JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Henri Cohen, Francisco Diaz Y Diaz, Michel Olivier

Counting cyclic quartic extensions of a number field

Tome 17, n° 2 (2005), p. 475-510.

<http://jtnb.cedram.org/item?id=JTNB_2005___17_2_475_0>

Journal de Théorie des Nombres
de Bordeaux **17** (2005), 475–510

Counting cyclic quartic extensions of a number field

par Henri COHEN, Francisco DIAZ Y DIAZ et Michel OLIVIER

Résumé. Nous donnons des formules asymptotiques pour le nombre d'extensions cycliques quartiques d'un corps de nombres général.

Abstract. In this paper, we give asymptotic formulas for the number of cyclic quartic extensions of a number field.

1. Galois, Kummer, and Hecke Theory

1.1. Introduction. Let K be a number field, fixed once and for all, and let G be a transitive subgroup of the symmetric group S_n on n letters. The *inverse problem of Galois theory* asks whether there exists an extension L/K of degree n such that the Galois group of the Galois closure of L is isomorphic to G. This problem is far from being solved, although great progress has been made by Matzat and his school, and hopes have been raised by Grothendieck's theory of dessins d'enfants. For specific groups G we can even ask for the *number* $N_{K,n}(G,X)$ of such extensions L/K up to K-isomorphism, such that the norm of the discriminant of L/K is at most equal to X, at least in an asymptotic sense. A general conjecture due to Malle (see [12] and [13]) states that there should exist constants $a_K(G)$, $b_K(G)$, and $c_K(G)$ such that

$$N_{K,n}(G,X) \sim c_K(G) X^{a_K(G)} \log(X)^{b_K(G)-1} ,$$

and gives formulas for the constants $a_K(G)$ and $b_K(G)$ (in [9], it is shown that the formula for $b_K(G)$ cannot be correct, but the conjecture is still believed to hold with corrected values). For a general base field K this conjecture is known to be true in a number of cases, and in particular thanks to the work of Wright [14], in the case of Abelian extensions, and the constants $a_K(G)$ and $b_K(G)$ agree with the predictions. Unfortunately it is very difficult to deduce from [14] the explicit value of the constant $c_K(G)$ (which is not given by Malle's conjecture), so all the subsequent work on the subject has been done independently of Wright's. When the

Manuscrit reçu le 26 mai 2005.

base field is $K = \mathbb{Q}$, the result is known in general: after work of many authors, Mäki in [10] and [11] gives the value of $c_{\mathbb{Q}}(G)$ for all Abelian groups G when the base field is $\mathbb{Q}$. On the other hand, for a general base field K and Abelian group G, the only known results are due to the authors, except for $G = C_2$ for which the result can be deduced from [8]: $G = C_\ell$ for prime ℓ (see [4] and [5]), $G = V_4 = C_2 \times C_2$ (see [6]), and $G = C_4$, which is the object of the present paper. Note that groups such as $G = C_n$ with *squarefree* n can be treated quite easily using the methods of [4] and [5], but the formulas are so complicated that there is not much point in doing so. Thus the main difficulty in the C_4 case is the fact that 4 is *not* squarefree. As in the C_ℓ case, the main tool that we need is simple Galois and Kummer theory, but we will also need a little local class field theory.

1.2. Galois and Kummer Theory. We first consider the Galois situation. Let L/K be a C_4-extension. Then there exists a unique quadratic subextension k/K. We will write $k = K(\sqrt{D})$ where for the moment D is an arbitrary element of K^* generating k/K. Then $L = k(\sqrt{\alpha})$ for some $\alpha \in k^*$, and it is well known and easy to see that a necessary and sufficient condition for L/K to be a C_4-extension is that $\mathcal{N}_{k/K}(\alpha) = Dz^2$ for some $z \in K$. Writing $\alpha = x + y\sqrt{D}$, it is clear that this immediately implies that D is a sum of two squares in K. Conversely, if $D = m^2 + n^2$ in K, then $\omega = \sqrt{D}(m + \sqrt{D})$ is such that $\omega \in k^*$ and $\mathcal{N}_{k/K}(\omega) = Dn^2$, hence $L = k(\sqrt{\omega})$ defines a C_4-extension of K. In other words, we have shown the well known result that a quadratic extension k/K can be embedded in a C_4-extension if and only if its discriminant is a sum of two squares.

In a large part of this paper, we fix the intermediate quadratic extension k/K with $k = K(\sqrt{D})$. We denote by τ the generator of the Galois group of k/K, by $\mathfrak{d} = \mathfrak{d}(k/K)$ the relative ideal discriminant, by $\mathfrak{D} = \mathfrak{D}(k/K)$ the different of k/K, and by T the set of prime ideals of K dividing $\mathfrak{d}$ (i.e., which ramify in k/K). Finally we fix once and for all an element $\omega \in k^*$ such that $\mathcal{N}_{k/K}(\omega) = Dn^2$ for some $n \in K$ (not necessarily the one given above).

We will constantly use the following lemma whose trivial proof (for example using Hilbert 90) is left to the reader.

Lemma 1.1. *Let $\alpha \in k^*$.*

(1) *$\mathcal{N}_{k/K}(\alpha)$ is a square in K if and only if there exists $z \in K$ and $\gamma \in k$ such that $\alpha = z\gamma^2$.*
(2) *$\mathcal{N}_{k/K}(\alpha)$ is equal to D times a square in K if and only if there exists $t \in K$ and $\gamma \in k$ such that $\alpha = \omega t\gamma^2$.*

Thus α defines a C_4-extension if and only if $\alpha = \omega t\gamma^2$ for some $t \in K^*$; since α is only defined up to squares, we may in fact assume that

$\alpha = \omega t$. Furthermore ωt and $\omega t'$ define K-isomorphic C_4-extensions if and only if they define k-isomorphic quadratic extensions, hence if and only if $t'/t \in k^{*2}$. Since $t'/t \in K^*$, this means that $t'/t \in K^{*2} \cup DK^{*2}$.

Thus, if we consider extensions $L = k(\sqrt{\omega t})$ for $t \in K^*/K^{*2}$ (note that the unit class must *not* be excluded), we will obtain exactly twice all C_4-extensions of K up to isomorphism. We have thus shown:

Proposition 1.2. *Let $k = K(\sqrt{D})$ be a quadratic extension of K which is embeddable in a C_4-extension, in other words such that there exists $\omega \in k^*$ such that $\mathcal{N}_{k/K}(\omega) = Dn^2$ for some $n \in K^*$. Then the set of isomorphism classes of C_4-extensions L/K containing k/K is in a noncanonical one-to-two correspondence with the group K^*/K^{*2}. The isomorphism class of C_4-extensions corresponding to $\overline{t} \in K^*/K^{*2}$ is $k(\sqrt{\omega t})$, and this is the same extension as the one corresponding to $\overline{tD}$.*

Definition. Recall that T is the set of prime ideals of K ramified in k/K. We denote by $< T >$ the subgroup of the group of fractional ideals of K generated by the elements of T.

(1) The T-class group $Cl_T(K)$ is the quotient group of the group of fractional ideals by the subgroup of ideals of the form $\beta\mathfrak{b}$, where $\beta \in K^*$ and $\mathfrak{b} \in < T >$. In other words $Cl_T(K) = Cl(K)/\overline{< T >}$, the quotient of the ordinary class group by the subgroup generated by the ideal classes of elements of T.

(2) The T-Selmer group $S_T(K)$ of K is the set of classes of elements $u \in K^*$ such that $u\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{b}$ for some ideal $\mathfrak{q}$ of K and some ideal $\mathfrak{b} \in < T >$, modulo squares of elements of K^*

We will also use this definition either for $T = \emptyset$, in which case we recover the notions of ordinary class and Selmer groups, which we will denote respectively by $Cl(K)$ and $S(K)$.

We will need the following lemma, whose easy proof is left to the reader:

Lemma 1.3. *The natural map from $S(K)$ to $S(k)$ induces an isomorphism from $S_T(K)$ to $S(k)^\tau$, where as usual $S(k)^\tau$ is the subgroup of elements of $S(k)$ stable by τ.*

The following lemma is well known in the case $T = \emptyset$ (see for example [2]), and its proof is the same.

Lemma 1.4. *There exists a noncanonical one-to-one correspondence between K^*/K^{*2} and pairs $(\mathfrak{a}, \overline{u})$, where $\mathfrak{a}$ is a squarefree[1] ideal of K coprime to $\mathfrak{d}$ whose ideal class is a square in the T-class group $Cl_T(K)$, and $\overline{u} \in S_T(K)$. If $\mathfrak{a}\mathfrak{q}_0^2\mathfrak{b} = t_0\mathbb{Z}_K$ for some $\mathfrak{b} \in < T >$ and $t_0 \in K^*$, the element of K^*/K^{*2} corresponding to $(\mathfrak{a}, \overline{u})$ is the class modulo squares of $t_0 u$.*

[1] We will only use the term "squarefree" to mean integral and squarefree

Note for future reference that by the approximation theorem $\mathfrak{q}_0$ and u (but of course not t_0 in general) can be chosen coprime to $2\mathbb{Z}_K$.

1.3. Kummer and Hecke Theory. Important notation. In this paper, the notation $\mathfrak{Q}$ will be used to denote a generic fractional ideal of k which need not be the same from one line to another. In addition, we recall the following notation introduced above:

- K is a number field, the base field fixed in the whole paper.
- k is a quadratic extension of K, which will be fixed in the first three sections of the paper, $D \in K$ is an element such that $k = K(\sqrt{D})$, $\mathfrak{d}$ and $\mathfrak{D}$ are the relative discriminant and different of k/K, τ is the generator of $\mathrm{Gal}(k/K)$, and ω is an element of k^* such that $\mathcal{N}_{k/K}(\omega) = Dn^2$ for some $n \in K$.
- T is the set of prime ideals of K which ramify in k/K, in other words dividing $\mathfrak{d}$.
- L is a quartic C_4-extension of K containing k.

Definition. If $\mathfrak{M}$ is any fractional ideal of k, we denote by $s(\mathfrak{M})$ the squarefree part of $\mathfrak{M}$, i.e., the unique squarefree ideal such that $\mathfrak{M} = s(\mathfrak{M})\mathfrak{Q}^2$ for some (fractional) ideal $\mathfrak{Q}$. If $\mathfrak{M} = \alpha\mathbb{Z}_k$ for some element α, we write $s(\alpha)$ instead of $s(\alpha\mathbb{Z}_k)$.

Note the following trivial but important lemma:

Lemma 1.5. *For two squarefree ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ define*

$$\mathfrak{a}_1 \triangle \mathfrak{a}_2 = \frac{\mathfrak{a}_1\mathfrak{a}_2}{(\mathfrak{a}_1, \mathfrak{a}_2)^2} ,$$

the "symmetric difference" of $\mathfrak{a}_1$ and $\mathfrak{a}_2$. Then for any two ideals $\mathfrak{M}_1$ and $\mathfrak{M}_2$ we have $s(\mathfrak{M}_1\mathfrak{M}_2) = s(\mathfrak{M}_1) \triangle s(\mathfrak{M}_2)$.

Lemma 1.6. *Let $\mathfrak{C}$ be an ideal of k and let $\mathfrak{M}$ be a fractional ideal of k. The following two conditions are equivalent:*

(1) *There exists an ideal $\mathfrak{Q}$ of k such that $(\mathfrak{M}\mathfrak{Q}^2, \mathfrak{C}) = 1$.*
(2) *We have $(s(\mathfrak{M}), \mathfrak{C}) = 1$.*

If, in addition, $\mathfrak{M}$ comes from K (i.e., $\mathfrak{M} = \mathfrak{m}\mathbb{Z}_k$ for some ideal $\mathfrak{m}$ of K), then in (1) we may choose $\mathfrak{Q}^2$ of the form $\mathfrak{b}\mathfrak{q}^2\mathbb{Z}_k$ for $\mathfrak{q}$ an ideal of K and $\mathfrak{b} \in <T>$.

Proof. Since $\mathfrak{M} = s(\mathfrak{M})\mathfrak{Q}^2$, we have (2) $\implies$ (1). Conversely, assume (1). If $\mathfrak{P}$ is a prime ideal dividing $\mathfrak{C}$ then $v_{\mathfrak{P}}(\mathfrak{M}\mathfrak{Q}^2) = 0$ hence $v_{\mathfrak{P}}(\mathfrak{M}) \equiv 0 \pmod 2$, so $v_{\mathfrak{P}}(s(\mathfrak{M})) = 0$, proving (2).

Finally, assume that $\mathfrak{M} = \mathfrak{m}\mathbb{Z}_k$, and write $\mathfrak{m} = \mathfrak{a}\mathfrak{q}^2\mathfrak{b}$ where $\mathfrak{a}$ is squarefree coprime to $\mathfrak{d}$ and $\mathfrak{b} \in <T>$. It is clear that $s(\mathfrak{M}) = \mathfrak{a}\mathbb{Z}_k$, so $\mathfrak{a}$ is coprime to $\mathfrak{C}$ by (2), hence if we take $\mathfrak{Q} = \mathfrak{q}^{-1}\mathfrak{B}^{-1}$, where $\mathfrak{B}^2 = \mathfrak{b}\mathbb{Z}_k$, we have $\mathfrak{M}\mathfrak{Q}^2 = \mathfrak{a}\mathbb{Z}_k$, so $\mathfrak{Q}$ is suitable. □

Definition. Let $\mathfrak{C}$ be an ideal of k dividing $2\mathbb{Z}_k$.

(1) We will denote by $Q(\mathfrak{C}^2)$ the group of elements $\alpha \in k^*$ satisfying the following two conditions:
- $(s(\alpha), \mathfrak{C}) = 1$ or equivalently, by the above lemma, there exists an ideal $\mathfrak{Q}$ of k such that $(\alpha\mathfrak{Q}^2, \mathfrak{C}) = 1$.
- The multiplicative congruence $\alpha/x^2 \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ has a solution in k.

(2) We will denote by $Q_K(\mathfrak{C}^2)$ the group of elements $z \in K^*$ satisfying the following two conditions:
- There exists an ideal $\mathfrak{b} \in < T >$ such that $(z\mathfrak{b}, \mathfrak{C}) = 1$.
- The multiplicative congruence $z/x^2 \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ has a solution in k (*not* necessarily in K).

Remarks.

(1) When α (or z) is already coprime to $\mathfrak{C}$ this means that $\alpha \equiv x^2 \pmod{{}^*\mathfrak{C}^2}$ has a solution. We will see that it is essential to have also the coprimeness condition.

(2) We clearly have $Q_K(\mathfrak{C}^2) \subset Q(\mathfrak{C}^2) \cap K$, but we do *not* have equality in general, since by Lemma 1.6 if $z \in Q(\mathfrak{C}^2) \cap K$ there exists $\mathfrak{q}$ and $\mathfrak{b} \in < T >$ such that $(z\mathfrak{q}^2\mathfrak{b}, \mathfrak{C}) = 1$, not necessarily with $\mathfrak{q} = 1$. What is true by the approximation theorem is that if $z \in Q(\mathfrak{C}^2) \cap K$, there exists $n \in K^*$ such that $zn^2 \in Q_K(\mathfrak{C}^2)$.

Since $\mathfrak{C}_1 \mid \mathfrak{C}_2 \mid 2\mathbb{Z}_k$ implies trivially that $Q(\mathfrak{C}_2^2) \subset Q(\mathfrak{C}_1^2)$, the following definition is reasonable:

Definition. With the above notations, for $\alpha \in k^*$ we denote by $\mathfrak{C}(\alpha)$ the largest ideal (for divisibility) dividing $2\mathbb{Z}_k$ and such that $\alpha \in Q(\mathfrak{C}^2)$.

With these notations, we recall the following important special case of a theorem of Hecke (see for example [2], Chapter 10):

Theorem 1.7. *Let k be a number field. Then for $\alpha \in k^*$ (including $\alpha \in k^{*2}$) the relative ideal discriminant $\mathfrak{d}(k(\sqrt{\alpha})/k)$ is given by*

$$\mathfrak{d}(k(\sqrt{\alpha})/k) = \frac{4s(\alpha)}{\mathfrak{C}(\alpha)^2}\,.$$

Thanks to Proposition 1.2 and Lemma 1.4, we see that we must apply this theorem to $\alpha = t_0 u \omega$, hence must first compute $s(\alpha)$. Note that $s(\mathfrak{M})$ will usually denote the squarefree part of the ideal $\mathfrak{M}$ *in* k, even if $\mathfrak{M}$ comes from an ideal of K. It will be clear from the context when the notation is used to denote the squarefree part in K.

By definition $t_0 u\mathbb{Z}_K = \mathfrak{a}\mathfrak{q}^2\mathfrak{b}$ for some squarefree ideal $\mathfrak{a}$ coprime to $\mathfrak{d}$ and some $\mathfrak{b} \in < T >$. Since the elements of T ramify in k/K and $\mathfrak{a}$ is coprime

to $\mathfrak{d}$, it follows that $s(t_0u) = \mathfrak{a}$ (this is of course the whole point of using ideals coprime to $\mathfrak{d}$).

Let us now compute $s(\omega)$.

Lemma 1.8. *Keep the above notation. There exists a squarefree ideal $\mathfrak{a}_\omega$ of K coprime to $\mathfrak{d}$ such that $s(\omega) = \mathfrak{a}_\omega s(\mathfrak{D})$, where $\mathfrak{D} = \mathfrak{D}(k/K)$ is the different of k/K.*

Furthermore, the class of $\mathfrak{a}_\omega$ in $Cl_T(K)/Cl_T(K)^2$ is independent of ω, i.e., depends only on the extension k/K.

Notation. If β is any element such that $\mathcal{N}_{k/K}(\beta) = Dz^2$ with $z \in K^*$, we will write $\mathfrak{a}_\beta$ for the squarefree ideal of K coprime to $\mathfrak{d}$ such that $s(\beta) = \mathfrak{a}_\beta s(\mathfrak{D})$. Moreover, ideals of k will be denoted by capital gothic letters and those of K by lowercase gothic letters.

Proof. Writing $\omega\mathbb{Z}_k = s(\omega)\mathfrak{Q}^2$ and taking norms from k to K, we see that $\mathcal{N}_{k/K}(s(\omega)) = D\mathfrak{q}^2$ for some ideal $\mathfrak{q}$ of K. Since the different satisfies $\mathcal{N}_{k/K}(\mathfrak{D}) = \mathfrak{d}$ and since $D\mathbb{Z}_K = \mathfrak{d}\mathfrak{m}^2$ for some ideal $\mathfrak{m}$, it follows that $\mathcal{N}_{k/K}(s(\omega)/\mathfrak{D}) = \mathfrak{q}_1^2$ for some ideal $\mathfrak{q}_1$ of K. By Hilbert 90 for ideals, or trivially directly, this is equivalent to

$$s(\omega) = \mathfrak{D}\mathfrak{q}_2\mathfrak{Q}^2 ,$$

for some ideal $\mathfrak{q}_2$ of K (and as usual $\mathfrak{Q}$ an ideal of k). Without loss of generality we may assume that $\mathfrak{q}_2$ is squarefree in K (include all squares in $\mathfrak{Q}$) and is coprime to $\mathfrak{d}$ (include all ramified primes in $\mathfrak{Q}$). The first part of the lemma follows from the fact that $s(\omega)$ is a squarefree ideal of k.

Furthermore, since the general solution to $\mathcal{N}_{k/K}(\alpha) = Dz^2$ is $\alpha = \omega t\beta^2$, we have $\mathfrak{a}_\alpha = s(\mathfrak{a}_\omega t)$. If $t\mathbb{Z}_K = \mathfrak{a}_t\mathfrak{q}^2\mathfrak{b}$ for $\mathfrak{b} \in < T >$, by Lemma 1.5 this is therefore equal to $\mathfrak{a}_\omega \triangle \mathfrak{a}_t = \mathfrak{a}_\omega\mathfrak{a}_t/(\mathfrak{a}_\omega, \mathfrak{a}_t)^2$. Since the class of $\mathfrak{a}_t$ is clearly a square in $Cl_T(K)$, the second part of the lemma follows. □

Since $s(t_0u) = \mathfrak{a}$, Lemma 1.5 gives the following:

Corollary 1.9. *With the above notation, we have $s(\omega t_0u) = (\mathfrak{a} \triangle \mathfrak{a}_\omega)s(\mathfrak{D})$.*

Corollary 1.10. *Keep the above notation and let $L = k(\sqrt{\omega t_0u})$. The relative ideal discriminant of L/k is given by*

$$\mathfrak{d}(L/k) = \frac{4(\mathfrak{a} \triangle \mathfrak{a}_\omega)s(\mathfrak{D})}{\mathfrak{C}(\omega t_0u)^2} .$$

2. The Dirichlet Series

As usual in this kind of investigation, we set

$$\Phi_{K,4}(C_4, s) = \sum_{L/K} \frac{1}{\mathcal{N}(\mathfrak{d}(L/K))^s} ,$$

where the symbol $\mathcal{N}$ without a subscript will always indicates the absolute norm from K to $\mathbb{Q}$, and L/K ranges over K-isomorphism classes of C_4-extensions. When using the relative norm from k to K, we will always write (as above) $\mathcal{N}_{k/K}$, and when using the absolute norm from k to $\mathbb{Q}$, we will always write $\mathcal{N}_{k/\mathbb{Q}}$.

By the Galois description of C_4-extensions and the discriminant-conductor formula $\mathfrak{d}(L/K) = \mathfrak{d}(k/K)^2 \mathcal{N}_{k/K}(\mathfrak{d}(L/k))$, we can write

$$\Phi_{K,4}(C_4, s) = \frac{1}{2} \sum_{k/K} \frac{1}{\mathcal{N}(\mathfrak{d}(k/K))^{2s}} \Phi_k(s) \ ,$$

where the sum is over isomorphism classes of quadratic extensions k/K which are embeddable in a C_4-extension, and

$$\Phi_k(s) = \sum_{\substack{[L:k]=2 \\ \mathrm{Gal}(L/K) \simeq C_4}} \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{d}(L/k))^s} \ .$$

In the above, the quadratic extensions L/k are of course only taken up to k-isomorphism, and the factor $1/2$ in front comes from the fact that we have a one-to-two correspondence in Proposition 1.2.

The goal of the following sections is to study the inner Dirichlet series $\Phi_k(s)$. We will come back to the global series $\Phi_{K,4}(C_4, s)$ only in Section 4.

Thus in this section and the following, we fix a quadratic extension k of K, an element $D \in K^*$ such that $k = K(\sqrt{D})$ which is a sum of two squares in K, an element $\omega \in k^*$ of relative norm D times a square, and more generally we keep the notations of the preceding section.

To simplify notations, denote by $\mathcal{I}$ the set of squarefree ideals of K which are coprime to $\mathfrak{d}$ and whose ideal class in $Cl_T(K)$ is a square. Let $n = [K : \mathbb{Q}]$ be the absolute degree of the base field K, so that $[k : \mathbb{Q}] = 2n$. It follows from Proposition 1.2, Lemma 1.4 and Corollary 1.10 that we have:

$$\begin{aligned} \Phi_k(s) &= \sum_{\mathfrak{a} \in \mathcal{I}} \sum_{\overline{u} \in S_T(K)} \mathcal{N}_{k/\mathbb{Q}}(4(\mathfrak{a} \triangle \mathfrak{a}_\omega) s(\mathfrak{D}) / \mathfrak{C}(\omega t_0 u)^2)^{-s} \\ &= \frac{\mathcal{N}(s(\mathfrak{d}))^{-s}}{4^{2ns}} \sum_{\substack{\mathfrak{C} | 2\mathbb{Z}_k \\ (\mathfrak{C}, s(\mathfrak{D}))=1}} \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s} \sum_{\substack{\mathfrak{a} \in \mathcal{I} \\ (\mathfrak{a} \triangle \mathfrak{a}_\omega, \mathfrak{C})=1}} \frac{g_{t_0}(\mathfrak{C})}{\mathcal{N}(\mathfrak{a} \triangle \mathfrak{a}_\omega)^{2s}} \ , \end{aligned}$$

where

$$g_{t_0}(\mathfrak{C}) = \sum_{\substack{\overline{u} \in S_T(K) \\ \mathfrak{C}(\omega t_0 u) = \mathfrak{C}}} 1 \ .$$

(We have used the trivial fact that $\mathcal{N}_{k/K}(s(\mathfrak{D})) = s(\mathfrak{d})$, where here $s(\mathfrak{d})$ of course denotes the squarefree part of $\mathfrak{d}$ in K).

For $\mathfrak{C}$ coprime to $s(\mathfrak{D})$ and to $\mathfrak{a} \triangle \mathfrak{a}_\omega$ (in other words to $s(\omega t_0 u)$), set

$$f_{t_0}(\mathfrak{C}) = \sum_{\substack{\overline{u} \in S_T(K) \\ \mathfrak{C} | \mathfrak{C}(\omega t_0 u)}} 1 = \sum_{\substack{\overline{u} \in S_T(K) \\ \omega t_0 u \in Q(\mathfrak{C}^2)}} 1 \, .$$

In the above notations g_{t_0} and f_{t_0}, we do not write the explicit dependence on $\mathfrak{a}$.

We clearly have

$$f_{t_0}(\mathfrak{C}) = \sum_{\mathfrak{C} | \mathcal{D} | 2} g_{t_0}(\mathcal{D}) \, ,$$

where we take only the $\mathcal{D}$ coprime to $s(\mathfrak{D})$ and to $\mathfrak{a} \triangle \mathfrak{a}_\omega$. Thus, by a form of the Möbius inversion formula we deduce that

$$g_{t_0}(\mathfrak{C}) = \sum_{\mathfrak{C} | \mathcal{D} | 2} \mu_K(\mathcal{D}/\mathfrak{C}) f_{t_0}(\mathcal{D})$$

(same restrictions on $\mathcal{D}$), where μ_K is the Möbius function on ideals of K. It follows that

$$\begin{aligned} \Phi_k(s) &= \frac{\mathcal{N}(s(\mathfrak{d}))^{-s}}{4^{2ns}} \sum_{\substack{\mathcal{D} | 2\mathbb{Z}_k \\ (\mathcal{D}, s(\mathfrak{D}))=1}} \sum_{\mathfrak{C} | \mathcal{D}} \mu_K(\mathcal{D}/\mathfrak{C}) \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s} \sum_{\substack{\mathfrak{a} \in \mathcal{I} \\ (\mathfrak{a} \triangle \mathfrak{a}_\omega, \mathcal{D})=1}} \frac{f_{t_0}(\mathcal{D})}{\mathcal{N}(\mathfrak{a} \triangle \mathfrak{a}_\omega)^{2s}} \\ &= \frac{\mathcal{N}(s(\mathfrak{d}))^{-s}}{4^{2ns}} \times \\ &\qquad \sum_{\substack{\mathfrak{C} | 2\mathbb{Z}_k \\ (\mathfrak{C}, s(\mathfrak{D}))=1}} \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s} \prod_{\mathfrak{P} | \mathfrak{C}} \left(1 - \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{P})^{2s}}\right) \sum_{\substack{\mathfrak{a} \in \mathcal{I} \\ (\mathfrak{a} \triangle \mathfrak{a}_\omega, \mathfrak{C})=1}} \frac{f_{t_0}(\mathfrak{C})}{\mathcal{N}(\mathfrak{a} \triangle \mathfrak{a}_\omega)^{2s}} \, . \end{aligned}$$

To compute $f_{t_0}(\mathfrak{C})$, we first need the following definitions and notations.

Definition. Let $\mathfrak{C}$ be an ideal of k dividing $2\mathbb{Z}_k$, and set $\mathfrak{c} = \mathfrak{C}^2 \cap K$.

(1) We define $Cl_{T,\mathfrak{C}^2}(K)$ as the quotient group of the group of fractional ideals of K coprime to $\mathfrak{c}$ by the subgroup of ideals of the form $z\mathfrak{b}$ which are coprime to $\mathfrak{c}$, where $\mathfrak{b} \in < T >$ and $z \in Q_K(\mathfrak{C}^2)$ (see Definition 1.3).

(2) We define $S_{T,\mathfrak{C}^2}(K)$ as the set of elements $\overline{u} \in S_T(K)$ such that $u \in Q_K(\mathfrak{C}^2)$ for some lift u (hence for all lifts u such that there exists $\mathfrak{b} \in < T >$ with $(u\mathfrak{b}, \mathfrak{C}) = 1$).

Note the important fact that although the elements z and u are in the base field K, the congruences defining $Q_K(\mathfrak{C}^2)$ are still in k and not in K.

Definition. Let $\mathfrak{C}$ be an ideal dividing $2\mathbb{Z}_k$ and coprime to $s(\mathfrak{D})$.

(1) We will say that $\mathfrak{C}$ satisfies condition $(*)$ if there exists $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ such that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square in K.

(2) Let $\mathfrak{a}$ be an ideal of K. We will say that $\mathfrak{a}$ satisfies condition $(**)_{\mathfrak{C}^2}$ if $\mathfrak{a}$ is squarefree and coprime to $\mathfrak{d}$, and if there exists $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ with $\mathcal{N}_{k/K}(\beta)$ equal to D times a square such that $(\mathfrak{a} \triangle \mathfrak{a}_\omega)s(\mathfrak{D}) = \beta\mathfrak{Q}^2$ (or, equivalently, $s(\beta) = (\mathfrak{a} \triangle \mathfrak{a}_\omega)s(\mathfrak{D}) = s(\omega\mathfrak{a})$).

Lemma 2.1. (1) *If $\mathfrak{a}$ satisfies condition $(**)_{\mathfrak{C}^2}$, then $\mathfrak{a} \triangle \mathfrak{a}_\omega$ is coprime to $\mathfrak{c}$ (or, equivalently, to $\mathfrak{C}$).*

(2) *If $\mathfrak{a}$ and $\mathfrak{a}_0$ satisfy condition $(**)_{\mathfrak{C}^2}$, then $\mathfrak{a}/\mathfrak{a}_0$ is coprime to $\mathfrak{c}$.*

Proof. (1). Let $\mathfrak{P}$ be a prime ideal of k dividing $\mathfrak{C}$. Then by assumption $v_{\mathfrak{P}}(s(\mathfrak{D})) = 0$ and $v_{\mathfrak{P}}(\beta) = 0$ for $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$. Thus condition $(**)_{\mathfrak{C}^2}$ implies that $v_{\mathfrak{P}}(\mathfrak{a} \triangle \mathfrak{a}_\omega) \equiv 0 \pmod 2$. Since $\mathfrak{a} \triangle \mathfrak{a}_\omega$ is squarefree and coprime to $\mathfrak{d}$, its extension to k is also squarefree so that in fact $v_{\mathfrak{P}}(\mathfrak{a} \triangle \mathfrak{a}_\omega) = 0$, proving (1).

(2). Assume that $s(\omega\mathfrak{a}_0) = s(\beta_0)$ and $s(\omega\mathfrak{a}) = s(\beta)$ with β_0 and β as above. Including the implicit ideals $\mathfrak{Q}^2$ of k and dividing, this implies that $(\mathfrak{a}/\mathfrak{a}_0)\mathbb{Z}_k = (\beta/\beta_0)\mathfrak{Q}^2$. As in (1), if $\mathfrak{P}$ is an ideal dividing $\mathfrak{C}$, we have $v_{\mathfrak{P}}(\mathfrak{a}/\mathfrak{a}_0) \equiv 0 \pmod 2$. Since $\mathfrak{a}$ and $\mathfrak{a}_0$ are squarefree and coprime to $\mathfrak{d}$, we have $v_{\mathfrak{P}}(\mathfrak{a}/\mathfrak{a}_0) \in \{-1, 0, 1\}$, hence $v_{\mathfrak{P}}(\mathfrak{a}/\mathfrak{a}_0) = 0$ as claimed. □

Proposition 2.2. *Fix an ideal $\mathfrak{C}$ dividing $2\mathbb{Z}_k$, let $\mathfrak{a}$ be an ideal of K and let t_0 be as above.*

(1) *We have $f_{t_0}(\mathfrak{C}) \neq 0$ if and only if $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$.*

(2) *There exists an ideal $\mathfrak{a}_0$ satisfying $(**)_{\mathfrak{C}^2}$ if and only if $\mathfrak{C}$ satisfies condition $(*)$. If $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ is such that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square in K, we may choose $\mathfrak{a}_0 = \mathfrak{a}_\beta \triangle \mathfrak{a}_\omega$.*

(3) *Let $\mathfrak{a}_0$ be some ideal satisfying $(**)_{\mathfrak{C}^2}$. Then $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$ if and only if the class of $\mathfrak{a}/\mathfrak{a}_0$ is a square in $Cl_{T,\mathfrak{C}^2}(K)$ or, equivalently, if the class of $(\mathfrak{a} \triangle \mathfrak{a}_\omega)/(\mathfrak{a}_0 \triangle \mathfrak{a}_\omega)$ is a square in $Cl_{T,\mathfrak{C}^2}(K)$.*

(4) *The ideal $\mathfrak{a}$ satisfies $(**)_{\mathbb{Z}_k}$ if and only if the class of $\mathfrak{a}$ is a square in $Cl_T(K)$. In particular this is the case when $\mathfrak{a}$ satisfies the stronger condition $(**)_{\mathfrak{C}^2}$.*

(5) *When $f_{t_0}(\mathfrak{C}) \neq 0$ (hence by (1) when $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$), we have*

$$f_{t_0}(\mathfrak{C}) = |S_{T,\mathfrak{C}^2}(K)| \ ,$$

and in particular this is independent of $\mathfrak{a}$ satisfying $(**)_{\mathfrak{C}^2}$.

Proof. (1). Assume that $\omega t_0 u \in Q(\mathfrak{C}^2)$ or, equivalently, that $x^2 = \omega t_0 u \beta$ for some $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$. By definition of $\mathfrak{a}$ and u, there exists $\mathfrak{b} \in < T >$ and $\mathfrak{q}$ such that $t_0 u\mathbb{Z}_K = \mathfrak{a}\mathfrak{q}^2\mathfrak{b}$, so that $t_0 u\mathbb{Z}_k = \mathfrak{a}\mathfrak{Q}^2$, hence by Corollary 1.9

$$x^2\mathbb{Z}_k = \beta(\mathfrak{a} \triangle \mathfrak{a}_\omega)s(\mathfrak{D})\mathfrak{Q}^2 \ .$$

In addition, taking norms from k to K of the equality $x^2 = \omega t_0 u\beta$, it is clear that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square of K, so that $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$.

Conversely, assume that $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$, so that $\omega t_0 \mathbb{Z}_k = \beta\mathfrak{Q}^2$. If we set $\alpha = \omega t_0/\beta$, this means that $\overline{\alpha} \in S(k)$, the ordinary Selmer group of k. On the other hand, taking relative norms we obtain $\mathcal{N}_{k/K}(\alpha) = y^2$ for some $y \in K$, so that by Lemma 1.1 we obtain as usual $\alpha = n\gamma^2$ for some $\gamma \in k$ and $n \in K$. Thus in $S(k)$ we have $\overline{\alpha} = \overline{n}$, hence $n \in S(k)^\tau$, and by Lemma 1.3 this means that $n \in S_T(K)$. Finally, setting $u = 1/n$, we see that $\overline{u}$ is an element of $S_T(K)$ such that $\omega t_0 u \in Q(\mathfrak{C}^2)$, proving (1).

(2). It follows from (1) that the existence of an ideal $\mathfrak{a}$ satisfying $(**)_{\mathfrak{C}^2}$ implies the existence of $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ such that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square. Conversely, if such a β exists, by Lemma 1.8 we can write $s(\beta) = \mathfrak{a}_\beta s(\mathfrak{D})$ for a squarefree ideal $\mathfrak{a}_\beta$ prime to $\mathfrak{d}$, and it is clear that $\mathfrak{a}_\omega \triangle \mathfrak{a}_\beta$ satisfies $(**)_{\mathfrak{C}^2}$.

(3). Assume that $\mathfrak{a}_0$ satisfies $(**)_{\mathfrak{C}^2}$ for some $\beta_0 \in k$. By construction, we know that $(\mathfrak{a} \triangle \mathfrak{a}_\omega)s(\mathfrak{D}) = \omega\mathfrak{a}\mathfrak{Q}^2$, hence by dividing, it is clear that $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$ if and only if $(\mathfrak{a}/\mathfrak{a}_0)\mathbb{Z}_k = \alpha\mathfrak{Q}^2$ for some $\alpha \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ of square norm. Thus by Lemma 1.1 we can write $\alpha = z\gamma^2$ for some $z \in K$ and $\gamma \in k$, and in particular, $z \in Q_K(\mathfrak{C}^2)$. On the other hand the fractional ideal $(\mathfrak{a}/\mathfrak{a}_0)/z$ of K extends to the square of the ideal $\mathfrak{Q}\gamma$ in k, hence is of the form $\mathfrak{q}^2\mathfrak{b}$ for some $\mathfrak{b} \in <T>$, so that $\mathfrak{a}/\mathfrak{a}_0 = z\mathfrak{q}^2\mathfrak{b}$. By the approximation theorem, by multiplying $\mathfrak{q}$ with a suitable $n \in K^*$ and changing z into z/n^2, we may assume that $\mathfrak{q}$ is coprime to $\mathfrak{c}$, hence that $z \in Q_K(\mathfrak{C}^2)$, and since by Lemma 2.1 (2) $\mathfrak{a}/\mathfrak{a}_0$ is coprime to $\mathfrak{c}$, this exactly means that the class of $\mathfrak{a}/\mathfrak{a}_0$ is a square in $Cl_{T,\mathfrak{C}^2}(K)$. Furthermore, since $(\mathfrak{a} \triangle \mathfrak{a}_\omega)/(\mathfrak{a}_0 \triangle \mathfrak{a}_\omega)$ is equal to the square of an ideal times $\mathfrak{a}/\mathfrak{a}_0$ which is coprime to $\mathfrak{c}$ by Lemma 2.1 (1), the second statement of (3) follows.

(4). If we take $\mathfrak{C} = \mathbb{Z}_k$, it is clear that $\mathfrak{a}_0 = \mathbb{Z}_k$ satisfies $(**)_{\mathbb{Z}_k}$ with $\beta = \omega$ (since $s(\omega) = \mathfrak{a}_\omega s(\mathfrak{D})$). Thus by (3) $\mathfrak{a}$ satisfies $(**)_{\mathbb{Z}_k}$ if and only if the class of $\mathfrak{a}$ is a square in $Cl_T(K) = Cl_{T,\mathbb{Z}_k}(K)$. In particular, this is true if $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$.

(5). Assume that $\mathfrak{a}$ satisfies condition $(**)_{\mathfrak{C}^2}$, so that there exists $v \in S_T(K)$ such that $\omega t_0 v \in Q(\mathfrak{C}^2)$. Thus $\omega t_0 u \in Q(\mathfrak{C}^2)$ if and only if $u/v \in Q(\mathfrak{C}^2)$, hence if and only if $\overline{u/v} \in S_{T,\mathfrak{C}^2}$. Thus the set of suitable $\overline{u}$ is equal to $\overline{v}S_{T,\mathfrak{C}^2}$, whose cardinality is of course equal to $|S_{T,\mathfrak{C}^2}|$. □

Thanks to this proposition, we can now easily prove an important preliminary formula for the Dirichlet series $\Phi_k(s)$.

Theorem 2.3. *To simplify notations, set* $\mathcal{G}_{\mathfrak{C}^2}(K) = Cl_{T,\mathfrak{C}^2}(K)/Cl_{T,\mathfrak{C}^2}(K)^2$. *Then*

$$\Phi_k(s) = \frac{\mathcal{N}(s(\mathfrak{d}))^{-s}}{4^{2ns}} \times \sum_{\substack{\mathfrak{C}|2\mathbb{Z}_k \\ (\mathfrak{C},s(\mathfrak{D}))=1 \\ \mathfrak{C} \text{ satisfies } (*)}} |S_{T,\mathfrak{C}^2}(K)|\, \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s} \prod_{\mathfrak{P}|\mathfrak{C}} \left(1 - \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{P})^{2s}}\right) P(\mathfrak{C}) \ ,$$

where

$$P(\mathfrak{C}) = \frac{1}{|\mathcal{G}_{\mathfrak{C}^2}(K)|} \sum_{\chi \in \widehat{\mathcal{G}_{\mathfrak{C}^2}(K)}} \chi(\mathfrak{a}_{\beta(\mathfrak{C}^2)}) \prod_{\mathfrak{p} \nmid \mathfrak{C}\mathfrak{d}} \left(1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{2s}}\right) \ ,$$

and $\beta(\mathfrak{C}^2)$ *is an element of* k *such that* $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ *with* $\mathcal{N}_{k/K}(\beta(\mathfrak{C}^2))$ *equal to* D *times a square of* K.

Proof. We replace $f_{t_0}(\mathfrak{C})$ by its value given by Proposition 2.2 in the last formula for $\Phi_k(s)$ given just before Definition 2 above. In particular, we can restrict the summation to ideals $\mathfrak{C}$ satisfying $(*)$, and to ideals $\mathfrak{a}$ satisfying $(**)_{\mathfrak{C}^2}$. However, by the same proposition if $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$ then the class of $\mathfrak{a}$ is automatically a square in $Cl_T(K)$. It follows that we can remove the restriction $\mathfrak{a} \in \mathcal{I}$ and replace it by the weaker condition that $\mathfrak{a} \in \mathcal{J}$, where by definition $\mathcal{J}$ is simply the set of squarefree ideals of K coprime to $\mathfrak{d}$. Thus

$$\Phi_k(s) = \frac{\mathcal{N}(s(\mathfrak{d}))^{-s}}{4^{2ns}} \times \sum_{\substack{\mathfrak{C}|2\mathbb{Z}_k \\ (\mathfrak{C},s(\mathfrak{D}))=1 \\ \mathfrak{C} \text{ satisfies } (*)}} |S_{T,\mathfrak{C}^2}(K)|\, \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s} \prod_{\mathfrak{P}|\mathfrak{C}} \left(1 - \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{P})^{2s}}\right) P(\mathfrak{C}) \ ,$$

where

$$P(\mathfrak{C}) = \sum_{\substack{\mathfrak{a} \in \mathcal{J} \\ (\mathfrak{a} \triangle \mathfrak{a}_\omega, \mathfrak{C})=1 \\ \mathfrak{a} \text{ satisfies } (**)_{\mathfrak{C}^2}}} \frac{1}{\mathcal{N}(\mathfrak{a} \triangle \mathfrak{a}_\omega)^{2s}} \ .$$

Note that the condition $\mathfrak{a} \in \mathcal{J}$ is equivalent to $\mathfrak{a} \triangle \mathfrak{a}_\omega \in \mathcal{J}$, and that the map $\mathfrak{a} \mapsto \mathfrak{a} \triangle \mathfrak{a}_\omega$ is an involution of $\mathcal{J}$. Furthermore, $\mathfrak{a} \triangle \mathfrak{a}_\omega$ is squarefree and coprime to $\mathfrak{C}$ and $\mathfrak{d}$, and by Proposition 2.2 (2) and (3), $\mathfrak{a}$ satisfies $(**)_{\mathfrak{C}^2}$ if and only if the class of $(\mathfrak{a} \triangle \mathfrak{a}_\omega)/(\mathfrak{a}_0(\mathfrak{C}^2) \triangle \mathfrak{a}_\omega)$ is a square in $Cl_{T,\mathfrak{C}^2}(K)$, with $\mathfrak{a}_0(\mathfrak{C}^2) = \mathfrak{a}_{\beta(\mathfrak{C}^2)} \triangle \mathfrak{a}_\omega$, hence if and only if the class of $(\mathfrak{a} \triangle \mathfrak{a}_\omega)/\mathfrak{a}_{\beta(\mathfrak{C}^2)}$ is

a square in $Cl_{T,\mathfrak{C}^2}$. Thus, changing $\mathfrak{a}$ into $\mathfrak{a}\triangle\mathfrak{a}_\omega$, we obtain

$$P(\mathfrak{C}) = \sum_{\substack{\mathfrak{a}\in\mathcal{J}\\(\mathfrak{a},\mathfrak{C})=1\\ \overline{\mathfrak{a}/\mathfrak{a}_{\beta(\mathfrak{C}^2)}}\in Cl_{T,\mathfrak{C}^2}(K)^2}} \frac{1}{\mathcal{N}(\mathfrak{a})^{2s}} ,$$

where $\beta(\mathfrak{C}^2)\equiv 1 \pmod{{}^*\mathfrak{C}^2}$ is of relative norm D times a square. Note that since $(\mathfrak{C}, s(\mathfrak{D}))=1$, $\mathfrak{a}_{\beta(\mathfrak{C}^2)}$ is coprime to $\mathfrak{C}$.

Since the class of an ideal $\mathfrak{m}$ is a square in $Cl_{T,\mathfrak{C}^2}(K)$ if and only if for each $\chi\in\widehat{\mathcal{G}_{\mathfrak{C}^2}(K)}$, the group of characters of $\mathcal{G}_{\mathfrak{C}^2}(K)$, we have $\chi(\mathfrak{m})=1$, we obtain

$$\begin{aligned} P(\mathfrak{C}) &= \frac{1}{|\mathcal{G}_{\mathfrak{C}^2}(K)|}\sum_{\chi\in\widehat{\mathcal{G}_{\mathfrak{C}^2}(K)}}\sum_{\substack{\mathfrak{a}\in\mathcal{J}\\(\mathfrak{a},\mathfrak{C})=1}}\frac{\chi(\mathfrak{a}/\mathfrak{a}_{\beta(\mathfrak{C}^2)})}{\mathcal{N}(\mathfrak{a})^{2s}}\\ &= \frac{1}{|\mathcal{G}_{\mathfrak{C}^2}(K)|}\sum_{\chi\in\widehat{\mathcal{G}_{\mathfrak{C}^2}(K)}}\chi(\mathfrak{a}_{\beta(\mathfrak{C}^2)})\prod_{\mathfrak{p}\nmid\mathfrak{c}\mathfrak{d}}\left(1+\frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{2s}}\right) , \end{aligned}$$

since χ is of order 2, proving the theorem. As in Lemma 1.8, it is easily shown that the class of $\mathfrak{a}_{\beta(\mathfrak{C}^2)}$ in $\mathcal{G}_{\mathfrak{C}^2}(K)$ is independent of the choice of $\beta(\mathfrak{C}^2)$, so that $\chi(\mathfrak{a}_{\beta(\mathfrak{C}^2)})$ is independent of $\beta(\mathfrak{C}^2)$. □

It remains to compute $|S_{T,\mathfrak{C}^2}(K)|$ and to study condition $(*)$.

3. Computation of $|S_{T,\mathfrak{C}^2}(K)|$ and study of condition $(*)$

We keep all the above notation. and in particular $\mathfrak{C}$ will always be an ideal dividing $2\mathbb{Z}_k$, coprime to $s(\mathfrak{D})$ and satisfying condition $(*)$.

3.1. Reduction of the problem.

Definition. As in Definition 2, set $\mathfrak{c}=\mathfrak{C}^2\cap K$.

(1) We will say that an element $z\in K^*$ is T-coprime to $\mathfrak{c}$ if there exists $\mathfrak{b}\in< T >$ such that the ideal $z\mathfrak{b}$ is coprime to $\mathfrak{c}$.
(2) We will denote by $\mathcal{Z}_{\mathfrak{C}^2}$ the quotient by $Q_K(\mathfrak{C}^2)$ of the group of elements of K^* which are T-coprime to $\mathfrak{c}$, i.e., the subgroup of such elements z for which the congruence $z/x^2\equiv 1 \pmod{{}^*\mathfrak{C}^2}$ is soluble in k.

Remarks.

(1) It is clear that if z is T-coprime to $\mathfrak{c}$, then $z^2\in Q_K(\mathfrak{C}^2)$, hence $\mathcal{Z}_{\mathfrak{C}^2}$ is an abelian group killed by 2, like all the other groups that we consider in this section. We will compute its cardinality explicitly later (see Corollaries 3.7 and 3.13).

(2) If we write $\mathfrak{c} = \mathfrak{c}_r\mathfrak{c}_u$ where $\mathfrak{c}_r = (\mathfrak{c}, \mathfrak{d}^\infty)$ and $(c_u, \mathfrak{d}) = 1$, it is clear that z is T-coprime to $\mathfrak{c}$ if and only if $(z, \mathfrak{c}_u) = 1$.

The basic tool which will enable us to compute $S_{T,\mathfrak{C}^2}$ is the following result. Recall that for any ideal $\mathfrak{C}$ dividing $2\mathbb{Z}_k$, we have set

$$\mathcal{G}_{\mathfrak{C}^2}(K) = Cl_{T,\mathfrak{C}^2}(K)/Cl_{T,\mathfrak{C}^2}(K)^2 \ .$$

In particular, $\mathcal{G}_{\mathbb{Z}_k}(K) = Cl_T(K)/Cl_T(K)^2$.

Proposition 3.1. *Let $\mathfrak{c} = \mathfrak{C}^2 \cap K$. There exists a natural long exact sequence*

$$1 \longrightarrow S_{T,\mathfrak{C}^2}(K) \longrightarrow S_T(K) \longrightarrow \mathcal{Z}_{\mathfrak{C}^2} \longrightarrow \mathcal{G}_{\mathfrak{C}^2}(K) \longrightarrow \mathcal{G}_{\mathbb{Z}_k}(K) \longrightarrow 1 \ ,$$

where the maps will be described in the proof.

Proof. Exactness at $S_{T,\mathfrak{C}^2}$ is trivial. If $\overline{u} \in S_T(K)$, then $u\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{b}$ with $\mathfrak{b} \in < T >$, and by the approximation theorem, changing u into n^2u if necessary, we may assume that $\mathfrak{q}$ is coprime to $\mathfrak{c}$, hence u is T-coprime to $\mathfrak{c}$. We then send such a u to its class in $\mathcal{Z}_{\mathfrak{C}^2}$. It is clear that it does not depend on the representative of the class $\overline{u}$ chosen T-coprime to $\mathfrak{c}$. Furthermore, $\overline{u}$ is sent to the unit element of $\mathcal{Z}_{\mathfrak{C}^2}$ if and only if $u \in Q_K(\mathfrak{C}^2)$, hence if and only if $\overline{u} \in S_{T,\mathfrak{C}^2}$, proving exactness at $S_T(K)$.

Let $\overline{z} \in \mathcal{Z}_{\mathfrak{C}^2}$. Since z is T-coprime to $\mathfrak{c}$, there exists a $\mathfrak{b} \in < T >$ such that $(z\mathfrak{b}, \mathfrak{c}) = 1$, hence also $(z\mathfrak{b}, \mathfrak{C}) = 1$. We will send $\overline{z}$ to the class of $z\mathfrak{b}$. By definition of $Cl_{T,\mathfrak{C}^2}(K)$, this class is independent of the choice of $\mathfrak{b}$. Furthermore, it is independent of the representative z of the class: indeed, if z' is another representative, then $z' = zn$ where n is such that there exists $\mathfrak{b}' \in < T >$ with $(n\mathfrak{b}', \mathfrak{c}) = 1$ and $n/x^2 \equiv 1 \pmod{\mathfrak{C}^2}$ soluble in k. It follows that $z'\mathfrak{b}\mathfrak{b}' = (z\mathfrak{b})(n\mathfrak{b}')$, and the class of $n\mathfrak{b}'$ is trivial since $n/x^2 \equiv 1 \pmod{\mathfrak{C}^2}$ is soluble in k. This shows that the map is well defined.

To show exactness at $\mathcal{Z}_{\mathfrak{C}^2}$, let z be T-coprime to $\mathfrak{c}$, let $\mathfrak{b} \in < T >$ with $(z\mathfrak{b}, \mathfrak{c}) = 1$, and assume that the class of $z\mathfrak{b}$ is trivial in $\mathcal{G}_{\mathfrak{C}^2}(K)$. This means that there exists an ideal $\mathfrak{q}$ coprime to $\mathfrak{c}$, an ideal $\mathfrak{b}' \in < T >$ and an element n such that $(n\mathfrak{b}', \mathfrak{c}) = 1$ and $n/x^2 \equiv 1 \pmod{\mathfrak{C}^2}$ soluble in k, with $z\mathfrak{b} = n\mathfrak{b}'\mathfrak{q}^2$, in other words $(z/n)\mathbb{Z}_K = \mathfrak{q}^2(\mathfrak{b}'/\mathfrak{b})$. Since $n \in Q_K(\mathfrak{C}^2)$, the class of z/n in $\mathcal{Z}_{\mathfrak{C}^2}$ is equal to the class of z. Thus choosing z/n instead of z as representative of its class, and noting that $\overline{z/n} \in S_T(K)$, we have shown exactness at $\mathcal{Z}_{\mathfrak{C}^2}$.

Let $\mathfrak{a}$ be an ideal coprime to $\mathfrak{c}$, and assume that its class as an element of $\mathcal{G}_{\mathbb{Z}_k}(K)$ is trivial. This means that $\mathfrak{a} = z\mathfrak{q}^2\mathfrak{b}$ for some $z \in K^*$, some ideal $\mathfrak{q}$ and some $\mathfrak{b} \in < T >$. Using as usual the approximation theorem, we may assume that we have chosen $\mathfrak{q}$ coprime to $\mathfrak{c}$, so that $(z\mathfrak{b}, \mathfrak{c}) = 1$. Since $(\mathfrak{q}, \mathfrak{c}) = 1$, the class of $\mathfrak{a}$ in $\mathcal{G}_{\mathfrak{C}^2}(K)$ is equal to that of $\mathfrak{a}/\mathfrak{q}^2 = z\mathfrak{b}$, and since z is T-coprime to $\mathfrak{c}$, this proves exactness at $\mathcal{G}_{\mathfrak{C}^2}(K)$. Note that $Q_K(\mathfrak{C}^2)$ is of course sent to the unit element of $\mathcal{G}_{\mathfrak{C}^2}(K)$.

Finally, if $\mathfrak{a}$ is an ideal of K, by the approximation theorem we can find β such that $(\beta\mathfrak{a}, \mathfrak{c}) = 1$, and the class of $\beta\mathfrak{a}$ in $\mathcal{G}_{\mathbb{Z}_k}(K)$ is equal to that of $\mathfrak{a}$, proving exactness at that group and finishing the proof of the proposition. □

The second much simpler exact sequence that we need is the following.

Proposition 3.2. *There exists a natural short exact sequence*

$$1 \longrightarrow \frac{U_T(K)}{U_T(K)^2} \longrightarrow S_T(K) \longrightarrow Cl_T(K)[2] \longrightarrow 1 \ ,$$

where $U_T(K)$ denotes the group of T-units of K (i.e., elements $\varepsilon \in K^*$ such that $v_{\mathfrak{p}}(\varepsilon) = 0$ for all prime ideals $\mathfrak{p} \notin T$), and for any group G, $G[2]$ denotes the subgroup of elements of G whose square is the unit element of G.

Proof. Let $\overline{u} \in S_T(K)$, so that $u\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{b}$ for some $\mathfrak{b} \in < T >$. We send $\overline{u}$ to the class of $\mathfrak{q}$ in $Cl_T(K)$. By definition, this class indeed belongs to $Cl_T(K)[2]$. Conversely, if $\overline{\mathfrak{q}} \in Cl_T(K)[2]$ then $\mathfrak{q}^2 = z\mathfrak{b}$ for some $\mathfrak{b} \in < T >$, so clearly $\overline{z} \in S_T(K)$ proving exactness at $Cl_T(K)[2]$. Finally, if $\overline{u} \in S_T(K)$ is sent to the unit element of $Cl_T(K)$, this means that $u\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{b}$ and that $\mathfrak{q} = z\mathfrak{b}'$ for some $\mathfrak{b}' \in < T >$. Hence $u\mathbb{Z}_K = z^2\mathfrak{b}''$ for still another $\mathfrak{b}'' \in < T >$, so u/z^2 (whose class in $S_T(K)$ is the same as that of u) is an T-unit, proving the proposition. □

Corollary 3.3. *Let (r_1, r_2) be the signature of K. We have*

$$|S_{T,\mathfrak{C}^2}(K)| = \frac{2^{r_1+r_2+|T|}|\mathcal{G}_{\mathfrak{C}^2}(K)|}{|\mathcal{Z}_{\mathfrak{C}^2}|} \ .$$

Proof. By Proposition 3.1, we have

$$|S_{T,\mathfrak{C}^2}(K)| = \frac{|S_T(K)||\mathcal{G}_{\mathfrak{C}^2}(K)|}{|\mathcal{Z}_{\mathfrak{C}^2}||\mathcal{G}_{\mathbb{Z}_k}(K)|} \ ,$$

and by Proposition 3.2 we have

$$|S_T(K)| = \left|\frac{U_T(K)}{U_T(K)^2}\right| |Cl_T(K)[2]| \ .$$

It is well known that $U_T(K)$ is isomorphic to the group of roots of unity of K times a free abelian group of rank $r_1 + r_2 - 1 + |T|$. Since the group of roots of unity is cyclic of even order, it follows that $|U_T(K)/U_T(K)^2| = 2^{r_1+r_2+|T|}$. On the other hand, for any finite abelian group G we have $|G/G^2| = |G[2]|$ (look at the kernel and cokernel of squaring), so that $|Cl_T(K)[2]| = |\mathcal{G}_{\mathbb{Z}_k}(K)|$. Putting everything together, we obtain the given formula. □

By Theorem 2.3, the term $|\mathcal{G}_{\mathfrak{C}^2}(K)|$ will cancel. It thus remains to compute $|\mathcal{Z}_{\mathfrak{C}^2}|$. By the Chinese remainder theorem, it is immediately checked on the definition that this is multiplicative in the following sense. Let $\mathfrak{C}_1$ and $\mathfrak{C}_2$ be two ideals of $\mathbb{Z}_k$, and set $\mathfrak{c}_i = \mathfrak{C}_i^2 \cap K$ for $i = 1, 2$. Then if $(\mathfrak{c}_1, \mathfrak{c}_2) = 1$, we have $|\mathcal{Z}_{(\mathfrak{c}_1\mathfrak{c}_2)^2}| = |\mathcal{Z}_{\mathfrak{C}_1^2}||\mathcal{Z}_{\mathfrak{C}_2^2}|$. Note that this coprimeness condition is *stronger* than the simple coprimeness condition $(\mathfrak{C}_1, \mathfrak{C}_2) = 1$, but is necessary since we work in K.

A similar result is also true for condition $(*)$: if $(\mathfrak{C}_1, \mathfrak{C}_2) = 1$, then $(*)$ is true for $\mathfrak{C}_1\mathfrak{C}_2$ if and only if it is true for $\mathfrak{C}_1$ and $\mathfrak{C}_2$.

Thus we can work individually for each prime ideal $\mathfrak{p}$ of K dividing $2\mathbb{Z}_K$. We will denote by $e = e(\mathfrak{p})$ the absolute ramification index of $\mathfrak{p}$ over 2.

Recall that the ideals $\mathfrak{C}$ which occur are coprime to $s(\mathfrak{D})$. In other words, the ideals $\mathfrak{p}$ of K which we consider are the ideals above 2 such that $v_{\mathfrak{p}}(\mathfrak{d}) \equiv 0 \pmod 2$.

Lemma 3.4. (1) *We can choose D defining k/K such that for all $\mathfrak{p} \mid 2$ we have $v_{\mathfrak{p}}(D) = v_{\mathfrak{p}}(\mathfrak{d})$.*

(2) *For such a choice of D, there exist a and b such that $D = a^2 + 4b$, where $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{d})/2$ and $v_{\mathfrak{p}}(b) = 1$ for every prime ideal $\mathfrak{p} \mid 2$ such that $v_{\mathfrak{p}}(\mathfrak{d}) > 0$, and $v_{\mathfrak{p}}(a) = 0$, $v_{\mathfrak{p}}(b) \geq 0$ for every prime ideal $\mathfrak{p} \mid 2$ such that $v_{\mathfrak{p}}(\mathfrak{d}) = 0$.*

(3) *We may choose ω coprime to all ideals $\mathfrak{C}$ dividing 2 which are coprime to $s(\mathfrak{D})$ (which are the only ideals $\mathfrak{C}$ that we use), and such that $\mathcal{N}_{k/K}(\omega) = Dz^2$ for some $z \in K^*$.*

Proof. (1). We know that $D\mathbb{Z}_K = \mathfrak{d}\mathfrak{m}^2$ for some ideal $\mathfrak{m}$ of K. By the approximation theorem, multiplying if necessary $\mathfrak{m}$ by a suitable $z \in K$ to make it coprime to 2 (which changes D into Dz^2, hence does not change $k = K(\sqrt{D})$), we may assume that $\mathfrak{m}$ is coprime to 2, proving (1).

(2). Let $\mathfrak{p}$ be a prime ideal above 2 such that $v_{\mathfrak{p}}(\mathfrak{d}) \equiv 0 \pmod 2$, hence $v_{\mathfrak{p}}(D) \equiv 0 \pmod 2$. By Hecke's theorem, there exists $x_{\mathfrak{p}}$ such that $x_{\mathfrak{p}}^2/D \equiv 1 \pmod{{}^*\mathfrak{p}^k}$ for $k = 2e(\mathfrak{p}) + 1 - v_{\mathfrak{p}}(\mathfrak{d})$ and for no larger value of k if $v_{\mathfrak{p}}(\mathfrak{d}) > 0$, and for $k = 2e(\mathfrak{p})$ if $v_{\mathfrak{p}}(\mathfrak{d}) = 0$ (and possibly for larger values of k). Since $v_{\mathfrak{p}}(D) = v_{\mathfrak{p}}(\mathfrak{d})$, for $v_{\mathfrak{p}}(\mathfrak{d}) > 0$ we have $x_{\mathfrak{p}}^2 \equiv D \pmod{{}^*\mathfrak{p}^{2e(\mathfrak{p})+1}}$, and this congruence is not soluble modulo any higher power of $\mathfrak{p}$, while $x_{\mathfrak{p}}^2 \equiv D \pmod{{}^*\mathfrak{p}^{2e(\mathfrak{p})}}$ for $v_{\mathfrak{p}}(\mathfrak{d}) = 0$. By the Chinese remainder theorem, we can find $a \in K$ such that for each $\mathfrak{p} \mid 2$ for which $v_{\mathfrak{p}}(\mathfrak{d}) \equiv 0 \pmod 2$ we have $a \equiv x_{\mathfrak{p}} \pmod{{}^*\mathfrak{p}^{2e(\mathfrak{p})+1}}$ or $a \equiv x_{\mathfrak{p}} \pmod{{}^*\mathfrak{p}^{2e(\mathfrak{p})}}$ respectively, so that $v_{\mathfrak{p}}((D - a^2)/4) = 1$ for all such $\mathfrak{p}$ with $v_{\mathfrak{p}}(\mathfrak{d}) > 0$, and $v_{\mathfrak{p}}((D - a^2)/4) \geq 0$ otherwise, proving (2).

(3). Recall that by Lemma 1.8 we have $\omega\mathbb{Z}_k = \mathfrak{a}_\omega s(\mathfrak{D})\mathfrak{Q}^2$. By the approximation theorem, multiplying ω by a square in k, and also by an element of K (which does not change the property that $\mathcal{N}_{k/K}(\omega)$ is equal

to D times a square of K) we may assume that $\mathfrak{Q}$ and $\mathfrak{a}_\omega$ are coprime to 2. Since the ideals $\mathfrak{C}$ divide $2\mathbb{Z}_k$ and are coprime to $s(\mathfrak{D})$, it follows that ω is coprime to $\mathfrak{C}$. □

In the sequel, we fix a and b satisfying the above lemma, and we always assume that ω is chosen satisfying (3). We will set $\rho = (a + \sqrt{D})/2$.

Before separating the unramified and ramified cases, note the following lemma which is common to both.

Lemma 3.5. *Assume D chosen as above. Let $\mathfrak{p}$ be an ideal of K above 2 such that $v_\mathfrak{p}(\mathfrak{d}) \equiv 0 \pmod 2$, and let $\mathfrak{P}$ be an ideal of k above $\mathfrak{p}$. Then $\alpha = u + v\rho$ is a $\mathfrak{P}$-integer in k if and only if u and v are $\mathfrak{p}$-integers of K.*

Proof. Note that the relative equation of ρ in k/K is $x^2 - ax - b = 0$, and since a and b are $\mathfrak{p}$-integers, ρ is a $\mathfrak{P}$-integer of k. The relative discriminant of the order $\mathbb{Z}_{K,\mathfrak{p}}[\rho]/\mathbb{Z}_{K,\mathfrak{p}}$ is equal to D, and we have $v_\mathfrak{p}(D) = v_\mathfrak{p}(\mathfrak{d})$, hence $\mathbb{Z}_{K,\mathfrak{p}}[\rho]$ is $\mathfrak{p}$-maximal, proving the lemma. Of course, we could also check this directly using trace and norm. □

3.2. Computation of $|\mathcal{Z}_{\mathfrak{C}^2}|$ in the Unramified Case. We assume in this subsection that $\mathfrak{p}$ is unramified, so that $v_\mathfrak{p}(\mathfrak{d}) = 0$ and $v_\mathfrak{p}(a) = 0$. We let $\mathfrak{P}$ be a prime ideal of k above $\mathfrak{p}$.

Proposition 3.6. *Keep the above notations, and let $t \le e = e(\mathfrak{p})$. If $n \in K^*$, the congruence $x^2 \equiv n \pmod{{}^*\mathfrak{p}^{2t}\mathbb{Z}_k}$ has a solution in k if and only if it has a solution in K.*

Proof. One direction is trivial, so assume that the congruence has a solution $x = u + v\rho \in k$ with u and v in K. We claim that $u^2 \equiv n \pmod{{}^*\mathfrak{p}^{2t}}$, which will prove the proposition. Indeed, we have

$$x^2 = (u^2 + v^2 b) + (2uv + v^2 a)\rho \equiv n \pmod{{}^*\mathfrak{p}^{2t}\mathbb{Z}_k} ,$$

hence by Lemma 3.5 $v_\mathfrak{p}(v(2u + va)) \ge 2t$ and $v_\mathfrak{p}(u^2 + v^2 b - n) \ge 2t$. Since $t \le e = e(\mathfrak{p})$, $v_\mathfrak{p}(a) = 0$, and $v_\mathfrak{p}(u) \ge 0$, it is clear that if $v_\mathfrak{p}(v) < t$ the first inequality leads to a contradiction, so that $v_\mathfrak{p}(v) \ge t$, thus proving our claim by replacing in the second inequality. □

Corollary 3.7. (1) *If $\mathfrak{p}$ is inert in k/K so that $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}$, and if $\mathfrak{C} = \mathfrak{P}^t$ with $1 \le t \le e(\mathfrak{p})$, then*

$$|\mathcal{Z}_{\mathfrak{C}^2}| = \mathcal{N}\mathfrak{p}^t .$$

(2) *If $\mathfrak{p}$ is split in k/K so that $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}\overline{\mathfrak{P}}$, and if $\mathfrak{C} = \mathfrak{P}^{t_1}\overline{\mathfrak{P}}^{t_2}$ with $0 \le t_1, t_2 \le e(\mathfrak{p})$, then*

$$|\mathcal{Z}_{\mathfrak{C}^2}| = \mathcal{N}\mathfrak{p}^{\max(t_1,t_2)} .$$

Proof. Note that $\mathfrak{c} = \mathfrak{C}^2 \cap K = \mathfrak{p}^{2t}$ with t as given in the inert case, and with $t = \max(t_1, t_2)$ in the split case. Thus

$$|(\mathbb{Z}_K/\mathfrak{c})^*| = \phi_K(\mathfrak{p}^{2t}) = \mathcal{N}\mathfrak{p}^{2t-1}(\mathcal{N}\mathfrak{p} - 1) \ ,$$

where ϕ_K is the Euler ϕ-function on ideals of K. Furthermore, when $(\mathfrak{C}, \mathfrak{d}) = 1$, it is clear that $\mathcal{Z}_{\mathfrak{C}^2} = (\mathbb{Z}_K/\mathfrak{c})^*/\overline{Q_K(\mathfrak{C}^2)}$, where $\overline{Q_K(\mathfrak{C}^2)}$ is the group of classes of elements of $Q_K(\mathfrak{C}^2)$ modulo $\mathfrak{c}$. By the above proposition $\overline{Q_K(\mathfrak{C}^2)}$ is the group of squares in $(\mathbb{Z}_K/\mathfrak{c})^*$. Since $\mathfrak{c} = (\mathfrak{p}^t)^2$ and $\mathfrak{p}^t \mid 2$, an elementary argument shows that the squaring map from $(\mathbb{Z}_K/\mathfrak{p}^t)^*$ to the squares in $(\mathbb{Z}_K/\mathfrak{p}^{2t})^*$ is well defined and is an isomorphism, so that $|\overline{Q_K(\mathfrak{C}^2)}| = \phi_K(\mathfrak{p}^t) = \mathcal{N}\mathfrak{p}^{t-1}(\mathcal{N}\mathfrak{p} - 1)$, proving the corollary. □

3.3. Study of Condition $(*)$ in the Unramified Case. We first prove the following proposition, which is a strengthening of Proposition 3.6.

Proposition 3.8. *As above, let $t \le e = e(\mathfrak{p})$, and denote by SQ the subgroup of elements $\overline{\alpha} \in (\mathbb{Z}_k/\mathfrak{p}^{2t}\mathbb{Z}_k)^*$ such that $\overline{\mathcal{N}_{k/K}(\alpha)}$ is a square in $(\mathbb{Z}_K/\mathfrak{p}^{2t})^*$ (this is of course independent of the choice of the representative α). We have a short exact sequence*

$$1 \longrightarrow (\mathbb{Z}_K/\mathfrak{p}^t)^* \longrightarrow (\mathbb{Z}_k/\mathfrak{p}^t\mathbb{Z}_k)^* \times (\mathbb{Z}_K/\mathfrak{p}^{2t})^* \longrightarrow SQ \longrightarrow 1 \ ,$$

where the first nontrivial map sends $\overline{m}$ to $(\overline{m}, \overline{m^2})$, and the second sends $(\overline{x}, \overline{n})$ to $\overline{nx^{-2}}$.

Proof. We have already mentioned that the squaring map gives an isomorphism from $(\mathbb{Z}_K/\mathfrak{p}^t)^*$ to $(\mathbb{Z}_K/\mathfrak{p}^{2t})^{*2}$, hence the first nontrivial map is clearly well defined and injective. Exactness in the middle is a restatement of Proposition 3.6. Finally, it is clear that the image of the second nontrivial map lands in SQ. We must show that it is all of SQ.

For this, we use the following well known result from local class field theory: since $\mathfrak{p}$ is unramified in the abelian extension k/K, the norm map from the units of $k_{\mathfrak{P}}$ to those of $K_{\mathfrak{p}}$ is surjective. In particular, this is also the case at the level of $\mathfrak{p}^{2t}$, in other words for any $\overline{m} \in (\mathbb{Z}_K/\mathfrak{p}^{2t})^*$ there exists $\beta \in K$ such that $\mathcal{N}_{k/K}(\beta) \equiv m \pmod{{}^*\mathfrak{p}^{2t}}$. The kernel of the norm map from $(\mathbb{Z}_k/\mathfrak{p}^{2t}\mathbb{Z}_k)^*$ to $(\mathbb{Z}_K/\mathfrak{p}^{2t})^*$ has cardinality $\phi_k(\mathfrak{p}^{2t}\mathbb{Z}_k)/\phi_K(\mathfrak{p}^{2t})$. On the other hand, SQ is the inverse image by the norm map of the squares of $(\mathbb{Z}_K/\mathfrak{p}^{2t})^*$, whose cardinality is equal to $\phi_K(\mathfrak{p}^t)$ as we have seen. Since the norm is surjective, it follows that

$$|SQ| = \phi_K(\mathfrak{p}^t)\frac{\phi_k(\mathfrak{p}^{2t}\mathbb{Z}_k)}{\phi_K(\mathfrak{p}^{2t})} = \frac{\phi_k(\mathfrak{p}^t\mathbb{Z}_k)\,\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{p}^t\mathbb{Z}_k)}{\mathcal{N}\mathfrak{p}^t} = \phi_k(\mathfrak{p}^t\mathbb{Z}_k)\mathcal{N}\mathfrak{p}^t \ .$$

On the other hand, the cardinality of the image of the second nontrivial map in the above sequence is equal to

$$\frac{\phi_k(\mathfrak{p}^t\mathbb{Z}_k)\phi_K(\mathfrak{p}^{2t})}{\phi_K(\mathfrak{p}^t)} = \phi_k(\mathfrak{p}^t\mathbb{Z}_k)\mathcal{N}\mathfrak{p}^t = |SQ| \ ,$$

thus showing that this map is surjective. □

Corollary 3.9. *Keep the above notations. There exists $n \in K$ coprime to $\mathfrak{p}$ such that the congruence $\omega \equiv nx^2 \pmod{{}^*\mathfrak{p}^{2t}\mathbb{Z}_k}$ has a solution in k. In other words, if $\mathfrak{C} = \mathfrak{P}^t$ for $\mathfrak{p}$ inert and $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}$, or if $\mathfrak{C} = \mathfrak{P}^{t_1}\overline{\mathfrak{P}}^{t_2}$ for $\mathfrak{p}$ split and $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}\overline{\mathfrak{P}}$ (and of course $\mathfrak{C} \mid 2\mathbb{Z}_k$ in both cases), then $\mathfrak{C}$ satisfies condition $(*)$.*

Proof. We know that $a^2 \equiv D \pmod{\mathfrak{p}^{2e}}$ with $v_\mathfrak{p}(a) = 0$. Writing $\mathcal{N}_{k/K}(\omega) = Dm^2$, where by assumption $v_\mathfrak{p}(m) = 0$, it follows that

$$\mathcal{N}_{k/K}(\omega) = Dm^2 \equiv (am)^2 \pmod{\mathfrak{p}^{2e}} \ .$$

Thus, $\mathcal{N}_{k/K}(\omega)$ is a square modulo $\mathfrak{p}^{2e}$, hence modulo $\mathfrak{p}^{2t}$ since $t \le e$, so that by definition $\overline{\omega} \in SQ$. The surjective property that we have shown is thus equivalent to the first part of the corollary. For the second part, note that by Lemma 1.1, $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square if and only if $\beta = \omega/(nx^2)$ for some $n \in K$, and the condition $\beta \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ is thus the same as $\omega \equiv nx^2 \pmod{{}^*\mathfrak{C}^2}$, so the corollary follows. □

3.4. Computation of $|\mathcal{Z}_{\mathfrak{C}^2}|$ in the Ramified Case. We now treat the ramified case, which is more delicate, both because the group $\mathcal{Z}_{\mathfrak{C}^2}$ is a little more complicated to compute, and because condition $(*)$ is not always satisfied, contrary to the unramified case.

Thus we assume here that $\mathfrak{p}$ is ramified and divides $\mathfrak{c}$, so that $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}^2$, and by Lemma 3.4 we have $v_\mathfrak{p}(D) = v_\mathfrak{p}(\mathfrak{d}) \equiv 0 \pmod 2$ (since $(\mathfrak{C}, s(\mathfrak{D})) = 1$), $D = a^2 + 4b$ with $v_\mathfrak{p}(a) = v_\mathfrak{p}(\mathfrak{d})/2 > 0$, and $v_\mathfrak{p}(b) = 1$.

In this case, we have $\mathfrak{C} = \mathfrak{P}^t$ with $1 \le t \le e(\mathfrak{P}) = 2e(\mathfrak{p}) = 2e$, so that $\mathfrak{C}^2 = \mathfrak{p}^t\mathbb{Z}_k$, $\mathfrak{c} = \mathfrak{C}^2 \cap K = \mathfrak{p}^t$, but t is not necessarily even. It is clear that any element of K^* is T-coprime to $\mathfrak{C}$: indeed, if $z \in K^*$, then $z\mathfrak{p}^{-v_\mathfrak{p}(z)}$ is coprime to $\mathfrak{C}$, and $\mathfrak{p} \in\!< T >$. We begin by the following lemma.

Lemma 3.10. *Let A and B be $\mathfrak{p}$-integral elements of K^* such that $v_\mathfrak{p}(B) = 0$, $v_\mathfrak{p}(A)$ is* odd, *and $v_\mathfrak{p}(A) < 2e$. There exist u and v in K such that $v_\mathfrak{p}(u^2 + Av^2 - B) \ge 2e$ if and only if there exists u such that $v_\mathfrak{p}(u^2 - B) \ge v_\mathfrak{p}(A)$. In particular, if $v_\mathfrak{p}(A) = 1$, this condition is always satisfied.*

Proof. By induction on $k \ge v_\mathfrak{p}(A)$, we will show that there exist u_k and v_k such that $v_\mathfrak{p}(u_k^2 + Av_k^2 - B) \ge k$. By assumption, this is true for $k = v_\mathfrak{p}(A)$. Assume that it is true for some k such that $v_\mathfrak{p}(A) \le k \le 2e - 1$, and let us

prove that it is also true for $k+1$. Write $u_{k+1} = u_k + x_k$ and $v_{k+1} = v_k + y_k$, so that the inequality for $k+1$ can be written

$$v_{\mathfrak{p}}(u_k^2 + 2u_k x_k + x_k^2 + A(v_k^2 + 2v_k y_k + y_k^2) - B) \geq k+1 \; .$$

If k is even, we choose $y_k = 0$ (in other words $v_{k+1} = v_k$). Since $\mathbb{Z}_K/\mathfrak{p}$ is a finite field, hence perfect, there exists x'_k such that

$$x_k'^{\,2} \equiv (B - (u_k^2 + Av_k^2))/\pi^k \pmod{\mathfrak{p}} \; ,$$

where π is some uniformizer of $\mathfrak{p}$ in K. We choose $x_k = \pi^{k/2} x'_k$. Note that $v_{\mathfrak{p}}(2u_k x_k) \geq e + k/2 \geq k+1$, since this last inequality is equivalent to $k+1 \leq 2e-1$, which is true since $k+1$ is odd and less than or equal to $2e$. Thus u_{k+1} is suitable.

If k is odd, we choose $x_k = 0$ (in other words $u_{k+1} = u_k$). As before, there exists y'_k such that

$$y_k'^{\,2} \equiv \frac{\pi^{v_{\mathfrak{p}}(A)}}{A} \cdot \frac{B - (u_k^2 + Av_k^2)}{\pi^k} \pmod{\mathfrak{p}} \; .$$

Since $k - v_{\mathfrak{p}}(A)$ is even, we can set $y_k = \pi^{(k-v_{\mathfrak{p}}(A))/2} y'_k$. Since

$$\begin{aligned} v_{\mathfrak{p}}(2Av_k y_k) &\geq e + v_{\mathfrak{p}}(A) + (k - v_{\mathfrak{p}}(A))/2 \\ &= e + (k + v_{\mathfrak{p}}(A))/2 \geq e + (k+1)/2 \geq k+1 \end{aligned}$$

as above, it follows that v_{k+1} is suitable. This proves the first part of the lemma by induction on k.

In the special case $v_{\mathfrak{p}}(A) = 1$, the condition $v_{\mathfrak{p}}(u^2 - B) \geq 1$ can always be satisfied since the field $\mathbb{Z}_K/\mathfrak{p}$ is perfect. □

Remark. The same question can be asked for $v_{\mathfrak{p}}(A)$ even. In that case the answer seems to be much more complicated, but fortunately we will not need it.

Proposition 3.11. *Let $\mathfrak{p}$ be ramified in k/K so that $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}^2$, and let t be such that $1 \leq t \leq 2e(\mathfrak{p}) - v_{\mathfrak{p}}(\mathfrak{d})/2$. If $n \in K^*$, a necessary and sufficient condition for the solubility in k of $n/x^2 \equiv 1 \pmod{{}^*\mathfrak{p}^t\mathbb{Z}_k}$ is the following:*

(1) *If $v_{\mathfrak{p}}(n)$ is odd, then $t \leq v_{\mathfrak{p}}(\mathfrak{d})/2 - 1$.*
(2) *If $v_{\mathfrak{p}}(n)$ is even, then either $t \leq v_{\mathfrak{p}}(\mathfrak{d})/2$ or the congruence $n/x^2 \equiv 1 \pmod{{}^*\mathfrak{p}^{2t_1+1}}$ is soluble in K for $t_1 = \lceil (t - v_{\mathfrak{p}}(\mathfrak{d})/2)/2 \rceil$.*

Proof. (1). Choose a uniformizer π of $\mathfrak{p}$ in K. Multiplying if necessary n by a power of π^2, we may assume that $v_{\mathfrak{p}}(n) = 1$, hence $v_{\mathfrak{P}}(x) = 1$. Write $x = u + v\rho$ with u and v $\mathfrak{p}$-integral. Since $v_{\mathfrak{p}}(\mathcal{N}_{k/K}(x)) = 1$, we have $v_{\mathfrak{p}}(u^2 + uva - v^2 b) = 1$. Since $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{d})/2 > 0$ and $v_{\mathfrak{p}}(b) = 1$, it follows that we must have $v_{\mathfrak{p}}(u) > 0$, hence also that $v_{\mathfrak{p}}(v) = 0$, and conversely when these conditions are satisfied we clearly have $v_{\mathfrak{P}}(x) = 1$.

Replacing x by $u + v\rho$ in our congruence, and using Lemma 3.5, we obtain the two inequalities $v_{\mathfrak{p}}(u^2 + v^2 b - n) \geq t + 1$ and $v_{\mathfrak{p}}(2uv + v^2 a) \geq t + 1$. Since $v_{\mathfrak{p}}(v) = 0$, $v_{\mathfrak{p}}(u) \geq 1$, and $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{d})/2 \leq e$, it follows that $v_{\mathfrak{p}}(2uv + v^2 a) = v_{\mathfrak{p}}(\mathfrak{d})/2$ for any choice of u and v satisfying the valuation conditions, hence the second inequality can be satisfied if and only if $t \leq v_{\mathfrak{p}}(\mathfrak{d})/2 - 1$. Assume this is the case. The first equality is thus satisfied if and only if $v_{\mathfrak{p}}(v^2 + (\pi^2/b)w^2 - (n/b)) \geq t$ has a solution, and since $v_{\mathfrak{p}}(\pi^2/b) = 1$ and $v_{\mathfrak{p}}((n/b)) = 0$, Lemma 3.10 allows us to conclude that this can be satisfied, proving (1).

(2). In this case, once again by multiplying n by a power of π^2, we may assume that $v_{\mathfrak{p}}(n) = 0$, hence $v_{\mathfrak{P}}(x) = 0$, in other words $v_{\mathfrak{p}}(\mathcal{N}_{k/K}(x)) = 0$, i.e., $v_{\mathfrak{p}}(u) = 0$ if we replace x by $u + v\rho$.

Here we obtain the two inequalities $v_{\mathfrak{p}}(u^2 + v^2 b - n) \geq t$ and $v_{\mathfrak{p}}(2uv + v^2 a) \geq t$. If $t \leq v_{\mathfrak{p}}(\mathfrak{d})/2 = v_{\mathfrak{p}}(a) \leq e$, the second inequality is automatically satisfied, and since $v_{\mathfrak{p}}(b) = 1$ and $v_{\mathfrak{p}}(n) = 0$, we deduce from Lemma 3.10 that the first inequality can be satisfied for $t \leq 2e$, which is the case. Thus, assume from now on that $t > v_{\mathfrak{p}}(\mathfrak{d})/2 = v_{\mathfrak{p}}(a)$.

Lemma 3.12. *Assume $v_{\mathfrak{p}}(\mathfrak{d})/2 \leq t \leq 2e - v_{\mathfrak{p}}(\mathfrak{d})/2$. The inequality $v_{\mathfrak{p}}(2uv + v^2 a) \geq t$ is equivalent to $v_{\mathfrak{p}}(v) \geq (t - v_{\mathfrak{p}}(\mathfrak{d})/2)/2$.*

Proof. If $v_{\mathfrak{p}}(v) \geq e - v_{\mathfrak{p}}(\mathfrak{d})/2$, then $v_{\mathfrak{p}}(2uv + v^2 a) \geq 2e - v_{\mathfrak{p}}(\mathfrak{d})/2 \geq t$ by assumption. On the other hand, if $v_{\mathfrak{p}}(v) < e - v_{\mathfrak{p}}(\mathfrak{d})/2$, we have $v_{\mathfrak{p}}(2uv + v^2 a) = 2v_{\mathfrak{p}}(v) + v_{\mathfrak{p}}(\mathfrak{d})/2$, and this is greater than or equal to t if and only if $v_{\mathfrak{p}}(v) \geq (t - v_{\mathfrak{p}}(\mathfrak{d})/2)/2$. □

We will see below that condition $(*)$ implies in particular that $t \leq 2e - v_{\mathfrak{p}}(\mathfrak{d})/2$.

Thus, set $t_1 = \lceil (t - v_{\mathfrak{p}}(\mathfrak{d})/2)/2 \rceil$ and $v = \pi^{t_1} v_1$, so that $v_{\mathfrak{p}}(v_1) \geq 0$ by this lemma. Our first inequality thus reads $v_{\mathfrak{p}}(u^2 + v_1^2 A - n) \geq t$ with $A = \pi^{2t_1} b$. Since we clearly have $t \geq 2t_1 + 1$ and that $v_{\mathfrak{p}}(A)$ is odd, Lemma 3.10 implies that this is soluble if and only if $u^2 \equiv n \pmod{{}^*\mathfrak{p}^{2t_1+1}}$ is soluble in K, proving (2). Note for future reference that by Hecke's theorem, the solubility for $2t_1 + 1$ is equivalent to that for $2t_1$. □

Corollary 3.13. *Under the same assumptions, let $\mathfrak{C} = \mathfrak{P}^t$ for $1 \leq t \leq 2e(\mathfrak{p}) - v_{\mathfrak{p}}(\mathfrak{d})/2$. Then*

$$|\mathcal{Z}_{\mathfrak{C}^2}| = \begin{cases} 1 & \text{if } t \leq v_{\mathfrak{p}}(\mathfrak{d})/2 - 1 \\ 2\mathcal{N}\mathfrak{p}^{\lceil (t - v_{\mathfrak{p}}(\mathfrak{d})/2)/2 \rceil} & \text{if } t \geq v_{\mathfrak{p}}(\mathfrak{d})/2\,. \end{cases}$$

Proof. We first note the following easy lemma.

Lemma 3.14. *There exists a noncanonical surjective map h:*

$$(\mathbb{Z}_K/\mathfrak{p}^t)^* \times (\mathbb{Z}/2\mathbb{Z}) \longrightarrow \mathcal{Z}_{\mathfrak{p}^t \mathbb{Z}_k}\,.$$

Proof. Choose a uniformizer π of $\mathfrak{p}$ in K, and define the map h by $h(\overline{n},\overline{j}) = \overline{n\pi^j}$, with evident meanings for the $\overline{\ }$ signs. This clearly does not depend on the choice of representative of $\overline{n}$ (since $n \equiv 1 \pmod{\mathfrak{p}^t}$ implies $n \in Q_K(\mathfrak{p}^t\mathbb{Z}_k)$), nor on the representative of $\overline{j}$ (since $\pi^2 \in Q_K(\mathfrak{p}^t\mathbb{Z}_k)$), hence it is clearly a well defined group homomorphism. To show surjectivity, let $\overline{n} \in \mathcal{Z}_{\mathfrak{p}^t\mathbb{Z}_k}$, and let $n \in K^*$ be a representative. If $v = v_{\mathfrak{p}}(n)$ is even, then $(\overline{n/\pi^{-v}},\overline{0})$ is a preimage of $\overline{n}$, while if v is odd then $(\overline{n/\pi^{-v}},\overline{1})$ is a preimage of $\overline{n}$. □

To prove the corollary, we must compute the cardinality of the kernel of h. By definition $(\overline{n},\overline{j}) \in \operatorname{Ker} h$ if and only if $n\pi^j \in Q_K(\mathfrak{p}^t\mathbb{Z}_k)$, hence if and only if there exists $x \in k$ with $n\pi^j/x^2 \equiv 1 \pmod{\mathfrak{p}^t\mathbb{Z}_k}$. By Proposition 3.11, if $t \le v_{\mathfrak{p}}(\mathfrak{d})/2-1$ then the kernel of h is equal to all of $(\mathbb{Z}_K/\mathfrak{p}^t)^*\times(\mathbb{Z}/2\mathbb{Z})$, hence is of cardinality $2\phi_K(\mathfrak{p}^t)$, so that $|\mathcal{Z}_{\mathfrak{p}^t\mathbb{Z}_k}| = 1$ in that case. If $t \ge v_{\mathfrak{p}}(\mathfrak{d})/2$, the kernel of h is equal to the number of elements of $(\mathbb{Z}_K/\mathfrak{p}^t)^* \times \{\overline{0}\}$ which are squares in $(\mathbb{Z}_K/\mathfrak{p}^{2t_1})^*$, hence is of cardinality equal to $\phi_K(\mathfrak{p}^{t_1})\mathcal{N}\mathfrak{p}^{t-2t_1} = \phi_K(\mathfrak{p}^{t-t_1})$ since $t_1 > 0$ (note that this formula is also valid for $t = v_{\mathfrak{p}}(\mathfrak{d})/2$). Thus

$$|\mathcal{Z}_{\mathfrak{p}^t\mathbb{Z}_k}| = 2\phi_K(\mathfrak{p}^t)/\phi_K(\mathfrak{p}^{t-t_1}) = 2\mathcal{N}\mathfrak{p}^{t_1} ,$$

finishing the proof of the corollary. □

3.5. Study of Condition $(*)$ in the Ramified Case. The result is as follows.

Proposition 3.15. *Let $\mathfrak{C} = \mathfrak{P}^t$ with $t \le 2e$. Then $\mathfrak{C}$ satisfies condition $(*)$ if and only if $t \le t_{\max}$, with*

$$t_{\max} = \begin{cases} e - v_{\mathfrak{p}}(\mathfrak{d})/2 & \text{if } v_{\mathfrak{p}}(\mathfrak{d}) \ge e+1 \\ 2e+1-3v_{\mathfrak{p}}(\mathfrak{d})/2 & \text{if } v_{\mathfrak{p}}(\mathfrak{d}) \le e\ . \end{cases}$$

It is clear that, as claimed above, this implies that in all cases $t_{\max} \le 2e - v_{\mathfrak{p}}(\mathfrak{d})/2$.

Proof. Recall that the ideal $\mathfrak{C} = \mathfrak{P}^t$ satisfies $(*)$ if and only if there exists $\beta \equiv 1 \pmod{{}^*\mathfrak{p}^t\mathbb{Z}_k}$ such that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square of K or, equivalently, if it is equal to $D/\pi^{v_{\mathfrak{p}}(\mathfrak{d})}$ times a square of K which is a $\mathfrak{p}$-unit.

We first show that the values given in the proposition are upper bounds. Note first that if γ is a $\mathfrak{P}$-integer then $v_{\mathfrak{p}}(\operatorname{Tr}_{k/K}(\gamma)) \ge v_{\mathfrak{p}}(\mathfrak{d})/2$. Indeed, if we write $\gamma = u + v\rho$ with u and $v \in K$ $\mathfrak{p}$-integers, $\operatorname{Tr}_{k/K}(\gamma) = 2u + va$ and our claim follows since $e \ge v_{\mathfrak{p}}(\mathfrak{d})/2$.

Thus, if $\beta = 1 + \pi^t\gamma$ for γ a $\mathfrak{P}$-integer, we have

$$\mathcal{N}_{k/K}(\beta) = 1 + \pi^t \operatorname{Tr}_{k/K}(\gamma) + \pi^{2t}\mathcal{N}_{k/K}(\gamma) \equiv 1 \pmod{{}^*\mathfrak{p}^j} ,$$

with $j = \min(t + v_{\mathfrak{p}}(\mathfrak{d})/2, 2t)$. Our assumption on β implies that there exists $z \in K$ such that

$$D/\pi^{v_{\mathfrak{p}}(\mathfrak{d})} \equiv z^2 \pmod{{}^*\mathfrak{p}^j} .$$

On the other hand, we know that the maximal exponent k for which $D/\pi^{v_{\mathfrak{p}}(\mathfrak{d})}$ is congruent to a square modulo $\mathfrak{p}^k$ is $2e + 1 - v_{\mathfrak{p}}(\mathfrak{d})$. We thus obtain

$$\min(t + v_{\mathfrak{p}}(\mathfrak{d})/2, 2t) \le 2e + 1 - v_{\mathfrak{p}}(\mathfrak{d}) ,$$

which is easily seen to imply the upper bounds given for $t_{\max}$ in the proposition.

Conversely, we must show that these bounds are attained. It is clear that we may choose ω such that $v_{\mathfrak{p}}(\mathcal{N}_{k/K}(\omega)) = 0$. Write $\mathcal{N}_{k/K}(\omega) = D/\pi^{v_{\mathfrak{p}}(\mathfrak{d})/2} m_1^2$ and $D/\pi^{v_{\mathfrak{p}}(\mathfrak{d})} \equiv m_2^2 \pmod{{}^*\mathfrak{p}^{2e+1-v_{\mathfrak{p}}(\mathfrak{d})}}$ (in fact with $m_2 = a/\pi^{v_{\mathfrak{p}}(\mathfrak{d})/2}$). It follows that $\mathcal{N}_{k/K}(\omega) \equiv m^2 \pmod{{}^*\mathfrak{p}^{2e+1-v_{\mathfrak{p}}(\mathfrak{d})}}$ for some $m \in K$ such that $v_{\mathfrak{p}}(m) = 0$. We consider two cases.

The Case $v_{\mathfrak{p}}(\mathfrak{d}) \ge e + 1$

In this case, we are going to show that $\beta = \omega/m$ satisfies the desired conditions. It is clear that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square of K, hence we must only show the congruence condition.

Set $\omega = m + \gamma$, so that

$$\mathcal{N}_{k/K}(\omega) - m^2 = m \operatorname{Tr}_{k/K}(\gamma) + \mathcal{N}_{k/K}(\gamma) \equiv 0 \pmod{{}^*\mathfrak{p}^{2e+1-v_{\mathfrak{p}}(\mathfrak{d})}} .$$

We claim that $v_{\mathfrak{P}}(\gamma) \ge 2e + 1 - v_{\mathfrak{p}}(\mathfrak{d})$. Indeed, assume that we have shown that $v_{\mathfrak{P}}(\gamma) \ge e_n$, which is true with $e_0 = 0$. Thus, $\gamma/\pi^{\lfloor e_n/2 \rfloor}$ is a $\mathfrak{P}$-integer, so that $v_{\mathfrak{p}}(\operatorname{Tr}_{k/K}(\gamma)) \ge \lfloor e_n/2 \rfloor + v_{\mathfrak{p}}(\mathfrak{d})/2$, hence $v_{\mathfrak{p}}(N_{k/K}(\gamma)) \ge \min(\lfloor e_n/2 \rfloor + v_{\mathfrak{p}}(\mathfrak{d})/2, 2e + 1 - v_{\mathfrak{p}}(\mathfrak{d}))$, and since $v_{\mathfrak{p}}(\mathcal{N}_{k/K}(\gamma)) = v_{\mathfrak{P}}(\gamma)$, we can thus take

$$e_{n+1} = \min(\lfloor e_n/2 \rfloor + v_{\mathfrak{p}}(\mathfrak{d})/2, 2e + 1 - v_{\mathfrak{p}}(\mathfrak{d})) .$$

Assume first that $e_n < 4e + 2 - 3v_{\mathfrak{p}}(\mathfrak{d})$, so that in particular $e_n < v_{\mathfrak{p}}(\mathfrak{d}) - 2$, and also $e_n/2 < 2e + 1 - 3v_{\mathfrak{p}}(\mathfrak{d})/2$. Thus,

$$e_{n+1} - e_n = \lfloor (v_{\mathfrak{p}}(\mathfrak{d}) - e_n)/2 \rfloor \ge 1 ,$$

so as long as $e_n < 4e + 2 - 3v_{\mathfrak{p}}(\mathfrak{d})$ the sequence e_n is strictly increasing. Thus, for some n_0 (possibly $n_0 = 0$) we must have $e_{n_0} \ge 4e + 2 - 3v_{\mathfrak{p}}(\mathfrak{d})$. We then have $e_n = 2e + 1 - v_{\mathfrak{p}}(\mathfrak{d})$ for all $n \ge n_0 + 1$, so that $v_{\mathfrak{P}}(\gamma) \ge 2e + 1 - v_{\mathfrak{p}}(\mathfrak{d})$, proving our claim. It follows that $\beta = \omega/m \equiv 1 \pmod{{}^*\mathfrak{p}^{e - v_{\mathfrak{p}}(\mathfrak{d})/2} \mathbb{Z}_k}$, so condition $(*)$ is satisfied for $\mathfrak{C} = \mathfrak{P}^{t_{\max}}$ with $t_{\max} = e - v_{\mathfrak{p}}(\mathfrak{d})/2$, proving the proposition when $v_{\mathfrak{p}}(\mathfrak{d}) \ge e + 1$.

The Case $v_{\mathfrak{p}}(\mathfrak{d}) \le e$

We first prove the following lemma.

Lemma 3.16. *Recall that $m \in K^*$ is such that*

$$\mathcal{N}_{k/K}(\omega) \equiv m^2 \pmod{{}^*\mathfrak{p}^{2e+1-v_\mathfrak{p}(\mathfrak{d})}} .$$

If $v_\mathfrak{p}(\mathfrak{d}) \le e$, we may choose $\omega = r + s\rho$ (still coprime to $\mathfrak{P}$ with $\mathcal{N}_{k/K}(\omega) = Dz^2$ with $z \in K^*$) so that $v_\mathfrak{p}(s) = v_\mathfrak{p}(r-m) = v_\mathfrak{p}(\mathfrak{d})/2$.

Proof. Using the same notations and reasoning as above, we obtain once again the recursion

$$e_{n+1} = \min(\lfloor e_n/2 \rfloor + v_\mathfrak{p}(\mathfrak{d})/2, 2e + 1 - v_\mathfrak{p}(\mathfrak{d})) .$$

However, here the situation is different, and we can only claim that $v_\mathfrak{P}(\gamma) \ge v_\mathfrak{p}(\mathfrak{d}) - 1$. Indeed, assume $e_n \le v_\mathfrak{p}(\mathfrak{d})$, otherwise there is nothing to prove. Then $e_{n+1} - e_n = \lfloor (v_\mathfrak{p}(\mathfrak{d}) - e_n)/2 \rfloor$, so that we can assert that $e_{n+1} > e_n$ only as long as $e_n \le v_\mathfrak{p}(\mathfrak{d}) - 2$, so that for some n_0 we will have $e_{n_0} \ge v_\mathfrak{p}(\mathfrak{d}) - 1$, proving our claim. This shows that if $\omega = r + s\rho$ then $v_\mathfrak{p}(s) \ge v_\mathfrak{p}(\mathfrak{d})/2 - 1$.

We first need to go one step further. It is easily seen that $v_\mathfrak{P}(u + v\rho) \ge 1$ if and only if v is a $\mathfrak{p}$ integer and $v_\mathfrak{p}(u) \ge 1$. Since $v_\mathfrak{P}(\gamma) \ge v_\mathfrak{p}(\mathfrak{d}) - 1$, we can thus write $\gamma = \pi^{v_\mathfrak{p}(\mathfrak{d})/2-1}(\pi u + v\rho)$, where u and v are $\mathfrak{p}$-integers. The condition

$$v_\mathfrak{p}(m \operatorname{Tr}_{k/K}(\gamma) + \mathcal{N}_{k/K}(\gamma)) \ge 2e + 1 - v_\mathfrak{p}(\mathfrak{d}) > v_\mathfrak{p}(\mathfrak{d})$$

implies that $v_\mathfrak{p}(v(v - m(a/\pi^{v_\mathfrak{p}(\mathfrak{d})/2})(\pi/b))) \ge 1$. Thus, either $v_\mathfrak{p}(v) \ge 1$, in which case $v_\mathfrak{P}(\gamma) \ge v_\mathfrak{p}(\mathfrak{d})$ so that $\omega/m \equiv 1 \pmod{{}^*\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{d})/2}}$. Or we have $v \equiv m(a/\pi^{v_\mathfrak{p}(\mathfrak{d})/2})(\pi/b) \pmod{{}^*\mathfrak{p}}$. In that case, $\gamma \equiv ma\rho/b \pmod{{}^*\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{d})/2}\mathbb{Z}_k}$, so that

$$\omega/m \equiv (b + a\rho)/b \equiv \rho^2/b \pmod{{}^*\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{d})/2}\mathbb{Z}_k} .$$

Thus, changing if necessary ω into $\omega b/\rho^2$ (which clearly is still coprime to $\mathfrak{p}$ and has the same norm as ω), we may assume that $\omega/m \equiv 1 \pmod{{}^*\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{d})/2}}$.

Write $\omega = r + s\rho$ for some $\mathfrak{p}$-integral r and s. It follows from the above that we always have $v_\mathfrak{p}(s) \ge v_\mathfrak{p}(\mathfrak{d})/2 - 1$, and that if necessary by changing ω we may assume that $v_\mathfrak{p}(s) \ge v_\mathfrak{p}(\mathfrak{d})/2$ and $v_\mathfrak{p}(r-m) \ge v_\mathfrak{p}(\mathfrak{d})/2$.

Note that $v_\mathfrak{p}(r) = 0$. If we had $v_\mathfrak{p}(s) > v_\mathfrak{p}(\mathfrak{d})/2$, then it is easily checked that if $\omega' = \omega(1+\rho)^2 = r' + s'\rho$, then $s' \equiv r(a+2) \pmod{{}^*\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{d})/2+1}}$, and since $v_\mathfrak{p}(\mathfrak{d})/2 < v_\mathfrak{p}(\mathfrak{d}) \le e$, it follows that $v_\mathfrak{p}(s') = v_\mathfrak{p}(\mathfrak{d})/2$. Thus, by changing if necessary once again ω into $\omega(1+\rho)^2$ (which preserves all the necessary properties of ω), we may assume that $v_\mathfrak{p}(s) = v_\mathfrak{p}(\mathfrak{d})/2$. Finally, note that

$$v_\mathfrak{p}(\mathcal{N}_{k/K}(r+s\rho) - m^2) = v_\mathfrak{p}(r^2 - m^2 + ars - bs^2) \ge 2e+1-v_\mathfrak{p}(\mathfrak{d}) \ge v_\mathfrak{p}(\mathfrak{d})+1$$

and since $v_\mathfrak{p}(bs^2) = v_\mathfrak{p}(\mathfrak{d}) + 1$ and $v_\mathfrak{p}(ars) = v_\mathfrak{p}(\mathfrak{d})$, we must have

$$v_\mathfrak{p}(r^2 - m^2) = v_\mathfrak{p}(r-m) + v_\mathfrak{p}(r - m + 2m) = v_\mathfrak{p}(\mathfrak{d}) .$$

Since $v_{\mathfrak{p}}(r-m) \geq v_{\mathfrak{p}}(\mathfrak{d})/2$, it follows that $v_{\mathfrak{p}}(r-m+2m) \geq \min(v_{\mathfrak{p}}(\mathfrak{d})/2, e) = v_{\mathfrak{p}}(\mathfrak{d})/2$. Thus $v_{\mathfrak{p}}(r-m) \leq v_{\mathfrak{p}}(\mathfrak{d}) - v_{\mathfrak{p}}(\mathfrak{d})/2 = v_{\mathfrak{p}}(\mathfrak{d})/2$, so that $v_{\mathfrak{p}}(r-m) = v_{\mathfrak{p}}(\mathfrak{d})/2$, proving the lemma. □

We can now finish the proof of Proposition 3.15. If we set $q = (r-m)/s$ and $n = (q^2+b)/r$, a small computation gives

$$\omega n - (q+\rho)^2 = \rho((m^2 - \mathcal{N}_{k/K}(\omega))/(rs)) \ .$$

Thus, since by the above lemma $v_{\mathfrak{p}}(q) \geq 0$, $v_{\mathfrak{p}}(r) = 0$, $v_{\mathfrak{p}}(s) = v_{\mathfrak{p}}(\mathfrak{d})/2$, and since

$$\mathcal{N}_{k/K}(\omega) \equiv m^2 \pmod{{}^*\mathfrak{p}^{2e+1-v_{\mathfrak{p}}(\mathfrak{d})}} \ ,$$

it follows that $v_{\mathfrak{p}}(n) = 0$ and that if we set

$$\beta = \omega n/(q+\rho)^2 \equiv 1 \pmod{{}^*\mathfrak{p}^{2e+1-3v_{\mathfrak{p}}(\mathfrak{d})/2}} \ ,$$

then $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square of K, so condition $(*)$ is satisfied for $t = t_{\max} = 2e+1-3v_{\mathfrak{p}}(\mathfrak{d})/2$. This terminates the proof of Proposition 3.15. □

4. Globalization

We first recall the following results which we have seen at the beginning of this paper.

Lemma 4.1. *Let K be a number field, and $k = K(\sqrt{D})$ be a quadratic extension of K. The following conditions are equivalent.*

1. *There exists a quadratic extension L/k such that the quartic extension L/K is abelian with Galois group isomorphic to C_4 (in other words, k is embeddable in a C_4-extension).*
2. *There exists $\omega \in k^*$ such that $\mathcal{N}_{k/K}(\omega)$ is equal to D times a square of K^**
3. *There exist m and n in K such that $D = m^2 + n^2$.*

We will denote by $\mathcal{L}_K$ the set of isomorphism classes of such quadratic extensions k of K.

4.1. A Preliminary Formula for $c_K(C_4)$. We can then summarize the results of the preceding sections (in particular Theorem 2.3 and all of the results of Section 3) in the following theorem.

Theorem 4.2. *Let K be a number field of signature (r_1, r_2) and absolute degree $n = r_1 + 2r_2$. We have*

$$\Phi_{K,4}(C_4, s) = \frac{1}{2} \sum_{k \in \mathcal{L}_K} \frac{1}{\mathcal{N}(\mathfrak{d}(k/K))^{2s}} \Phi_k(s)$$

where, if we write $\mathfrak{d}$ *instead of* $\mathfrak{d}(k/K)$*, and if we denote by* $\omega_K(\mathfrak{d}) = |T|$ *the number of distinct prime ideals dividing* $\mathfrak{d}$*, we have*

$$\Phi_k(s) = \frac{2^{r_1+r_2+\omega_K(\mathfrak{d})}}{4^{2ns}\mathcal{N}(s(\mathfrak{d}))^s} \sum_{\substack{\mathfrak{C}|2\mathbb{Z}_k \\ (\mathfrak{C},s(\mathfrak{D}))=1 \\ \mathfrak{C} \text{ satisfies } (*)}} \frac{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s}}{|\mathcal{Z}_{\mathfrak{C}^2}|} \prod_{\mathfrak{P}|\mathfrak{C}} \left(1 - \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{P})^{2s}}\right) P_1(\mathfrak{C}) \ .$$

Here

$$P_1(\mathfrak{C}) = \sum_{\chi \in \widehat{\mathcal{G}_{\mathfrak{C}^2}(K)}} \chi(\mathfrak{a}_{\beta(\mathfrak{C}^2)}) \prod_{\mathfrak{p} \nmid \mathfrak{c}\mathfrak{d}} \left(1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{2s}}\right) \ ,$$

and $\beta(\mathfrak{C}^2)$ *is an element of* k *such that* $\beta(\mathfrak{C}^2) \equiv 1 \pmod{{}^*\mathfrak{C}^2}$ *with* $\mathcal{N}_{k/K}(\beta(\mathfrak{C}^2))$ *equal to* D *times a square of* K*.*

In the above, condition $(*)$ *is satisfied for* $\mathfrak{C}$ *if and only if for every ramified prime ideal* $\mathfrak{P}$ *dividing* $\mathfrak{C}$ *we have* $v_{\mathfrak{P}}(\mathfrak{C}) \le t_{\max}$*, with* $t_{\max}$ *given by Proposition 3.15,* $|\mathcal{Z}_{\mathfrak{C}^2}|$ *is equal to the product of its local components, these being given by Corollaries 3.7 and 3.13,* $\mathcal{G}_{\mathfrak{C}^2}(K) = Cl_{T,\mathfrak{C}^2}(K)/Cl_{T,\mathfrak{C}^2}(K)^2$*, and finally* $\mathfrak{a}_\beta$ *is the unique squarefree ideal of* K *coprime to* $\mathfrak{d}$ *such that* $\beta\mathbb{Z}_k = s(\mathfrak{D})\mathfrak{a}_\beta\mathfrak{Q}^2$*.*

To rearrange terms in this formula, we first introduce the following notations.

Definition. For any ideal $\mathfrak{c}$ of K dividing $4\mathbb{Z}_K$, we set

$$G(\mathfrak{c}) = Cl_{\mathfrak{c}}(K)/Cl_{\mathfrak{c}}(K)^2.$$

Then for any character χ on $G(\mathfrak{c})$ we define $\mathcal{L}_K(\chi)$ as being the subset of elements $k \in \mathcal{L}_K$ satisfying the following conditions, where as usual we set $\mathfrak{d} = \mathfrak{d}(k/K)$.

(1) If $\mathfrak{p} \mid \mathfrak{c}$ and $\mathfrak{p} \nmid \mathfrak{d}$ then $2 \mid v_{\mathfrak{p}}(\mathfrak{c})$.
(2) If $\mathfrak{p} \mid \mathfrak{c}$ and $\mathfrak{p} \mid \mathfrak{d}$ then $2 \mid v_{\mathfrak{p}}(\mathfrak{d})$ and $v_{\mathfrak{p}}(\mathfrak{c}) \le t_{\max}$.
(3) If $\mathfrak{p} \nmid \mathfrak{c}$ and $\mathfrak{p} \mid \mathfrak{d}$ then $\chi(\mathfrak{p}) = 1$.
(4) More generally if $z \in Q_K(\mathfrak{c}\mathbb{Z}_k)$ (see Definition 1.3) and $\mathfrak{b} \in < T >$ are such that $(z\mathfrak{b}, \mathfrak{c}) = 1$, then $\chi(z\mathfrak{b}) = 1$.

Theorem 4.3. *With the above notations, we have*

$$\Phi_{K,4}(C_4, s) = \frac{2^{r_1+r_2-1}}{4^{2ns}\zeta_K(4s)} \sum_{\mathfrak{c}|4\mathbb{Z}_K} \mathcal{N}\mathfrak{c}^{2s} \sum_{\chi \in \widehat{G(\mathfrak{c})}} L_K(\chi, 2s) F_{\mathfrak{c},\chi}(s) \ ,$$

where $\zeta_K(s)$ *is the Dedekind zeta function of* K*,* $L_K(\chi, s)$ *is the standard abelian* L*-function,*

$$F_{\mathfrak{c},\chi}(s) = \sum_{k \in \mathcal{L}_K(\chi)} \frac{\chi(\mathfrak{a}_{\beta(\mathfrak{c})})}{|\mathcal{Z}_{\mathfrak{C}^2}|} \frac{2^{\omega_K(\mathfrak{d})}}{\mathcal{N}(\mathfrak{d})^{2s}\mathcal{N}(s(\mathfrak{d}))^s \prod_{\mathfrak{p}|\mathfrak{d}}(1 + 1/\mathcal{N}\mathfrak{p}^{2s})} \ ,$$

and $\mathfrak{C}$ *is any ideal of* k *such that* $\mathfrak{C}^2 \cap K = \mathfrak{c}$.

Proof. It is clear that $\mathcal{G}_{\mathfrak{C}^2}(K)$ is a quotient of $G(\mathfrak{c})$, and that χ is a character of $\mathcal{G}_{\mathfrak{C}^2}(K)$ if and only if χ can be considered as a character of $G(\mathfrak{c})$ such that $\chi(z\mathfrak{b}) = 1$ for any pair $(z, \mathfrak{b})$ with $z \in Q_K(\mathfrak{C}^2)$, $\mathfrak{b} \in < T >$, and $(z\mathfrak{b}, \mathfrak{c}) = 1$.

In addition, we note that by Corollary 3.7, $|\mathcal{Z}_{\mathfrak{C}^2}|$ does not depend on the ideal $\mathfrak{C}$ such that $\mathfrak{C}^2 \cap K = \mathfrak{c}$. Similarly, by Corollary 3.9, there exists $\beta \equiv 1 \pmod{\mathfrak{C}^2}$ such that $\mathcal{N}_{k/K}(\beta)$ is equal to D times a square of K if and only if such a β exists with $\beta \equiv 1 \pmod{\mathfrak{c}\mathbb{Z}_k}$, so we may assume that we choose $\beta(\mathfrak{C}^2) = \beta(\mathfrak{c}\mathbb{Z}_k)$. Finally, by the same corollaries we have $Q_K(\mathfrak{C}^2) = Q_K(\mathfrak{c}\mathbb{Z}_k)$. Thus the only term which still depends explicitly on the ideal $\mathfrak{C}$ such that $\mathfrak{C}^2 \cap K = \mathfrak{c}$ is the following sum:

$$T(\mathfrak{c}) = \sum_{\mathfrak{C} | 2\mathbb{Z}_k} \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{C})^{2s} \prod_{\mathfrak{P} | \mathfrak{C}} \left(1 - \frac{1}{\mathcal{N}_{k/\mathbb{Q}}(\mathfrak{P})^{2s}}\right) .$$

This is given by the following lemma.

Lemma 4.4. *We have*

$$T(\mathfrak{c}) = \mathcal{N}\mathfrak{c}^{2s} \prod_{\mathfrak{p} | \mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right) \prod_{\mathfrak{p} | \mathfrak{c},\ \mathfrak{p} \nmid \mathfrak{d}} \left(1 + \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right) .$$

Proof. It is clear that $T(\mathfrak{c})$ is multiplicative. If $\mathfrak{c} = \mathfrak{p}^{2t}$ with $\mathfrak{p}$ inert then $\mathfrak{C} = \mathfrak{p}^t\mathbb{Z}_k$, and if $\mathfrak{c} = \mathfrak{p}^t$ with $\mathfrak{p}$ ramified then $\mathfrak{C} = \mathfrak{P}^t$, and the given formula is clear. So assume that $\mathfrak{c} = \mathfrak{p}^{2t}$ with $\mathfrak{p}$ split as $\mathfrak{p}\mathbb{Z}_k = \mathfrak{P}\overline{\mathfrak{P}}$. Then $\mathfrak{C} = \mathfrak{P}^{t_1}\overline{\mathfrak{P}}^{t_2}$ with $\max(t_1, t_2) = t$. By separating the terms $(t_1, t_2) = (0, t)$, $(t_1, t_2) = (t_1, t)$ with $1 \le t_1 \le t - 1$, $(t_1, t_2) = (t, 0)$, and $(t_1, t_2) = (t, t_2)$ with $1 \le t_2 \le t$, we find that

$$T(\mathfrak{c}) = \mathcal{N}\mathfrak{p}^{4ts} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^{4s}}\right) ,$$

corresponding to the formula given in the lemma. □

Finally, it is easy to check that we have

$$\prod_{\mathfrak{p} | \mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right) \frac{\prod_{\mathfrak{p} | \mathfrak{c},\ \mathfrak{p} \nmid \mathfrak{d}} \left(1 + \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right)}{\prod_{\mathfrak{p} | \mathfrak{d},\ \mathfrak{p} \nmid \mathfrak{c}} \left(1 + \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right)} \prod_{\mathfrak{p} \nmid \mathfrak{c}} \left(1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{2s}}\right) = \frac{L_K(\chi, 2s)}{\zeta_K(4s) \prod_{\mathfrak{p} | \mathfrak{d}} (1 + 1/\mathcal{N}\mathfrak{p}^{2s})} ,$$

hence using the above lemma and rearranging terms with $\mathfrak{c}$ and χ fixed is easily seen to give the formula of the theorem. □

Corollary 4.5. (1) *The function $\Phi_{K,4}(C_4,s)$ converges absolutely for $\mathrm{Re}(s)>1/2$ and extends analytically to $\mathrm{Re}(s)>1/3$ into a meromorphic function with a simple pole at $s=1/2$ having a residue equal to $c_K(C_4)/2$, where*

$$c_K(C_4)=\frac{1}{2^{n+r_2+1}}\frac{\zeta_K(1)}{\zeta_K(2)}\sum_{\mathfrak{c}\mid 4\mathbb{Z}_K}\mathcal{N}\mathfrak{c}\prod_{\mathfrak{p}\mid\mathfrak{c}}\left(1-\frac{1}{\mathcal{N}\mathfrak{p}}\right)F_{\mathfrak{c},1}(1/2)\ ,$$

with

$$F_{\mathfrak{c},1}(1/2)=\sum_{k\in\mathcal{L}_K(1)}\frac{1}{|\mathcal{Z}_{\mathfrak{c}^2}|}\frac{2^{\omega_K(\mathfrak{d})}}{\mathcal{N}(\mathfrak{d})\,\mathcal{N}(s(\mathfrak{d}))^{1/2}\prod_{\mathfrak{p}\mid\mathfrak{d}}(1+1/\mathcal{N}\mathfrak{p})}\ .$$

(2) *The number of C_4-extensions of K up to isomorphism whose ideal discriminant has norm less than or equal to X satisfies*

$$N_{K,4}(C_4,X)=c_K(C_4)\cdot X^{1/2}+O(X^{1/3+\varepsilon})$$

for all $\varepsilon>0$.

Proof. Note first that by Hecke's theorem we have $\mathfrak{d}=\mathfrak{d}(k/K)=4\mathfrak{a}/\mathfrak{c}^2$ for a suitable squarefree ideal $\mathfrak{a}$ of K, hence $\mathfrak{d}/s(\mathfrak{d})=4/\mathfrak{c}^2$ so that $\mathcal{N}(\mathfrak{d})/\mathcal{N}(s(\mathfrak{d}))\le\mathcal{N}(4\mathbb{Z}_K)=4^n$. Thus, for any $\varepsilon>0$ the Dirichlet series $F_{\mathfrak{c},\chi}(s)$ is termwise bounded from above by $A_\varepsilon\sum_{k\in\mathcal{L}_K}\mathcal{N}(\mathfrak{d})^{-(3s-\varepsilon)}$ for a suitable constant A_ε depending on ε, and it is well known and easy that this series converges absolutely for $3s-\varepsilon>1$, proving that $F_{\mathfrak{c},\chi}(s)$ converges absolutely for $\mathrm{Re}(s)>1/3$. On the other hand, the L-functions $L_K(\chi,2s)$ extend to the whole complex plane to holomorphic functions if χ is not the trivial character, and to meromorphic functions with a simple pole at $s=1/2$ of residue $(1/2)\zeta_K(1)\prod_{\mathfrak{p}\mid\mathfrak{c}}(1-1/\mathcal{N}\mathfrak{p})$ if χ is the trivial character modulo $\mathfrak{c}$. Since $\Phi_{K,4}(C_4,s)$ is a finite linear combination of expressions of the form $L_K(\chi,2s)F_{\mathfrak{c},\chi}(s)$, the first part of the corollary follows. The second part is an immediate consequence of the first, using standard contour integration techniques. □

Remark. It is not difficult to prove that $F_{\mathfrak{c},\chi}(s)$ extends to a meromorphic function to $\mathrm{Re}(s)>1/4$ with a simple pole at $s=1/3$ whose residue can be computed. Thus, in the case $K=\mathbb{Q}$ only, it is possible to prove a refined formula of the form

$$N_{\mathbb{Q},4}(C_4,X)=c_{\mathbb{Q}}(C_4)\cdot X^{1/2}+c'_{\mathbb{Q}}(C_4)X^{1/3}+O(X^{1/4+\varepsilon})\ ,$$

see [7] for the value of the constants.

The formula given above for $c_K(C_4)$ can be considerably simplified.

Corollary 4.6. *We have*

$$c_K(C_4)=\frac{1}{2^{r_2+1}}\frac{\zeta_K(1)}{\zeta_K(2)}\sum_{k\in\mathcal{L}_K}\frac{2^{\omega_K(\mathfrak{d})}}{\mathcal{N}(\mathfrak{d})^{3/2}\prod_{\mathfrak{p}\mid\mathfrak{d}}(1+1/\mathcal{N}\mathfrak{p})}\ .$$

Proof. First note that by Hecke's theorem, if $\mathfrak{p} \mid 2$ we have either $v_{\mathfrak{p}}(\mathfrak{d}) \equiv 0 \pmod 2$ or $v_{\mathfrak{p}}(\mathfrak{d}) = 2e(\mathfrak{p}) + 1$. Thus

$$\mathcal{N}(s(\mathfrak{d}))^{-1/2} = \mathcal{N}(\mathfrak{d})^{-1/2} \prod_{\substack{\mathfrak{p}\mid 2\\ v_{\mathfrak{p}}(\mathfrak{d})\equiv 0 \pmod 2}} \mathcal{N}\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{d})/2} \prod_{\substack{\mathfrak{p}\mid 2\\ v_{\mathfrak{p}}(\mathfrak{d})\equiv 1 \pmod 2}} \mathcal{N}\mathfrak{p}^{e(\mathfrak{p})} .$$

On the other hand, thanks to Corollary 4.5 we have

$$c_K(C_4) = \frac{1}{2^{n+r_2+1}} \frac{\zeta_K(1)}{\zeta_K(2)} \sum_{k\in\mathcal{L}_K} \frac{2^{\omega_K(\mathfrak{d})}}{\mathcal{N}(\mathfrak{d})\,\mathcal{N}(s(\mathfrak{d}))^{1/2} \prod_{\mathfrak{p}\mid\mathfrak{d}}(1+1/\mathcal{N}\mathfrak{p})} U_k$$

with

$$U_k = \sum_{\substack{\mathfrak{c}\mid 4\mathbb{Z}_K\\ (\mathfrak{c},s(\mathfrak{d}))=1\\ \mathfrak{p}\mid\mathfrak{c} \text{ and } \mathfrak{p}\nmid\mathfrak{d} \Longrightarrow v_{\mathfrak{p}}(\mathfrak{c})\equiv 0 \pmod 2}} \frac{\mathcal{N}\mathfrak{c}}{|\mathcal{Z}_{\mathfrak{C}^2}|} \prod_{\mathfrak{p}\mid\mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}}\right) .$$

It is clear that $U_k = \prod_{\mathfrak{p}\mid 2} U_{k,\mathfrak{p}}$, where the sums $U_{k,\mathfrak{p}}$ are the same as U_k but restricted to ideals $\mathfrak{c} \mid 4$ which are powers of a single prime ideal $\mathfrak{p}$.

When $\mathfrak{p}$ is inert or split, we know from Corollary 3.7 that for $\mathfrak{c} = \mathfrak{p}^{2t}$ we have $|\mathcal{Z}_{\mathfrak{C}^2}| = \mathcal{N}\mathfrak{p}^t$, and since t varies between 0 and $e(\mathfrak{p})$, a trivial computation gives $U_{k,\mathfrak{p}} = \mathcal{N}\mathfrak{p}^{e(\mathfrak{p})}$.

When $\mathfrak{p}$ is ramified, we consider two cases.

• If $v_{\mathfrak{p}}(\mathfrak{d}) \geq e(\mathfrak{p}) + 1$, then $t_{\max} = e(\mathfrak{p}) - v_{\mathfrak{p}}(\mathfrak{d})/2 \leq v_{\mathfrak{p}}(\mathfrak{d})/2$, hence using Corollary 3.13, another trivial computation gives $U_{k,\mathfrak{p}} = \mathcal{N}\mathfrak{p}^{e(\mathfrak{p})-v_{\mathfrak{p}}(\mathfrak{d})/2}$.

• If $v_{\mathfrak{p}}(\mathfrak{d}) \leq e(\mathfrak{p})$, then $t_{\max} = 2e(\mathfrak{p}) + 1 - 3v_{\mathfrak{p}}(\mathfrak{d})/2$. Using Corollary 3.13 and separating the term $t = 0$, the terms with $1 \leq t \leq v_{\mathfrak{p}}(\mathfrak{d})/2 - 1$ and the terms with $v_{\mathfrak{p}}(\mathfrak{d})/2 \leq t \leq t_{\max}$, a small computation gives again $U_{k,\mathfrak{p}} = \mathcal{N}\mathfrak{p}^{e(\mathfrak{p})-v_{\mathfrak{p}}(\mathfrak{d})/2}$. It follows that this formula is valid for any prime $\mathfrak{p}$ dividing 2, ramified or not, so that

$$U_k = \prod_{\substack{\mathfrak{p}\mid 2\\ v_{\mathfrak{p}}(\mathfrak{d})\equiv 0 \pmod 2}} \frac{\mathcal{N}\mathfrak{p}^{e(\mathfrak{p})}}{\mathcal{N}\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{d})/2}} .$$

Putting everything together, we obtain the formula of the corollary. □

4.2. Computation of $c_K(C_4)$. We will now start the computation of the final formula for $c_K(C_4)$, which does not involve the intermediate quadratic extensions k/K. To simplify notations, we denote by $Q_2(K)$ the subgroup of elements of K^* which are sums of two squares of K^*, and $s(\mathfrak{a})$ will denote the squarefree part of an ideal $\mathfrak{a}$ in K.

We begin by the following proposition.

Proposition 4.7. *Let $\mathfrak{a}$ be a fractional ideal of K. The following conditions are equivalent.*

(1) *There exists an ideal $\mathcal{A}$ of $K(i)$ such that $\mathfrak{a} = \mathcal{N}_{K(i)/K}(\mathcal{A})$.*
(2) *If $\mathfrak{p}$ is a prime ideal dividing $s(\mathfrak{a})$, then $\mathfrak{p}$ is not inert in $K(i)/K$ (no condition if $K(i) = K$).*

Furthermore, if there exists an ideal $\mathfrak{q}$ and an element $D \in Q_2(K)$ such that $\mathfrak{a}\mathfrak{q}^2 = D\mathbb{Z}_K$ then these conditions are satisfied.

Proof. If $\mathfrak{p}$ is inert in $K(i)/K$ then if $\mathfrak{a} = \mathcal{N}_{K(i)/K}(\mathcal{A})$ we have $v_{\mathfrak{p}}(\mathfrak{a}) = 2v_{\mathfrak{p}\mathbb{Z}_{K(i)}}(\mathcal{A}) \equiv 0 \pmod 2$, hence $\mathfrak{p} \nmid s(\mathfrak{a})$. Conversely, if this is the case for all inert primes $\mathfrak{p}$, we can write $\mathfrak{a} = s(\mathfrak{a})\mathfrak{b}^2$ and it is clear that if we set

$$\mathcal{A} = \mathfrak{b}\mathbb{Z}_{K(i)} \prod_{\mathfrak{p} \mid s(\mathfrak{a})} \mathfrak{P} \, ,$$

where for each $\mathfrak{p} \mid s(\mathfrak{a})$, $\mathfrak{P}$ denotes an ideal of $K(i)$ above $\mathfrak{p}$, then $\mathcal{N}_{K(i)/K}(\mathcal{A}) = \mathfrak{a}$, proving the equivalence of (1) and (2).

Finally, if $\mathfrak{a}\mathfrak{q}^2 = D\mathbb{Z}_K$ with $D = m^2 + n^2$, we clearly have

$$\mathfrak{a} = \mathcal{N}_{K(i)/K}((m + in)\mathfrak{q}^{-1}) \, ,$$

proving the last statement. □

Definition. Let $\mathfrak{c} \mid 2\mathbb{Z}_K$.

(1) We denote by $\mathcal{I}^q$ the group of fractional ideals $\mathfrak{a}$ of K satisfying the equivalent conditions of the above proposition.
(2) We set

$$Cl^q_{\mathfrak{c}^2}(K) = \frac{\{\mathfrak{a} \in \mathcal{I}^q, \ (\mathfrak{a}, \mathfrak{c}) = 1\}}{\{\beta\mathbb{Z}_K, \ \beta \in Q_2(K), \ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}\}}$$

(note that when $\beta \in Q_2(K)$ we indeed have $\beta\mathbb{Z}_K \in \mathcal{I}^q$ by the above proposition).
(3) We set

$$\mathcal{D}^q_{\mathfrak{c}^2}(K) = \frac{\{\mathfrak{q}^2\beta, \ (\mathfrak{q}, \mathfrak{c}) = 1, \ \beta \in Q_2(K), \ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}\}}{\{\beta\mathbb{Z}_K, \ \beta \in Q_2(K), \ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}\}}$$

and $G^q(\mathfrak{c}^2) = Cl^q_{\mathfrak{c}^2}(K)/\mathcal{D}^q_{\mathfrak{c}^2}(K)$.
(4) We define $S^q_{\mathfrak{c}^2}(K)$ as the subgroup of elements $\overline{u}$ in the Selmer group $S(K)$ such that for any lift $u \in K^*$ we have $u \in Q_2(K)$ and $u/x^2 \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ soluble in K.
(5) In all the above notations, we omit the subscript $_{\mathfrak{c}^2}$ when $\mathfrak{c} = \mathbb{Z}_K$.

Note that in this section all the Hecke congruences will be in K, not in any larger field.

We will set

$$\Psi_K(s) = 1 + \sum_{k \in \mathcal{L}_K} \frac{2^{\omega_K(\mathfrak{d})}}{\mathcal{N}(\mathfrak{d})^s \prod_{\mathfrak{p}|\mathfrak{d}}(1+1/\mathcal{N}\mathfrak{p})} \cdot$$

The aim of this section is to compute $\Psi_K(s)$, once again using Hecke's description of discriminants of relative quadratic extensions. This will give us the following theorem.

Theorem 4.8. *For any ideal $\mathfrak{c} \mid 2\mathbb{Z}_K$, denote by $h(\mathfrak{c})$ the number of prime ideals dividing $2\mathbb{Z}_K/\mathfrak{c}$ which are either unramified in $K(i)/K$ or which divide $\mathfrak{c}$ and are ramified in $K(i)/K$ (thus no additional condition if $i \in K$). Set $r_z = 1$ if $i \notin K$ and $r_z = 0$ otherwise. We then have*

$$c_K(C_4) = \frac{1}{2^{r_2+1}} \frac{\zeta_K(1)}{\zeta_K(2)} (\Psi_K(3/2) - 1) \ ,$$

with

$$\Psi_K(s) = \frac{2^{r_2+r_z}}{4^{ns}} \sum_{\mathfrak{c}|2\mathbb{Z}_K} 2^{h(\mathfrak{c})} \mathcal{N}(\mathfrak{c})^{2s-1} P(\mathfrak{c}, s) S(\mathfrak{c}, s) \ ,$$

where

$$P(\mathfrak{c}, s) = \frac{1}{\prod_{\mathfrak{p}|2/\mathfrak{c}}(1+1/\mathcal{N}\mathfrak{p})} \prod_{\mathfrak{p}|(\mathfrak{c},2/\mathfrak{c})} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right) \times \prod_{\mathfrak{p}|\mathfrak{c},\ \mathfrak{p}\nmid 2/\mathfrak{c}} \left(1 - \frac{2}{\mathcal{N}\mathfrak{p}^{2s}(1+1/\mathcal{N}\mathfrak{p})}\right) \ ,$$

$$S(\mathfrak{c}, s) = \sum_{\chi \in \widehat{G^q(\mathfrak{c}^2)}} \prod_{\mathfrak{p}|2,\ \mathfrak{p}\nmid\mathfrak{c},\ \mathfrak{p}\in\mathcal{I}^q} \left(1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s}\right) \times \prod_{\mathcal{N}\mathfrak{p}\equiv 1 \pmod 4} \left(1 + \frac{2\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s(1+1/\mathcal{N}\mathfrak{p})}\right) \ .$$

Proof. We follow quite closely Section 2, but in a different context, hence we are brief.

Proposition 4.9. *There exists a noncanonical one-to-one correspondence between elements of $\mathcal{L}_K$ together with the trivial extension K/K and pairs $(\mathfrak{a}, \overline{u})$, where $\mathfrak{a}$ is a squarefree ideal whose class belongs to $\mathcal{D}^q$ and $\overline{u} \in S^q(K)$. The (isomorphism class of) extension $k \in \mathcal{L}_K$ corresponding to $(\mathfrak{a}, \overline{u})$ is $k = K(\sqrt{D_0 u})$, where $\mathfrak{a}\mathfrak{q}_0^2 = D_0\mathbb{Z}_K$ with $D_0 \in Q_2(K)$ fixed.*

Proof. Clear from the definitions. □

Denote by $\mathcal{I}$ the set of squarefree ideals whose class belongs to $\mathcal{D}^q(K)$ (this conflicts with the notation used in Section 2, which will not be used anymore), so that $\mathcal{I} \subset \mathcal{I}^q$ by Proposition 4.7. By the above proposition

and Hecke's theorem, we have with an evident notation analogous to that used in Section 2

$$\Psi_K(s) = \sum_{\mathfrak{a}\in\mathcal{I}} \sum_{\overline{u}\in S^q(K)} \frac{2^{\omega_K(4\mathfrak{a}/\mathfrak{c}(D_0u)^2)}}{\mathcal{N}(4\mathfrak{a}/\mathfrak{c}(D_0u)^2)^s \prod_{\mathfrak{p}|4\mathfrak{a}/\mathfrak{c}(D_0u)^2}(1+1/\mathcal{N}\mathfrak{p})}$$
$$= \frac{1}{4^{ns}} \sum_{\mathfrak{c}|2\mathbb{Z}_K} \mathcal{N}(\mathfrak{c})^{2s} \frac{2^{\omega_K(2/\mathfrak{c})}}{\prod_{\mathfrak{p}|2/\mathfrak{c}}(1+1/\mathcal{N}\mathfrak{p})} \sum_{\substack{\mathfrak{a}\in\mathcal{I}\\(\mathfrak{a},\mathfrak{c})=1}} \frac{g_{D_0}(\mathfrak{c})2^{\omega_K(\mathfrak{a}_{\mathrm{odd}})}}{\mathcal{N}(\mathfrak{a})^s \prod_{\mathfrak{p}|\mathfrak{a}_{\mathrm{odd}}}(1+1/\mathcal{N}\mathfrak{p})}$$

where $\mathfrak{a}_{\mathrm{odd}}$ denotes the part of the ideal $\mathfrak{a}$ coprime to 2 (i.e., $\mathfrak{a}/(\mathfrak{a}, 2\mathbb{Z}_K)$ since $\mathfrak{a}$ is squarefree), and

$$g_{D_0}(\mathfrak{c}) = \sum_{\substack{\overline{u}\in S^q(K)\\ \mathfrak{c}(D_0u)=\mathfrak{c}}} 1 \, .$$

Similarly to what we did in Section 2, we set

$$f_{D_0}(\mathfrak{c}) = \sum_{\substack{\overline{u}\in S^q(K)\\ \mathfrak{c}(D_0u)|\mathfrak{c}}} 1 = \sum_{\substack{\overline{u}\in S^q(K)\\ \exists x,\ D_0u/x^2\equiv 1 \pmod{\mathfrak{c}^2}}} 1 \, ,$$

and once again a version of the Möbius inversion formula gives

$$g_{D_0}(\mathfrak{c}) = \sum_{\substack{\mathfrak{c}_1,\ \mathfrak{c}|\mathfrak{c}_1|2\mathbb{Z}_K\\(\mathfrak{c}_1,\mathfrak{a})=1}} \mu_K(\mathfrak{c}_1/\mathfrak{c}) f_{D_0}(\mathfrak{c}_1) \, .$$

Replacing in our formula for $\Psi_K(s)$, we obtain

$$\Psi_K(s) = \frac{1}{4^{ns}} \sum_{\mathfrak{c}_1|2\mathbb{Z}_K} \mathcal{N}(\mathfrak{c}_1)^{2s} Q(\mathfrak{c}_1, s) \sum_{\substack{\mathfrak{a}\in\mathcal{I}\\(\mathfrak{a},\mathfrak{c})=1}} \frac{f_{D_0}(\mathfrak{c})}{\mathcal{N}(\mathfrak{a})^s} \, ,$$

with

$$Q(\mathfrak{c}_1, s) = \sum_{\mathfrak{c}|\mathfrak{c}_1} \frac{\mu_K(\mathfrak{c}_1/\mathfrak{c}) 2^{\omega_K(2/\mathfrak{c})}}{\mathcal{N}(\mathfrak{c}_1/c)^{2s} \prod_{\mathfrak{p}|2/\mathfrak{c}}(1+1/\mathcal{N}\mathfrak{p})} \, .$$

A small computation gives

$$Q(\mathfrak{c}, s) = \frac{2^{\omega_K(2/\mathfrak{c})}}{\prod_{\mathfrak{p}|2/\mathfrak{c}}(1+1/\mathcal{N}\mathfrak{p})} \prod_{\mathfrak{p}|(\mathfrak{c},2/\mathfrak{c})} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^{2s}}\right)$$
$$\times \prod_{\mathfrak{p}|\mathfrak{c},\ \mathfrak{p}\nmid 2/\mathfrak{c}} \left(1 - \frac{2}{\mathcal{N}\mathfrak{p}^{2s}(1+1/\mathcal{N}\mathfrak{p})}\right) \, .$$

On the other hand, we have the following result.

Proposition 4.10. *We have $f_{D_0}(\mathfrak{c}) \neq 0$ if and only if the class of $\mathfrak{a}$ belongs to $\mathcal{D}^q_{\mathfrak{c}^2}(K)$. In that case, we have $f_{D_0}(\mathfrak{c}) = |S^q_{\mathfrak{c}^2}(K)|$.*

Proof. Assume that there exists $\overline{u} \in S^q(K)$ and $x \in K^*$ such that $D_0 u/x^2 \equiv 1 \pmod{{}^*\mathfrak{c}^2}$, in other words $\beta x^2 = D_0 u$ with $\beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}$. Since D_0 and u are in $Q_2(K)$, it follows that $\beta \in Q_2(K)$. Thus, we have $\mathfrak{a} = \beta\mathfrak{q}^2$ for some ideal $\mathfrak{q}$, which we may assume coprime to $\mathfrak{c}$ by changing x if necessary, and this exactly means that the class of $\mathfrak{a}$ belongs to $\mathcal{D}^q_{\mathfrak{c}^2}(K)$. Similarly, it is easy to show that this condition implies that $f_{D_0}(\mathfrak{c}) \neq 0$.

Finally, assume that $f_{D_0}(\mathfrak{c}) \neq 0$, and let $\overline{v} \in S^q(K)$ such that $D_0 v = x_0^2 \beta_0$ with $\beta_0 \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ and $\beta_0 \in Q_2(K)$. Clearly $D_0 u = x^2\beta$ if and only if $u/v = (x/x_0)^2(\beta/\beta_0)$ hence if and only if $u \in vS^q_{\mathfrak{c}^2}(K)$, proving the proposition. □

Recall that we have set $G^q(\mathfrak{c}^2) = Cl^q_{\mathfrak{c}^2}(K)/\mathcal{D}^q_{\mathfrak{c}^2}(K)$. If we denote by $\mathcal{J}$ the set of squarefree ideals belonging to $\mathcal{I}^q$, we have thus

$$\Psi_K(s) = \frac{1}{4^{ns}} \sum_{\mathfrak{c} \mid 2\mathbb{Z}_K} |S^q_{\mathfrak{c}^2}(K)|\, \mathcal{N}(\mathfrak{c})^{2s} Q(\mathfrak{c}, s) \sum_{\substack{\mathfrak{a} \in \mathcal{I} \\ \overline{\mathfrak{a}} \in \mathcal{D}^q_{\mathfrak{c}^2}(K)}} \frac{2^{\omega_K(\mathfrak{a}_{\mathrm{odd}})}}{\mathcal{N}(\mathfrak{a})^s \prod_{\mathfrak{p} \mid \mathfrak{a}_{\mathrm{odd}}} (1 + 1/\mathcal{N}\mathfrak{p})}$$

$$= \frac{1}{4^{ns}} \sum_{\mathfrak{c} \mid 2\mathbb{Z}_K} \frac{|S^q_{\mathfrak{c}^2}(K)|}{|G^q(\mathfrak{c}^2)|} \mathcal{N}(\mathfrak{c})^{2s} Q(\mathfrak{c}, s) S(\mathfrak{c}, s)\ ,$$

where $Q(\mathfrak{c}, s)$ is given above and

$$S(\mathfrak{c}, s) = \sum_{\chi \in \widehat{G^q(\mathfrak{c}^2)}} \sum_{\mathfrak{a} \in \mathcal{J}} \frac{\chi(\mathfrak{a}) 2^{\omega_K(\mathfrak{a}_{\mathrm{odd}})}}{\mathcal{N}(\mathfrak{a})^s \prod_{\mathfrak{p} \mid \mathfrak{a}_{\mathrm{odd}}} (1 + 1/\mathcal{N}\mathfrak{p})}$$

$$= \sum_{\chi \in \widehat{G^q(\mathfrak{c}^2)}} \prod_{\mathfrak{p} \mid 2,\ \mathfrak{p} \nmid \mathfrak{c},\ \mathfrak{p} \in \mathcal{I}^q} \left(1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s}\right) \prod_{\mathfrak{p} \nmid 2,\ \mathfrak{p} \in \mathcal{I}^q} \left(1 + \frac{2\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s (1 + 1/\mathcal{N}\mathfrak{p})}\right)$$

$$= \sum_{\chi \in \widehat{G^q(\mathfrak{c}^2)}} \prod_{\mathfrak{p} \mid 2,\ \mathfrak{p} \nmid \mathfrak{c},\ \mathfrak{p} \in \mathcal{I}^q} \left(1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s}\right) \prod_{\substack{\mathcal{N}\mathfrak{p} \equiv 1 \\ (\mathrm{mod}\ 4)}} \left(1 + \frac{2\chi(\mathfrak{p})}{\mathcal{N}\mathfrak{p}^s (1 + 1/\mathcal{N}\mathfrak{p})}\right)\ ,$$

since it is easily shown that if $\mathfrak{p} \nmid 2$, then $\mathfrak{p}$ is not inert in $K(i)$ (i.e., is split) if and only if $x^2 \equiv -1 \pmod{{}^*\mathfrak{p}}$ is soluble in K, hence if and only if $\mathcal{N}\mathfrak{p} \equiv 1 \pmod 4$.

Finally, we need to compute $|S^q_{\mathfrak{c}^2}(K)|$. For this, we first need the following definitions and results.

Definition. We define $(\mathbb{Z}_K/\mathfrak{c}^2)^q$ as the subgroup of elements $\overline{\gamma} \in (\mathbb{Z}_K/\mathfrak{c}^2)^*$ such that $\gamma \in Q_2(K)$ for at least one representative γ of the class, and we set $Z^q_{\mathfrak{c}^2} = (\mathbb{Z}_K/\mathfrak{c}^2)^q/(\mathbb{Z}_K/\mathfrak{c}^2)^{*2}$.

Note that this strongly depends on the chosen representative γ, and that $(\mathbb{Z}_K/\mathfrak{c}^2)^q$ is *not* equal to the group of elements of $(\mathbb{Z}_K/\mathfrak{c}^2)^*$ which are sums of two squares of $\mathbb{Z}_K/\mathfrak{c}^2$.

Proposition 4.11. *We have the following natural exact sequences:*

$$1 \longrightarrow S^q_{\mathfrak{c}^2}(K) \longrightarrow S^q(K) \longrightarrow Z^q_{\mathfrak{c}^2} \longrightarrow G^q(\mathfrak{c}^2) \longrightarrow G^q(\mathbb{Z}_K) \longrightarrow 1\ .$$

In particular, we have

$$\frac{|S^q_{\mathfrak{c}^2}(K)|}{|G^q(\mathfrak{c}^2)|} = \frac{1}{|Z^q_{\mathfrak{c}^2}|}\frac{|S^q(K)|}{|G^q(\mathbb{Z}_K)|}\ .$$

Proof. All the maps are clear and well defined. To show exactness, we use the fact that if $\alpha \in Q_2(K)$ then by Proposition 4.7 we have $\alpha\mathbb{Z}_K \in \mathcal{I}^q$. The details are left to the reader. The last equality immediately follows. □

We thus need to compute separately $|Z^q_{\mathfrak{c}^2}|$ and $|S^q(K)|/|G^q(\mathbb{Z}_K)|$. The first is given as follows:

Lemma 4.12. *We have*

$$|Z^q_{\mathfrak{c}^2}| = \mathcal{N}(\mathfrak{c})/2^{\omega_K((\mathfrak{c},\mathfrak{d}(K(i)/K)))}\ .$$

Proof. With evident notation, we can write

$$\begin{aligned}|(\mathbb{Z}_K/\mathfrak{c}^2)^*/(\mathbb{Z}_K/\mathfrak{c}^2)^q| &= \prod_{\mathfrak{p}|\mathfrak{c}} |\mathbb{Z}^*_{\mathfrak{p}}/\mathbb{Z}^q_{\mathfrak{p}}| \\ &= \prod_{\mathfrak{p}|\mathfrak{c}} [\mathbb{Z}^*_{\mathfrak{p}} : \mathcal{N}_{K(i)/K}(\mathbb{Z}_{\mathfrak{p}}(i)^*)] \\ &= \prod_{\mathfrak{p}|\mathfrak{c}} e(\mathfrak{P}/\mathfrak{p})\end{aligned}$$

by local class field theory, where $\mathfrak{P}$ is any ideal of $K(i)$ above $\mathfrak{p}$. Thus prime ideals $\mathfrak{p}$ of K which are unramified in $K(i)$ do not contribute to the product, and each ramified $\mathfrak{p}$ dividing $\mathfrak{c}$ contributes a factor 2. Thus

$$|(\mathbb{Z}_K/\mathfrak{c}^2)^*/(\mathbb{Z}_K/\mathfrak{c}^2)^q| = 2^{\omega_K((\mathfrak{c},\mathfrak{d}(K(i)/K)))}\ .$$

On the other hand, since the map $x \mapsto x^2$ is a bijection from $(\mathbb{Z}_K/\mathfrak{c})^*$ to $(\mathbb{Z}_K/\mathfrak{c}^2)^{*^2}$, it is clear that $|(\mathbb{Z}_K/\mathfrak{c}^2)^*/(\mathbb{Z}_K/\mathfrak{c}^2)^{*^2}| = \mathcal{N}(\mathfrak{c})$, proving the lemma. □

Finally, we note that $|S^q(K)|/|G^q(\mathbb{Z}_K)|$ can also be computed using local class field theory, but the computation is rather long and given in a sequel to this paper kindly written for us by S. Bosca [1]. We state the result:

Theorem 4.13 (Bosca)**.** *If $i \notin K$, we have*

$$\frac{|S^q(K)|}{|G^q(\mathbb{Z}_K)|} = 2^{r_2+1-\omega_K(\mathfrak{d}(K(i)/K))}\ ,$$

while if $i \in K$ then

$$\frac{|S^q(K)|}{|G^q(\mathbb{Z}_K)|} = 2^{r_2}\ .$$

Corollary 4.14. *Denote by $j(\mathfrak{c})$ the number of prime ideals $\mathfrak{p}$ such that $\mathfrak{p} \mid 2\mathbb{Z}_K/\mathfrak{c}$, $\mathfrak{p} \nmid \mathfrak{c}$ and $\mathfrak{p}$ ramified in $K(i)/K$. Then if $i \notin K$ we have*

$$\frac{|S^q_{\mathfrak{c}^2}(K)|}{|G^q(\mathfrak{c}^2)|} = \frac{2^{r_2+1-j(\mathfrak{c})}}{\mathcal{N}(\mathfrak{c})} ,$$

while if $i \in K$ then

$$\frac{|S^q_{\mathfrak{c}^2}(K)|}{|G^q(\mathfrak{c}^2)|} = \frac{2^{r_2}}{\mathcal{N}(\mathfrak{c})} .$$

Proof. Indeed, from the two lemmas above we obtain the given formula when $i \in K$, and also when $i \notin K$ with

$$j(\mathfrak{c}) = \omega_K(\mathfrak{d}(K(i)/K)) - \omega_K((\mathfrak{c}, \mathfrak{d}(K(i)/K))) ,$$

which is equal to the number of prime ideals of K which do not divide $\mathfrak{c}$ and which are ramified in $K(i)/K$. □

Putting everything together, it is clear that this corollary implies Theorem 4.8. □

4.3. Examples. It is not difficult to give explicit and efficient algorithms to compute the quantities which enter in the formula for $c_K(C_4)$ given in Theorem 4.8, and in particular the groups $G^q(\mathfrak{c}^2)$. In this subsection, we give three examples. The numerical values that we give (which can easily be computed to thousands of decimal places if desired) are computed using methods analogous to those of [3], together with Euler–MacLaurin type methods for computing the Hurwitz zeta function.

4.3.1. $K = \mathbb{Q}$. In this case we have $h(\mathbb{Z}_K) = h(2\mathbb{Z}_K) = 0$, $P(\mathbb{Z}_K, 3/2) = 2/3$, $P(2\mathbb{Z}_K, 3/2) = 5/6$, the groups $G^q(\mathfrak{c}^2)$ are both trivial, $S(\mathbb{Z}_K, 3/2) = (1+\sqrt{2}/4)\Pi$, $S(2\mathbb{Z}_K, 3/2) = \Pi$ with $\Pi = \prod_{p\equiv 1 \pmod 4}(1+2/(p^{3/2}+p^{1/2}))$, hence Theorem 4.8 gives the known formula

$$c_{\mathbb{Q}}(C_4) = \frac{3}{\pi^2}\left(\left(1+\frac{\sqrt{2}}{24}\right)\prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{3/2}+p^{1/2}}\right)-1\right) .$$

Numerically, we find that

$$c_{\mathbb{Q}}(C_4) = 0.12205267325139676092260805289651294225790522361498\ldots$$

4.3.2. $K = \mathbb{Q}(\sqrt{-7})$. In this case we can write $2\mathbb{Z}_K = \mathfrak{p}\bar{\mathfrak{p}}$, and we have $h(\mathbb{Z}_K) = h(\mathfrak{p}) = h(\bar{\mathfrak{p}}) = h(2\mathbb{Z}_K) = 0$, $P(\mathbb{Z}_K, 3/2) = 4/9$, $P(\mathfrak{p}, 3/2) = P(\bar{\mathfrak{p}}, 3/2) = 5/9$, $P(2\mathbb{Z}_K, 3/2) = 25/36$, the groups $G^q(\mathfrak{c}^2)$ are all trivial, $S(\mathbb{Z}_K, 3/2) = (1+\sqrt{2}/4)^2\Pi$, $S(\mathfrak{p}, 3/2) = S(\bar{\mathfrak{p}}, 3/2) = (1+\sqrt{2}/4)\Pi$,

$S(2\mathbb{Z}_K) = \Pi$ with $\Pi = \prod_{\mathcal{N}\mathfrak{p}\equiv 1 \pmod 4}(1 + 2/(\mathcal{N}\mathfrak{p}^{3/2} + \mathcal{N}\mathfrak{p}^{1/2}))$, hence Theorem 4.8 gives the formula

$$c_K(C_4) = \frac{\pi}{4\sqrt{7}\zeta_K(2)}\left(\left(1 + \frac{\sqrt{2}}{24}\right)^2 P_1P_2^2 - 1\right) \text{ , with}$$

$$P_1 = \prod_{p\equiv 3,5,6 \pmod 7}\left(1 + \frac{2}{p^3 + p}\right)$$

$$P_2 = \prod_{p\equiv 1,9,25 \pmod{28}}\left(1 + \frac{2}{p^{3/2} + p^{1/2}}\right) .$$

Numerically, we find that

$$c_K(C_4) = 0.05066242776902399140025815954292368926178218475114 2\ldots$$

4.3.3. $K = \mathbb{Q}(i)$. In this case we can write $2\mathbb{Z}_K = \mathfrak{p}^2$, and we have $h(\mathbb{Z}_K) = h(\mathfrak{p}) = 1$, $h(2\mathbb{Z}_K) = 0$, $P(\mathbb{Z}_K, 3/2) = 2/3$, $P(\mathfrak{p}, 3/2) = 7/12$, $P(2\mathbb{Z}_K, 3/2) = 5/6$, the groups $G^q(\mathbb{Z}_K)$ and $G^q(2\mathbb{Z}_K)$ are both trivial but the group $G^q(4\mathbb{Z}_K)$ is of order 2. It is easy to find explicitly the nontrivial character of this group, and we obtain $S(\mathbb{Z}_K, 3/2) = (1 + \sqrt{2}/4)\Pi$, $S(\mathfrak{p}, 3/2) = \Pi$, $S(2\mathbb{Z}_K) = \Pi + \Pi'$ with $\Pi = \prod_{\mathcal{N}\mathfrak{p}\equiv 1 \pmod 4}(1 + 2/(\mathcal{N}\mathfrak{p}^{3/2} + \mathcal{N}\mathfrak{p}^{1/2}))$ and $\Pi' = \prod_{\mathcal{N}\mathfrak{p}\equiv 1 \pmod 4}(1+(-1)^{(\mathcal{N}\mathfrak{p}-1)/4}2/(\mathcal{N}\mathfrak{p}^{3/2}+\mathcal{N}\mathfrak{p}^{1/2})$. Note that any $\mathfrak{p}$ not dividing 2 satisfies $\mathcal{N}\mathfrak{p} \equiv 1 \pmod 4$, and that if $p \equiv 3 \pmod 4$, $\mathcal{N}(p\mathbb{Z}_K) \equiv 1 \pmod 8$. Thus Theorem 4.8 gives the formula

$$c_K(C_4) = \frac{\pi}{16\zeta_K(2)}\left(\left(\frac{58 + \sqrt{2}}{96}\right)P_1P_2^2 + \frac{5}{12}P_1P_3^2 - 1\right) \text{ , with}$$

$$P_1 = \prod_{p\equiv 3 \pmod 4}\left(1 + \frac{2}{p^3 + p}\right) ,$$

$$P_2 = \prod_{p\equiv 1 \pmod 4}\left(1 + \frac{2}{p^{3/2} + p^{1/2}}\right) ,$$

$$P_3 = \prod_{p\equiv 1 \pmod 4}\left(1 + (-1)^{(p-1)/4}\frac{2}{p^{3/2} + p^{1/2}}\right) .$$

Numerically, we find that

$$c_K(C_4) = 0.06106984137030074031319537138216924851419966347396 5\ldots$$

References

[1] S. Bosca, *Comparing orders of Selmer groups*. Jour. Théo. Nomb. Bordeaux **17** (2005), 467–473.
[2] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag, 2000.
[3] H. Cohen, *High precision computation of Hardy–Littlewood constants*, preprint available on the author's web page.
[4] H. Cohen, F. Diaz y Diaz, M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. reine angew. Math. **550** (2002), 169–209.
[5] H. Cohen, F. Diaz y Diaz, M. Olivier, *Cyclotomic extensions of number fields*, Indag. Math. (N.S.) **14** (2003), 183–196.
[6] H. Cohen, F. Diaz y Diaz, M. Olivier, *Counting biquadratic extensions of a number field*, preprint.
[7] H. Cohen, F. Diaz y Diaz, M. Olivier, *Counting discriminants of number fields*, submitted.
[8] B. Datskovsky, D. J. Wright, *Density of discriminants of cubic extensions*, J. reine angew. Math. **386** (1988), 116–138.
[9] J. Klüners, *A counter-example to Malle's conjecture on the asymptotics of discriminants*, C. R. Acad. Sci. Paris **340** (2005), 411–414.
[10] S. Mäki, *On the density of abelian number fields*, Thesis, Helsinki, 1985.
[11] S. Mäki, *The conductor density of abelian number fields*, J. London Math. Soc. **(2) 47** (1993), 18–30.
[12] G. Malle, *On the distribution of Galois groups*, J. Number Th. **92** (2002), 315–329.
[13] G. Malle, *On the distribution of Galois groups II*, Exp. Math. **13** (2004), 129–135.
[14] D. J. Wright, *Distribution of discriminants of Abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), 17–50.

Henri Cohen, Francisco Diaz y Diaz et Michel Olivier
Laboratoire A2X, U.M.R. 5465 du C.N.R.S.,
Université Bordeaux I, 351 Cours de la Libération,
33405 TALENCE Cedex, FRANCE
E-mail : cohen,diaz,olivier@math.u-bordeaux1.fr