rangle$, it might be possible, using other methods, e.g. ideas from [1] and [2], to prove a similar result where 2-rank and 4-rank are replaced by the indices $[\mathrm{Cl}(L) : \mathrm{Cl}(L)^{1-\sigma}]$ and $[\mathrm{Cl}(L)^{1-\sigma} : \mathrm{Cl}(L)^{(1-\sigma)^2}]$.

5. Quadratic extensions of $\mathbb{Q}(i)$. Let $(\pi_1),\dots,(\pi_t)$ be distinct prime ideals in $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ and assume that (π_j) is the only ramified prime in $\mathbb{Q}(i,\sqrt{\pi_j})/\mathbb{Q}(i)$. Put $\alpha := \pi_1\cdots\pi_t$. Since we are asking whether $x^2-\alpha y^2 = i$

is solvable in $\mathbb{Z}[i]$, we shall assume that the necessary condition for solvability,

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi_j) \equiv 1 \pmod 8 \quad \text{for all } j \in \{1,\dots,t\},$$

is fulfilled. This means that $i \in \mathcal{O}^*_{\mathbb{Q}(i)}$ is the relative norm of a *number* in $\mathbb{Q}(i,\sqrt{\alpha})$, and so this is also a necessary (and sufficient) condition for

$$\mathrm{rank}_2(\mathrm{Cl}(\mathbb{Q}(i,\sqrt{\alpha}))) = t-1$$

(cf. Lemma 2 and the ambiguous class number formula).

We begin by considering the case where $\alpha := d = \pi_1 \cdots \pi_t$ where $d \neq \pm 1$ is a square-free rational integer. Let $\overline{\mathfrak{p}}_j$ be the prime ideal in $L := \mathbb{Q}(i,\sqrt{d})$ above (π_j).

Remark 3. According to [5],

$$\mathrm{rank}_{\mathbb{F}_2}(\{[\overline{\mathfrak{p}}_1^{a_1} \cdots \overline{\mathfrak{p}}_t^{a_t}]_L \mid a_i \in \{0,1\}\}) \in \{t-2, t-1\}$$

and the following statements are equivalent:

(1) $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$.
(2) There exist $\varepsilon \in \mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$ and $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ such that $\gamma^2 = 2\varepsilon$.
(3) $\mathrm{rank}_{\mathbb{F}_2}(\{[\overline{\mathfrak{p}}_1^{a_1} \cdots \overline{\mathfrak{p}}_t^{a_t}]_L \mid a_i \in \{0,1\}\}) = t-1$.

Note that the equivalence of (1) and (3) also follows from Proposition 1.

From the equivalence of (1) and (2) we deduce a *rational* (and complete) criterion for i being in $N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$:

Theorem 5. (1) $i \in N_{\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{2})})$.

Let $d \in \mathbb{N} \setminus \{1,2\}$ be square-free.

(2) *If $d \equiv 1 \pmod 4$, then $i \notin N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$.*
(3) *If the negative Pell equation $x^2 - dy^2 = -1$ is solvable (in $\mathbb{Z}$), then $i \notin N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$.*
(4) *If $d \not\equiv 1 \pmod 4$ and $x^2 - dy^2 = -1$ is not solvable (in $\mathbb{Z}$), then:*

$$i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})}) \Leftrightarrow \exists x,y \in \mathbb{Z} : x^2 - dy^2 = \pm 2.$$

Proof. (1) This is immediate from Remark 3.

(2) Assume that $\gamma^2 = 2\varepsilon$, $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $\varepsilon \in \mathcal{O}^*_{\mathbb{Q}(\sqrt{d})}$; write $\gamma = (x + y\sqrt{d})/2$. We see that $x^2 - dy^2 = \pm 8$. Since also

$$2\varepsilon = \gamma^2 = \pm 2 + \frac{y^2 d + xy\sqrt{d}}{2},$$

we conclude that $2 \mid x, y$. But an equation $(x')^2 - d(y')^2 = \pm 2$ is impossible modulo 4.

(3) Let $x^2-dy^2=-4$ be solvable and let ε be a fundamental unit of $\mathbb{Q}(\sqrt{d})$ which has norm -1. If $i\in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then we have an equation $\gamma^2=\pm 2\varepsilon^k$ with $k\in\{0,1\}$. As $\sqrt{2}\notin\mathbb{Q}(\sqrt{d})$, we must have $k=1$. This gives the following contradiction:

$$0<(N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\gamma))^2=N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(2\varepsilon)=-4.$$

(4) As $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}=\mathbb{Z}[\sqrt{d}]$, the implication "⇒" is clear. So assume that $x^2-dy^2=2(-1)^k$; put $\gamma:=x+y\sqrt{d}$. Just note that

$$\gamma^2=x^2+dy^2+2xy\sqrt{d}=2((-1)^k+dy^2+xy\sqrt{d})$$

and

$$\begin{aligned}N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}((-1)^k+dy^2+xy\sqrt{d})&=1+d^2y^4+2dy^2(-1)^k-dx^2y^2\\&=1+dy^2(dy^2+2(-1)^k-x^2)=1.\ \blacksquare\end{aligned}$$

Remark 4. Let $d\in\mathbb{Z}\backslash\{\pm1,2\}$ be square-free and assume that $d\not\equiv 1 \pmod 4$ and that $x^2-dy^2=-1$ is not solvable (in $\mathbb{Z}$). If $q_1,\ldots,q_c\equiv 3 \pmod 4$ are (some of the) prime factors of d and if $\exists x,y\in\mathbb{Z}: x^2-dy^2=\pm 2$, then, clearly, $q_1\equiv\cdots\equiv q_c \pmod 8$ and exactly one of the equations is solvable; in that case, $x^2-dy^2=2$ is solvable if $q_i\equiv 7\pmod 8$ and $x^2-dy^2=-2$ is solvable if $q_i\equiv 3\pmod 8$.

Corollary 1. *Let $q\equiv 3 \pmod 4$ be a prime number. Then*

$$i\in N_{\mathbb{Q}(i,\sqrt{q})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{q})})\quad\textit{and}\quad i\in N_{\mathbb{Q}(i,\sqrt{2q})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{2q})}).$$

Proof. It is well known that one of the equations $x^2-qy^2=\pm 2$ and one of the equations $x^2-2qy^2=\pm 2$ is solvable (see for instance [11]). $\blacksquare$

Lemma 4. *Let K be a quadratic number field with discriminant D, and let q and p_1,p_2 be prime numbers such that (q) is inert in K and p_1,p_2 are split with prime (principal) ideal factorizations*

$$(p_1)=(\pi_1)(\widetilde{\pi}_1)\quad\textit{and}\quad(p_2)=(\pi_2)(\widetilde{\pi}_2)$$

in K. Assume that each of π_1 and π_2 is congruent to a square modulo 4 in $\mathcal{O}_K$. Then the following statements about quadratic residue symbols hold:

(1) $\left(\frac{q}{\pi_i}\right)=\left(\frac{q}{\widetilde{\pi}_i}\right)=\left(\frac{q}{p_i}\right)$ *where the last symbol is an ordinary (rational) Legendre symbol.*

(2) $\left(\frac{\widetilde{\pi}_1}{\pi_2}\right)=\left(\frac{\pi_1}{\widetilde{\pi}_2}\right)$.

(3) *If the Legendre symbol $\left(\frac{p_1}{p_2}\right)$ has the value 1, then $\left(\frac{\pi_1}{\pi_2}\right)=\left(\frac{\widetilde{\pi}_1}{\pi_2}\right)$ and $\left(\frac{\pi_1}{\widetilde{\pi}_2}\right)=\left(\frac{\widetilde{\pi}_1}{\widetilde{\pi}_2}\right)$; if $\left(\frac{p_1}{p_2}\right)=-1$, then $\left(\frac{\pi_1}{\pi_2}\right)\neq\left(\frac{\widetilde{\pi}_1}{\pi_2}\right)$ and $\left(\frac{\pi_1}{\widetilde{\pi}_2}\right)\neq\left(\frac{\widetilde{\pi}_1}{\widetilde{\pi}_2}\right)$.*

If $K\not\subseteq\mathbb{R}$, each of these quadratic residue symbols retains its value when reversed.

Proof. (1), (2) and (3) are clear. The last claim follows from the Quadratic Reciprocity Law in quadratic fields (Theorem 165 of [4]), which states the following. Let $\alpha,\beta\in\mathcal{O}_K$, with real conjugates $\alpha_1,\dots,\alpha_{r_1}$ and $\beta_1,\dots,\beta_{r_1}$, be coprime to 2, and suppose that α or β is congruent to a square modulo 4; then

$$\left(\frac{\alpha}{\beta}\right)\cdot\left(\frac{\beta}{\alpha}\right)=(-1)^{\sum_{i=1}^{n}((\mathrm{sgn}(\alpha_i)-1)/2)\cdot((\mathrm{sgn}(\beta_i)-1)/2)}. \ \blacksquare$$

The (right) Rédei matrices we encounter in the rest of this paper will be symmetric because of the Quadratic Reciprocity Law in quadratic fields.

We shall now give some applications of Theorem 4 for $K=\mathbb{Q}(i)$ and $\alpha:=d=\pi_1\cdots\pi_t$ where d is a rational integer.

Note that if $q\equiv 3 \pmod 4$ is a prime number and $a\in\mathbb{Z}$, then, in $\mathcal{O}_K=\mathbb{Z}[i]$, a is a quadratic residue modulo q.

Recall that $e_4(L)$ denotes the 4-rank of the class group of the number field L; also, if the odd d satisfies $i\in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then $d\equiv 3 \pmod 4$.

The first application is immediate:

Theorem 6. *Let $q_1,\dots,q_t\equiv 3 \pmod 4$ be prime numbers. Put $d:=q_1\cdots q_t$. Then*:

(1) $e_4(\mathbb{Q}(i,\sqrt{d}))\in\{t-2,t-1\}$.

(2) *If $i\in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and*

$$e_4(\mathbb{Q}(i,\sqrt{d}))=t-1;$$

in particular, $e_4(\mathbb{Q}(i,\sqrt{d}))$ *is even.*

Proof. The right Rédei matrix $M_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}$ is the zero matrix. ■

Theorem 7. *Let $q_1,\dots,q_t\equiv 3 \pmod 4$ and $p\equiv 1 \pmod 8$ be prime numbers. Put $d:=q_1\cdots q_t p$. Then*:

(1) $e_4(\mathbb{Q}(i,\sqrt{d}))\in\{t-2,t-1,t,t+1\}$.

(2) *If $i\in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and*

$$e_4(\mathbb{Q}(i,\sqrt{d}))\in\{t-1,t+1\};$$

in particular, $e_4(\mathbb{Q}(i,\sqrt{d}))$ *is even.*

Proof. In $\mathbb{Q}(i)$, let the prime factorization of p be $p=\pi\overline{\pi}$ where we can assume that $\pi\equiv\overline{\pi}\equiv 1 \pmod 4$. We only have to prove that the number of factorizations of $\alpha=q_1\cdots q_t\pi\overline{\pi}$ of the second kind is 2^{t-1} or 2^{t+1}; the other assertions follow from this.

We can write $\alpha=q_1\cdots q_a q_1'\cdots q_b'\pi\overline{\pi}$ where $\left(\frac{\pi}{q_i}\right)=\left(\frac{\overline{\pi}}{q_i}\right)=1$ and $\left(\frac{\pi}{q_j'}\right)=\left(\frac{\overline{\pi}}{q_j'}\right)=-1$.

Consider a factorization $\alpha = \alpha_1\alpha_2$ of α. Assume that $\pi \mid \alpha_1$ and $\overline{\pi} \mid \alpha_2$. If $b > 0$, then (for example) $q'_1 \mid \alpha_1$ and hence $\big(\frac{\alpha_2}{q'_1}\big) = \big(\frac{\overline{\pi}}{q'_1}\big) = -1$ and so $\alpha = \alpha_1\alpha_2$ is not of the second kind. If $b = 0$, then, clearly, $\alpha = \alpha_1\alpha_2$ is of the second kind; and there are 2^t such factorizations of the second kind.

For factorizations of the form

$$\alpha_1 = q_{i_1}\cdots q_{i_c}q'_{j_1}\cdots q'_{j_d}, \qquad \alpha_2 = q_{i_{c+1}}\cdots q_{i_a}q'_{j_{d+1}}\cdots q'_{j_b}\pi\overline{\pi}$$

where $\big(\frac{\pi}{q_{i_k}}\big) = \big(\frac{\overline{\pi}}{q_{i_k}}\big) = 1$ and $\big(\frac{\pi}{q'_{j_k}}\big) = \big(\frac{\overline{\pi}}{q'_{j_k}}\big) = -1$ it is easily seen that

$$\alpha = \alpha_1\alpha_2 \text{ is of the second kind } \Leftrightarrow\ 2 \mid d.$$

Hence

the number of such factorizations of the second kind

$= $ (number of subsets of $\{1,\ldots,b\}$ with an even number of elements)

$\cdot$ (number of subsets of $\{1,\ldots,a\}$)

$$= \begin{cases} 1\cdot 2^a = 2^t & \text{if } b = 0,\\ 2^{b-1}\cdot 2^a = 2^{t-1} & \text{if } b > 0.\end{cases}$$

Therefore, the total number of factorizations of the second kind is

$$\begin{cases} 2^t + 2^t = 2^{t+1} & \text{if } b = 0,\\ 0 + 2^{t-1} = 2^{t-1} & \text{if } b > 0. \ \blacksquare\end{cases}$$

THEOREM 8. *Let $q_1,\ldots,q_t \equiv 3 \pmod 4$ and $p_1,\ldots,p_a \equiv 1 \pmod 8$ be prime numbers and suppose that all the Legendre symbols $\big(\frac{q_i}{p_j}\big)$ and $\big(\frac{p_k}{p_j}\big)$ are equal to* 1. *Put $d := q_1\cdots q_tp_1\cdots p_a$. Then*:

(1) $e_4(\mathbb{Q}(i,\sqrt{d})) \in \{t+a-2,\ldots,t+2a-1\}$.

(2) *If $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and $e_4(\mathbb{Q}(i,\sqrt{d}))$ is even.*

Proof. We have

$$\alpha = q_1\cdots q_t\pi_1\overline{\pi}_1\cdots\pi_a\overline{\pi}_a;$$

here the prime factorization of p_i is $p_i = \pi_i\overline{\pi}_i$ where we can assume that $\pi \equiv \overline{\pi} \equiv 1 \pmod 4$.

Put $\beta := \pi_1\overline{\pi}_1\cdots\pi_a\overline{\pi}_a$, $\alpha_1 = q_{i_1}\cdots q_{i_c}\beta_1$ and $\alpha_2 = q_{i_{c+1}}\cdots q_{i_t}\beta_2$. Since, clearly,

$$\alpha = \alpha_1\alpha_2 \text{ is of the second kind } \Leftrightarrow\ \beta = \beta_1\beta_2 \text{ is of the second kind}$$

(because the Legendre symbols $\big(\frac{q_i}{p_j}\big)$ are equal to 1), the number of factorizations of the second kind of α is 2^t multiplied by the number of factorizations of the second kind of β. The right Rédei matrix $M_{\mathbb{Q}(i,\sqrt{\beta})/\mathbb{Q}(i)}$ is a block matrix built of 2×2 blocks of the form $\big[\begin{smallmatrix} x & x\\ x & x\end{smallmatrix}\big]$ (because the Legendre symbols $\big(\frac{p_k}{p_j}\big)$ are equal to 1). If we replace each such block with the entry x, we get an antisymmetric $a\times a$ matrix of the same $\mathbb{F}_2$-rank as $M_{\mathbb{Q}(i,\sqrt{\beta})/\mathbb{Q}(i)}$. By §91 of [14], this rank is even. Hence the number of factorizations of the second kind of α is of the form $2^t \cdot 2^{2a-1-2k}$ where $2k \in \{0,1,\ldots,a\}$. The theorem follows. ■

Let d be a product of t prime numbers congruent to 3 modulo 4. As noted in Theorem 6, $e_4(\mathbb{Q}(i,\sqrt{d})) = t-2$ or $t-1$. So, it would be natural to ask if we can decide, just by looking at the prime factors of d modulo 8, exactly when the case $e_4(\mathbb{Q}(i,\sqrt{d})) = t-1$ occurs. This is done in the next theorem.

Remark 5. Let $d > 1$ be a square-free integer. Consider the natural map

$$\begin{gathered}\phi : \mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \times \mathrm{Cl}(\mathbb{Q}(\sqrt{-d})) \to \mathrm{Cl}(\mathbb{Q}(i,\sqrt{d})),\\ ([\mathfrak{a}]_{\mathbb{Q}(\sqrt{d})}, [\mathfrak{b}]_{\mathbb{Q}(\sqrt{-d})}) \mapsto [\mathfrak{a}]_{\mathbb{Q}(i,\sqrt{d})}[\mathfrak{b}]_{\mathbb{Q}(i,\sqrt{d})}.\end{gathered}$$

(1) In [7], it is proved that the kernel and cokernel of ϕ are elementary abelian 2-groups.

(2) When d is a product of prime numbers congruent to 3 modulo 4, the image of ϕ is exactly the subgroup of $\mathrm{Cl}(\mathbb{Q}(i,\sqrt{d}))$ consisting of squares of ideal classes. (More precisely, this follows from the fact that, in this case, Hilbert's concepts of "Hauptgeschlecht" and "Geschlechter der Hauptart" coincide for the extension $\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)$; see [5].)

For the (unique) factorization $D = D_1 \cdots D_m$ of the discriminant D of a quadratic field K as a product of prime discriminants D_i, let χ_i be the genus character of the strict class group $\mathrm{Cl}_\mathrm{s}(K)$ corresponding to D_i. A strict ideal class $C \in \mathrm{Cl}_\mathrm{s}(K)$ is the square of a strict class if and only if at least $m-1$ of $\chi_1(C),\ldots,\chi_m(C)$ are equal to 1 (since $\chi_1\cdots\chi_m = 1$); see [15]. We can now state and prove:

Theorem 9. *Let $t \in \mathbb{N}$. Let the positive square-free integer d have the prime factorization*

$$d = q_1 \cdots q_s q_{s+1} \cdots q_t$$

with prime numbers $q_1 \equiv \cdots \equiv q_s \equiv 3$, $q_{s+1} \equiv \cdots \equiv q_t \equiv 7 \pmod 8$.

(1) *If $s = 0$, then $e_4(\mathbb{Q}(i,\sqrt{d})) = t-1$.*

(2) *If $s = t$, then* $e_4(\mathbb{Q}(i,\sqrt{d})) = \begin{cases} t-1 & \text{if } 2\nmid t,\\ t-2 & \text{if } 2\mid t.\end{cases}$

(3) *If $0 < s < t$, then*

$$e_4(\mathbb{Q}(i,\sqrt{d})) = t-1 \ \Leftrightarrow\ \left(\frac{q_{s+1}\cdots q_t}{q_i}\right) = (-1)^{t-1} \text{ for all } i \in \{1,\ldots,s\} \text{ and}$$
$$\left(\frac{q_1\cdots q_s}{q_j}\right) = 1 \text{ for all } j \in \{s+1,\ldots,t\},$$

where the above symbols are the ordinary Legendre symbols.

Proof. First note that for $t = 1$ the class number of $\mathbb{Q}(i, \sqrt{d})$ is odd, so the assertion is true in this case. So suppose that $t \geq 2$. Put

$$K_1 := \mathbb{Q}(\sqrt{d}) \quad \text{and} \quad K_2 := \mathbb{Q}(\sqrt{-d}).$$

In this proof, we shall use a superscript "s" to denote strict ideal classes: $[\mathfrak{a}]^{\mathrm{s}}_{K_i} \in \mathrm{Cl}_{\mathrm{s}}(K_i)$. The (ramified) primes in K_1 and in K_2 above $q_1, \ldots, q_s$, $q_{s+1}, \ldots, q_t$ are inert in $L := \mathbb{Q}(i, \sqrt{d})$. Put $q_0 := 2$. In K_1 resp. K_2, we shall denote the prime above q_i by $\mathfrak{p}_j$ resp. $\mathfrak{q}_j$ for $j = 0, \ldots, t$. Note that $[\mathfrak{p}_0]_L = [\mathfrak{q}_0]_L = [(1+i)]_L = 1$ and $[\mathfrak{p}_i]_L = [\mathfrak{q}_i]_L$ for $i = 1, \ldots, t$.

Observe that if $i \in N_{\mathbb{Q}(i,\sqrt{d})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{d})})$, then t is odd and $e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1$ and $s = 0$ or $s = t$. If t is odd, then:

$\mathfrak{p}_0$ is a principal ideal $\Rightarrow$ $x^2 - dy^2 = \pm 2$ is solvable $\Rightarrow$ $e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1$.

Let t be odd and assume that $x^2 - dy^2 = \pm 2$ is not solvable; so $\mathfrak{p}_0$ is not a principal ideal. Then we have (with ϕ as above):

$$\begin{aligned}
& e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1 \\
& \Leftrightarrow \ \mathrm{rank}_2(\mathrm{im}(\phi)) = t - 1 \\
& \Leftrightarrow \ \exists y \in \mathrm{im}(\phi) \backslash \{[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_L \mid a_i \in \{0, 1\}\} : \mathrm{ord}(y) = 2 \\
& \Leftrightarrow \ \exists x \in \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2) : \mathrm{ord}(x) = 4 \text{ and } \mathrm{ord}(\phi(x)) = 2 \\
& \Leftrightarrow \ \exists z \in \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2) : z \text{ is a square, } \mathrm{ord}(z) = 2 \text{ and } \phi(z) = 1 \\
& \Leftrightarrow \ \exists a_0, a_1, \ldots, a_t, b_1, \ldots, b_t \in \{0, 1\} : ([\mathfrak{p}_0^{a_0} \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_{K_1}, [\mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_t^{b_t}]_{K_2}) \text{ is} \\
& \qquad \text{a square in } \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2) \text{ of order 2 and } [\mathfrak{p}_1^{a_1} \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{q}_t^{b_t}]_L = 1 \\
& \Leftrightarrow \ ([\mathfrak{p}_0 \mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}, [\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) \text{ is a square in } \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2) \text{ of order 2.}
\end{aligned}$$

The first "⇔" follows from Remark 5(2). The third "⇔" follows from Remark 5(1) (about the kernel of ϕ).

The last "⇒" requires a proof. Assume that

$$z_1 := [\mathfrak{p}_0^{a_0} \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_{K_1} \in \mathrm{Cl}(K_1) \quad \text{and} \quad z_2 := [\mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_t^{b_t}]_{K_2} \in \mathrm{Cl}(K_2)$$

are squares with $\mathrm{ord}((z_1, z_2)) = 2$ and $[\mathfrak{p}_1^{a_1} \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{q}_t^{b_t}]_L = 1$. We have

$$\mathrm{rank}_{\mathbb{F}_2}(\{[\mathfrak{p}_1^{x_1} \cdots \mathfrak{p}_t^{x_t}]_{K_1} \mid x_i \in \{0, 1\}\}) \in \{t - 2, t - 1\};$$

let r be this rank. (For t even it is always the case that $r = t - 2$.)

Consider the equation $[\mathfrak{p}_1^{a_1} \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{q}_t^{b_t}]_L = 1$, i.e. $[\mathfrak{p}_1^{a_1+b_1} \cdots \mathfrak{p}_t^{a_t+b_t}]_L = 1$. If $r = t - 2$, then, by Remark 3, we must have $[\mathfrak{p}_1^{a_1+b_1} \cdots \mathfrak{p}_t^{a_t+b_t}]_{K_1} = 1$, i.e. $[\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}]_{K_1} = [\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_t^{b_t}]_{K_1}$; hence we can assume that $(a_1, \ldots, a_t) = (b_1, \ldots, b_t)$.

In the case we are considering, i.e. t odd, another way (which covers both of the cases $r = t - 2$ and $r = t - 1$) of realizing that we can assume that

$(a_1,\dots,a_t)=(b_1,\dots,b_t)$ is the following. As $\mathfrak{p}_0$ is not a principal ideal, the map

$$\{[\mathfrak{p}_0^{x_0}\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]_{K_1}\mid x_i\in\{0,1\}\}\ \to\ \{[\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]_L\mid x_i\in\{0,1\}\},$$
$$[\mathfrak{p}_0^{x_0}\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]\mapsto[\mathfrak{p}_1^{x_1}\cdots\mathfrak{p}_t^{x_t}]_L$$

has kernel $\{1,[\mathfrak{p}_0]_{K_1}\}$. Hence $[\mathfrak{p}_1^{a_1+b_1}\cdots\mathfrak{p}_t^{a_t+b_t}]_{K_1}=[\mathfrak{p}_0]_{K_1}^{\gamma}$ for a $\gamma\in\{0,1\}$, and this implies that $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}=[\mathfrak{p}_0^{a_0+\gamma}\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_t^{b_t}]_{K_1}$; and we can assume that $(a_1,\dots,a_t)=(b_1,\dots,b_t)$.

Since $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}$ is a square in $\mathrm{Cl}(K_1)$, either $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^{\mathrm{s}}$ or $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1+1}\cdots\mathfrak{p}_t^{a_t+1}]_{K_1}^{\mathrm{s}}$ is a square in $\mathrm{Cl}_{\mathrm{s}}(K_1)$. As $z_2=z_2\cdot[\mathfrak{q}_1\cdots\mathfrak{q}_t]_{K_2}$, we can assume that $[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^{\mathrm{s}}$ is a square in $\mathrm{Cl}_{\mathrm{s}}(K_1)$.

Let $\chi_k^{(1)}$ resp. $\chi_k^{(2)}$ be the kth genus character of K_1 resp. K_2 ($\chi_0^{(i)}$ corresponds to the prime discriminant -4 if 2 is ramified in $K_i/\mathbb{Q}$).

If $(a_1,\dots,a_t)=(0,\dots,0)$, then $\operatorname{ord}((z_1,z_2))=2$ implies that $a_0=1$; hence $[\mathfrak{p}_0]_{K_1}^{\mathrm{s}}=[\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^{\mathrm{s}}$ is a square in $\mathrm{Cl}_{\mathrm{s}}(K_1)$. As

$$\chi_i^{(1)}([\mathfrak{p}_0]_{K_1}^{\mathrm{s}})=\left(\frac{-q_i}{2}\right),\qquad i=1,\dots,t,$$

we conclude that $q_1\equiv\cdots\equiv q_t\equiv 7\pmod 8$, i.e. $s=0$, and so "⇒" is proved in this case.

Let $(a_1,\dots,a_t)\neq(0,\dots,0)$ and consider a $j\in\{1,\dots,t\}$ with $a_j=1$. We have

$$1=\chi_j^{(1)}([\mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_t^{a_t}]_{K_1}^{\mathrm{s}})=\prod_{\substack{i=0\\ i\neq j}}^{t}\chi_j^{(1)}([\mathfrak{p}_i^{a_i}]_{K_1}^{\mathrm{s}})\cdot\prod_{\substack{k=0\\ k\neq j}}^{t}\chi_k^{(1)}([\mathfrak{p}_j]_{K_1}^{\mathrm{s}})$$

and

$$1=\chi_j^{(2)}([\mathfrak{q}_1^{a_1}\cdots\mathfrak{q}_t^{a_t}]_{K_2})=\prod_{\substack{i=1\\ i\neq j}}^{t}\chi_j^{(2)}([\mathfrak{q}_i^{a_i}]_{K_2})\cdot\prod_{\substack{k=1\\ k\neq j}}^{t}\chi_k^{(2)}([\mathfrak{q}_j]_{K_2}).$$

For $i,k\in\{1,\dots,t\},\ i\neq k$, we have

$$\chi_k^{(1)}([\mathfrak{p}_i]_{K_1}^{\mathrm{s}})=\left(\frac{-q_k}{q_i}\right)=\chi_k^{(2)}([\mathfrak{q}_i]_{K_2}).$$

This and the above equalities imply that

$$1=\chi_j^{(1)}([\mathfrak{p}_0^{a_0}]_{K_1}^{\mathrm{s}})\cdot\chi_0^{(1)}([\mathfrak{p}_j]_{K_1}^{\mathrm{s}})=\left(\frac{-q_j}{2}\right)^{a_0}\cdot\left(\frac{-4}{q_j}\right)=\left(\frac{-q_j}{2}\right)^{a_0}\cdot(-1),$$

and hence $a_0=1$ and $q_j\equiv 3\pmod 8$. In particular, $a_{s+1}=\cdots=a_t=0$.

Assume now that $j \in \{1, \ldots, s\}$ and $a_j = 0$. Then

$$1 = \chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}]_{K_1}^{\mathrm{s}}) = \chi_j^{(1)}([\mathfrak{p}_0]_{K_1}^{\mathrm{s}}) \cdot \prod_{\substack{i=1 \\ i \neq j}}^{s} \chi_j^{(1)}([\mathfrak{p}_i^{a_i}]_{K_1}^{\mathrm{s}})$$

and

$$1 = \chi_j^{(2)}([\mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_s^{a_s}]_{K_2}) = \prod_{\substack{i=1 \\ i \neq j}}^{s} \chi_j^{(2)}([\mathfrak{q}_i^{a_i}]_{K_2}),$$

which implies that $1 = \chi_j^{(1)}([\mathfrak{p}_0]_{K_1}^{\mathrm{s}}) = \left(\frac{-q_j}{2}\right) = -1$, which is a contradiction; hence $a_1 = \cdots = a_s = 1$. This completes the proof of "⇒".

For t even it is proved in a similar way (without the assumption of $\mathfrak{p}_0$ not being principal) that

$$\begin{aligned} &e_4(\mathbb{Q}(i, \sqrt{d})) = t - 1 \\ \Leftrightarrow\ \ &([\mathfrak{p}_1 \cdots \mathfrak{p}_s]_{K_1}, [\mathfrak{q}_0\mathfrak{q}_1 \cdots \mathfrak{q}_s]_{K_2}) \text{ is a square in } \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2) \text{ of order 2.} \end{aligned}$$

We now go through the cases of the theorem:

(1) $q_1 \equiv \cdots \equiv q_t \equiv 7 \pmod 8$: Let t be odd. If $\mathfrak{p}_0$ is a principal ideal, we are done; so assume that $\mathfrak{p}_0$ is not a principal ideal, i.e. $\mathrm{ord}([\mathfrak{p}_0]_{K_1}) = 2$. We just have to note that

$$\chi_j^{(1)}([\mathfrak{p}_0]_{K_1}^{\mathrm{s}}) = \left(\frac{-q_j}{2}\right) = 1, \quad j = 1, \ldots, t.$$

Let t be even. We have $\mathrm{ord}([\mathfrak{q}_0]_{K_1}) = 2$ since $\mathfrak{q}_1 \cdots \mathfrak{q}_t$ is the only non-trivial principal ideal in $\{\mathfrak{q}_0^{x_0}\mathfrak{q}_1^{x_1} \cdots \mathfrak{q}_t^{x_t} \mid x_i \in \{0, 1\}\}$. Note that

$$\chi_j^{(2)}([\mathfrak{q}_0]_{K_1}) = \left(\frac{-q_j}{2}\right) = 1, \quad j = 1, \ldots, t.$$

(2) $q_1 \equiv \cdots \equiv q_t \equiv 3 \pmod 8$: Let t be odd. If $\mathfrak{p}_0$ is a principal ideal, we are done; so we can assume that $\mathrm{ord}([\mathfrak{p}_0]_{K_1}) = 2$. Note that $[\mathfrak{p}_0]_{K_1} = [\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_t]_{K_1}$. For $j = 1, \ldots, t$ we have

$$\begin{aligned} \chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_t]_{K_1}^{\mathrm{s}}) &= \prod_{\substack{i=0 \\ i \neq j}}^{t} \chi_j^{(1)}([\mathfrak{p}_i]_{K_1}^{\mathrm{s}}) \cdot \prod_{\substack{k=0 \\ k \neq j}}^{t} \chi_k^{(1)}([\mathfrak{p}_j]_{K_1}^{\mathrm{s}}) \\ &= \left(\frac{-q_j}{2}\right) \prod_{\substack{i=1 \\ i \neq j}}^{t} \left(\frac{-q_j}{q_i}\right) \cdot \left(\frac{-4}{q_j}\right) \prod_{\substack{k=1 \\ k \neq j}}^{t} \left(\frac{-q_k}{q_j}\right) \\ &= (-1) \cdot (-1) \cdot (-1)^{t-1} \cdot (-1)^{t-1} \prod_{\substack{m=1 \\ m \neq j}}^{t} \left(\left(\frac{q_j}{q_m}\right)\left(\frac{q_m}{q_j}\right)\right) \\ &= (-1) \cdot (-1) \cdot (-1)^{t-1} \cdot (-1)^{t-1} \cdot (-1)^{t-1} = 1 \end{aligned}$$

and

$$\chi_j^{(2)}([\mathfrak{q}_1\cdots\mathfrak{q}_t]_{K_2}) = \chi_j^{(2)}(1) = 1,$$

as required.

Let t be even. As

$$\begin{aligned}
\chi_1^{(2)}([\mathfrak{q}_0\mathfrak{q}_1\cdots\mathfrak{q}_t]_{K_2}) &= \prod_{\substack{i=0\\ i\neq 1}}^{t} \chi_1^{(2)}([\mathfrak{q}_i]_{K_2}) \cdot \prod_{\substack{k=0\\ k\neq 1}}^{t} \chi_k^{(2)}([\mathfrak{q}_1]_{K_1})\\
&= \left(\frac{-q_1}{2}\right)\prod_{i=2}^{t}\left(\frac{-q_1}{q_i}\right)\cdot\left(\frac{-4}{q_1}\right)\prod_{k=2}^{t}\left(\frac{-q_k}{q_1}\right)\\
&= (-1)\cdot(-1)\cdot(-1)^{t-1}\cdot(-1)^{t-1}\prod_{m=2}^{t}\left(\left(\frac{q_1}{q_m}\right)\left(\frac{q_m}{q_1}\right)\right)\\
&= (-1)\cdot(-1)\cdot(-1)^{t-1}\cdot(-1)^{t-1}\cdot(-1)^{t-1} = -1,
\end{aligned}$$

$[\mathfrak{q}_0\mathfrak{q}_1\cdots\mathfrak{q}_t]_{K_2}$ is not a square in $\mathrm{Cl}(K_2)$, as required.

(3) $q_1 \equiv \cdots \equiv q_s \equiv 3,\ q_{s+1} \equiv \cdots \equiv q_t \equiv 7 \pmod 8$ and $0 < s < t$: First note that $\mathrm{ord}([\mathfrak{q}_1\cdots\mathfrak{q}_s]_{K_2}) = 2$ for t odd and that $\mathrm{ord}([\mathfrak{q}_0\mathfrak{q}_1\cdots\mathfrak{q}_s]_{K_2}) = 2$ for t even. Let $j \in \{1,\ldots,s\}$. For t odd we have

$$\begin{aligned}
&\chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1\cdots\mathfrak{p}_s]^{\mathrm{s}}_{K_1})\\
&\quad= \prod_{\substack{i=0\\ i\neq j}}^{s} \chi_j^{(1)}([\mathfrak{p}_i]^{\mathrm{s}}_{K_1}) \cdot \prod_{\substack{k=0\\ k\neq j}}^{t} \chi_k^{(1)}([\mathfrak{p}_j]^{\mathrm{s}}_{K_1})\\
&\quad= \left(\frac{-q_j}{2}\right)\prod_{\substack{i=1\\ i\neq j}}^{s}\left(\frac{-q_j}{q_i}\right)\cdot\left(\frac{-4}{q_j}\right)\prod_{\substack{k=1\\ k\neq j}}^{t}\left(\frac{-q_k}{q_j}\right)\\
&\quad= (-1)\cdot(-1)\cdot(-1)^{s-1}\cdot(-1)^{t-1}\prod_{\substack{m=1\\ m\neq j}}^{s}\left(\left(\frac{q_j}{q_m}\right)\left(\frac{q_m}{q_j}\right)\right)\cdot\left(\frac{q_{s+1}\cdots q_t}{q_j}\right)\\
&\quad= (-1)^{t-1}\left(\frac{q_{s+1}\cdots q_t}{q_j}\right).
\end{aligned}$$

Similar computations show that

$$\chi_j^{(2)}([\mathfrak{q}_1\cdots\mathfrak{q}_s]_{K_2}) = (-1)^{t-1}\left(\frac{q_{s+1}\cdots q_t}{q_j}\right) \quad \text{for } t \text{ odd}$$

and

$$\chi_j^{(1)}([\mathfrak{p}_1\cdots\mathfrak{p}_s]^{\mathrm{s}}_{K_1}) = \chi_j^{(2)}([\mathfrak{q}_0\mathfrak{q}_1\cdots\mathfrak{q}_s]_{K_2}) = (-1)^{t-1}\left(\frac{q_{s+1}\cdots q_t}{q_j}\right) \quad \text{for } t \text{ even.}$$

Finally, let $j \in \{s+1, \ldots, t\}$. Then it is easily seen that

$$\chi_j^{(1)}([\mathfrak{p}_0\mathfrak{p}_1\cdots\mathfrak{p}_s]^{\mathrm{s}}_{K_1}) = \chi_j^{(2)}([\mathfrak{q}_1\cdots\mathfrak{q}_s]_{K_2}) = \left(\frac{q_1\cdots q_s}{q_j}\right) \quad \text{for } t \text{ odd}$$

and

$$\chi_j^{(1)}([\mathfrak{p}_1\cdots\mathfrak{p}_s]^{\mathrm{s}}_{K_1}) = \chi_j^{(2)}([\mathfrak{q}_0\mathfrak{q}_1\cdots\mathfrak{q}_s]_{K_2}) = \left(\frac{q_1\cdots q_s}{q_j}\right) \quad \text{for } t \text{ even.}$$

The assertion in (3) of the theorem follows from this. This completes the proof of the theorem. ∎

Before we give an application of Theorem 3, we state the following lemma (whose combinatorial proof we skip).

Lemma 5. *Let $a, b \in \mathbb{N}_0$. Consider the $(2a+2b+1)\times(2a+2b+1)$ matrix over $\mathbb{F}_2$:*

$$M = \begin{bmatrix} 0 & 1 & \cdots & \cdots & \cdots & 1 \\ 1 & & & | & & \\ \vdots & & M_{11} & | & M_{12} & \\ \vdots & - & - & + & - & - \\ \vdots & & M_{21} & | & M_{22} & \\ 1 & & & | & & \end{bmatrix}$$

where M_{11} is a $2a \times 2a$ matrix, M_{12} is a $2a \times 2b$ matrix, M_{21} is a $2b \times 2a$ matrix and M_{22} is a $2b \times 2b$ matrix; these four matrices are constructed as block matrices built of 2×2 matrices in the following way:

M_{11} has the form

$$\begin{bmatrix} \begin{bmatrix} * & x_1 \\ x_1 & * \end{bmatrix} & & \\ & \ddots & \\ & & \begin{bmatrix} * & x_a \\ x_a & * \end{bmatrix} \end{bmatrix}$$

with $\left[\begin{smallmatrix} * & x_i \\ x_i & * \end{smallmatrix}\right]$-blocks on the main diagonal, $x_i \in \mathbb{F}_2$, and all other blocks of the form $\left[\begin{smallmatrix} y & y+1 \\ y+1 & y \end{smallmatrix}\right]$, $y \in \mathbb{F}_2$ (with possibly different y).

Every block of M_{12} or of M_{21} is of the form $\left[\begin{smallmatrix} z & z \\ z & z \end{smallmatrix}\right]$, $z \in \mathbb{F}_2$ (with varying z).

M_{22} comes in two types:

(I) *Every block on the main diagonal of M_{22} is of the form $\left[\begin{smallmatrix} * & x \\ x & * \end{smallmatrix}\right]$, $x \in \mathbb{F}_2$ (with varying x), and all other blocks are of the form $\left[\begin{smallmatrix} y & y \\ y & y \end{smallmatrix}\right]$, $y \in \mathbb{F}_2$ (with varying y).*

(II) *Every block on the main diagonal of* M_{22} *is of the form* $\left[\begin{smallmatrix} * & x \\ x & * \end{smallmatrix}\right]$, $x \in \mathbb{F}_2$ (*with varying* x), *and all other blocks are of the form* $\left[\begin{smallmatrix} z & z+1 \\ z+1 & z \end{smallmatrix}\right]$, $z \in \mathbb{F}_2$ (*with varying* z).

Finally, *and in all cases*, *the entries on the main diagonal of* M *are chosen such that all column sums of* M *are* 0.

Then the following statements hold:

(i) *If* a *is even and if* M_{22} *is of type* (I), *then* M *has maximal* $\mathbb{F}_2$*-rank*, *namely* $2a+2b$.

(ii) *If both* a *and* b *are even and if* M_{22} *is of type* (II), *then* M *has maximal* $\mathbb{F}_2$*-rank*, $2a+2b$.

We can now give the promised application of Theorem 3 (and Theorem 4, for the claim about 2-class groups):

Theorem 10. *Let* $a, b \in \mathbb{N}_0$ *and let* a *be even. Let* $q \equiv 3 \pmod 4$ *and* $p_1 \equiv \cdots \equiv p_a \equiv p_1' \equiv \cdots \equiv p_b' \equiv 1 \pmod 8$ *be prime numbers such that*:

(1) $\left(\frac{q}{p_1}\right) = \cdots = \left(\frac{q}{p_a}\right) = \left(\frac{q}{p_1'}\right) = \cdots = \left(\frac{q}{p_b'}\right) = -1$;

(2) $\left(\frac{p_i}{p_j}\right) = -1$ *for* $i, j \in \{1, \ldots, a\}$, $i \neq j$;

(3) $\left(\frac{p_i}{p_u'}\right) = 1$ *for* $i \in \{1, \ldots, a\}, u \in \{1, \ldots, b\}$;

(4) *for* $u, v \in \{1, \ldots, b\}, u \neq v$, *either*

(i) *all the Legendre symbols* $\left(\frac{p_u'}{p_v'}\right)$ *have the value* 1, *or*

(ii) b *is even and all the Legendre symbols* $\left(\frac{p_u'}{p_v'}\right)$ *have the value* -1.

Then

$$i \in N_{\mathbb{Q}(i,\sqrt{qp_1\cdots p_a p_1'\cdots p_b'})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{qp_1\cdots p_a p_1'\cdots p_b'})})$$

and the 2*-class group* $\mathrm{Cl}_2(\mathbb{Q}(i, \sqrt{qp_1\cdots p_a p_1'\cdots p_b'}))$ *is elementary abelian.* (*And one of the equations* $x^2 - qp_1\cdots p_a p_1'\cdots p_b' y^2 = \pm 2$ *is solvable in* $\mathbb{Z}$.)

Proof. We can write $p_i = \pi_i\overline{\pi}_i$ and $p_u' = \pi_u'\overline{\pi}_u'$ where $(\pi_i), (\overline{\pi}_i), (\pi_u'), (\overline{\pi}_u')$ are prime ideals of $K := \mathbb{Q}(i)$ and $\pi_i \equiv \pi_i' \equiv \pi_u \equiv \pi_u' \equiv 1 \pmod 4$. Then

$$\alpha = d = q\pi_1\overline{\pi}_1\cdots\pi_a\overline{\pi}_a\pi_1'\overline{\pi}_1'\cdots\pi_b'\overline{\pi}_b'.$$

Note that for $\gamma \in \{q, \pi_1, \overline{\pi}_1, \ldots, \pi_a, \overline{\pi}_a, \pi_1', \overline{\pi}_1', \ldots, \pi_b', \overline{\pi}_b'\}$, the prime ideal $(1+i)$ and hence every prime of K different from (γ) is unramified in the extension $K(\sqrt{\gamma})/K$. So by Theorem 3 it is enough to show that the (right) Rédei matrix $M_{\mathbb{Q}(i,\sqrt{\alpha})/\mathbb{Q}(i)}$ has maximal rank; this follows immediately from Lemmas 4 and 5. ∎

We now investigate the case where $(\alpha) = (\pi)$ is a prime of $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. By the above, we only need to consider the split case, i.e. π of the form

$\pi = a + bi$, $a, b \in \mathbb{Z}$, where $N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) = a^2 + b^2 \equiv 1 \pmod 8$ is a prime number; hence $4 \mid ab$.

The following lemma comes from the unpublished paper [9].

Lemma 6. *Let $\pi = a + bi$ be a prime of $\mathbb{Z}[i]$ with $2 \mid a$ and $a + b \equiv \pm 1$ $\pmod 8$. Then*

$$4 \mid h(\mathrm{Cl}(\mathbb{Q}(i, \sqrt{\pi}))) \Leftrightarrow 8 \mid a.$$

Proof. For the convenience of the reader, we sketch the proof from [9]. Put $K := \mathbb{Q}(i, \sqrt{\pi})$ and $L := \mathbb{Q}(\sqrt{i}, \sqrt{\pi})$. As L/K is unramified, we have $2 \mid h(K)$. Since also the 2-class group $\mathrm{Cl}_2(\mathbb{Q}(i, \sqrt{\pi}))$ is cyclic, we have

$$4 \mid h(K) \Leftrightarrow 2 \mid h(L).$$

By the ambiguous class number formula, applied to the extension L/F where $F = \mathbb{Q}(\sqrt{i})$, we have

$$2 \mid h(L) \Leftrightarrow [\mathcal{O}_F^* : N_{L/F}(L^*) \cap \mathcal{O}_F^*] = 1$$

since $h(F)$ is odd. A calculation of this index gives the result. ∎

Theorem 11. *Let $\pi = a + bi$ be a prime of $\mathbb{Z}[i]$.*

(i) *If $4 \mid b$, then $i \in N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$.*

(ii) *If $4 \mid a$ and $a + b \equiv \pm 3 \pmod 8$, then $i \in N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$.*

(iii) *If $4 \parallel a$ and $a + b \equiv \pm 1 \pmod 8$, then $i \notin N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$.*

Proof. (i) By [5], (π) is the only ramified prime ideal of the extension $\mathbb{Q}(i, \sqrt{\pi})/\mathbb{Q}(i)$. Hence the assertion follows from Proposition 1.

(ii) By [5], there are exactly two ramified primes of $\mathbb{Q}(i, \sqrt{\pi})/\mathbb{Q}(i)$, namely (π) and $(1 + i)$. Let $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(i,\sqrt{\pi})}$ be the prime ideal above $(1 + i)$. By Proposition 1, it is enough to show that $\mathfrak{p}$ is not principal.

As $(1+i)$ is inert in $\mathbb{Q}(i, \sqrt{i\pi})$ (by [5]), $\mathfrak{p}$ is inert in $L := \mathbb{Q}(\sqrt{i}, \sqrt{\pi})$. Since the extension $L/\mathbb{Q}(i, \sqrt{\pi})$ is unramified, it follows from class field theory that $\mathfrak{p}$ is not principal.

(iii) As $2 \parallel h(\mathrm{Cl}(\mathbb{Q}(i, \sqrt{\pi})))$ (by Lemma 6) and $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})/\mathbb{Q}(i, \sqrt{\pi})$ is unramified, $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})$ must be the 2-class field of $\mathbb{Q}(i, \sqrt{\pi})$. By [5], $(1 + i)$ splits completely in $\mathbb{Q}(i, \sqrt{i\pi})$ and $(1 + i)$ is ramified in $\mathbb{Q}(i, \sqrt{\pi})$. Hence the prime $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(i,\sqrt{\pi})}$ above $(1 + i)$ splits completely in $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})$; so $\mathfrak{p}$ must be principal. Since $N_{\mathbb{Q}(i)/\mathbb{Q}}(\pi) \equiv 1 \pmod 8$, the prime (π) splits completely in $\mathbb{Q}(\sqrt{i})$; hence the prime $\mathfrak{p}_1 \subseteq \mathcal{O}_{\mathbb{Q}(i,\sqrt{\pi})}$ above (π) splits completely in $\mathbb{Q}(\sqrt{i}, \sqrt{\pi})$; so $\mathfrak{p}_1$ is also principal. The theorem now follows from Proposition 1. ∎

Remark 6. In the remaining case, $8 \mid a$ and $a + b \equiv \pm 1 \pmod 8$, there seems to be no simple answer. For example, for some π of this kind it *is* true that $i \in N_{\mathbb{Q}(i,\sqrt{\pi})/\mathbb{Q}(i)}(\mathcal{O}^*_{\mathbb{Q}(i,\sqrt{\pi})})$ and for some π this is false.

References

[1] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, I*, Ann. Inst. Fourier (Grenoble) 23 (1973), no. 3, 1–48.

[2] —, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, II*, ibid., no. 4, 1–44.

[3] —, *Sur la norme du groupe des unités d'extensions quadratiques relatives*, Acta Arith. 61 (1992), 307–317.

[4] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.

[5] D. Hilbert, *Über den Dirichletschen biquadratischen Zahlkörper*, Math. Ann. 45 (1894), 309–340.

[6] L. Holzer, *Zahlentheorie*, *II*, Teubner, Leipzig, 1958-1959.

[7] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. 10 (1956), 65–85.

[8] S. Lang, *Cyclotomic Fields II*, Springer, 1980.

[9] F. Lemmermeyer, *Class Number Parity*, unpublished.

[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, 1989.

[11] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, Leipzig, 1929.

[12] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1934), 69–74.

[13] H. Reichardt, *Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper*, ibid., 75–82.

[14] B. L. van der Waerden, *Algebra*, Zweiter Teil, Springer, 1967.

[15] D. Zagier, *Zetafunktionen und quadratische Körper*, Springer, 1981.

Department of Mathematics
University of Copenhagen
2100 Copenhagen, Denmark
E-mail: tommy@math.ku.dk

Received on 7.6.2004
and in revised form on 31.1.2005 (4783)