Journal of Algebra 325 (2011) 461–478

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Counting cubic extensions with given quadratic resolvent

Henri Cohen, Anna Morra *,[1]

Université Bordeaux I, Institut de Mathématiques de Bordeaux, 351 Cours de la Libération, 33405 Talence Cedex, France

ARTICLE INFO

Article history:
Received 24 August 2010
Available online 6 October 2010
Communicated by John Cremona

Keywords:
Discriminant counting
Cubic extensions
Kummer theory

ABSTRACT

Given a number field k and a quadratic extension K_2, we give an explicit asymptotic formula for the number of isomorphism classes of cubic extensions of k whose Galois closure contains K_2 as quadratic subextension, ordered by the norm of their relative discriminant ideal. The main tool is Kummer theory. We also study in detail the error term of the asymptotics and show that it is $O(X^{\alpha})$, for an explicit $\alpha < 1$.

1. Introduction and statement of results

1.1. Introduction

Let k be a number field, fixed once and for all as our base field, let K/k be a cubic extension of k, and let N be a Galois closure of K/k. When K/k is not cyclic we have $\mathrm{Gal}(N/k) \simeq S_3 \simeq D_3$, and the field N contains a unique quadratic subextension K_2/k.

When K/k is cyclic we have $N = K$ and $\mathrm{Gal}(N/k) \simeq C_3$. Although this case has already been treated in [5], since the methods are almost identical we include it in the present paper by setting $K_2 = k$, which by abuse of language we will still call a quadratic extension of k, even though $[K_2 : k] = 1$.

We fix the quadratic extension K_2/k, and we call $\mathcal{F}(K_2)$ the set of cubic extensions K/k (up to k-isomorphism) such that the quadratic subextension of the Galois closure of K/k is isomorphic to K_2. Our goal is to compute an asymptotic formula for

$$N(K_2/k, X) = \left|\left\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\left(\mathfrak{d}(K/k)\right) \leqslant X\right\}\right|,$$

where $\mathfrak{d}(K/k)$ is the relative discriminant ideal of K/k and $\mathcal{N}_{k/\mathbb{Q}}$ denotes the absolute norm.

* Corresponding author.
E-mail addresses: Henri.Cohen@math.u-bordeaux1.fr (H. Cohen), Anna.Morra@math.u-bordeaux1.fr (A. Morra).
URLs: http://www.math.u-bordeaux1.fr/~cohen/ (H. Cohen), http://www.math.u-bordeaux1.fr/~morra/ (A. Morra).

[1] The author was supported by the European Community under the Marie Curie Research Training Network GTEM (MRTN-CT-2006-035495).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2010.08.027

By a well-known theorem (see for example Theorem 9.2.6 of [1]), the conductor of the cyclic extension N/K_2 is of the form $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$, where $\mathfrak{f}(K/k)$ is an ideal of the base field k (when K/k is noncyclic this is of course not a conductor in the usual sense). When $k = \mathbb{Q}$ we will write $f(K)$ for the positive integer generating the ideal $\mathfrak{f}(K/\mathbb{Q})$ of $\mathbb{Z}$.

Since $\mathfrak{d}(K/k) = \mathfrak{d}(K_2/k)\mathfrak{f}(K/k)^2$, it is clear that

$$N(K_2/k, X) = M\big(K_2/k, \big(X/\mathcal{N}_{k/\mathbb{Q}}\big(\mathfrak{d}(K_2/k)\big)\big)^{1/2}\big),$$

where

$$M(K_2/k, X) = \big|\big\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\big(\mathfrak{f}(K/k)\big) \leqslant X\big\}\big|,$$

so we will in fact only study $M(K_2/k, X)$. When $k = \mathbb{Q}$, we will omit the letter k from the notation.

Some results of this paper are obtained using tools which are similar to the ones used (in a slightly different context) in previous papers of the first author and collaborators [4,5]. Thus, for brevity we have decided to omit or only sketch some long and technical proofs, and we refer to [4,5] for complete proofs which can be easily adapted to our situation.

On the other hand we would like to emphasize that the Galois structure and the use of Kummer theory are more complex in our case than in the cyclic case [5], so some results require new proofs, which we give in detail.

Moreover, unlike [5], we give an explicit formula for the error term, since this kind of technique, although considered "standard", is not easy to find in detail in the literature.

Finally, in some cases it is possible to give simple explicit formulas by using Scholz's Spiegelungssatz, and this is done in Section 7.4.

1.2. Statement of results

The result in the case of a general base field k is a little complicated (see Corollary 6.2), so we state it here only for $k = \mathbb{Q}$.

Theorem 1.1. *As above, let $K_2 = \mathbb{Q}(\sqrt{D})$ be an extension of $\mathbb{Q}$ with $[K_2 : \mathbb{Q}] \leqslant 2$, denote by $K_2' = \mathbb{Q}(\sqrt{-3D})$ the mirror field of K_2, and set $g(K_2') = 3$ if $K_2' = \mathbb{Q}(\sqrt{-3})$, and $g(K_2') = 1$ otherwise. Then*:

(1) (*Pure cubic fields.*) *We have*

$$M\big(\mathbb{Q}(\sqrt{-3}), X\big) = C_1\big(\mathbb{Q}(\sqrt{-3})\big)X\big(\log(X) + C_2\big(\mathbb{Q}(\sqrt{-3})\big) - 1\big) + O\big(X^{2/3+\varepsilon}\big),$$

for every $\varepsilon > 0$, where

$$C_1\big(\mathbb{Q}(\sqrt{-3})\big) = \frac{7}{30}\prod_p\Big(1 - \frac{3}{p^2} + \frac{2}{p^3}\Big),$$

$$C_2\big(\mathbb{Q}(\sqrt{-3})\big) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2},$$

and γ is Euler's constant.

(2) (*General case.*) *For $D \neq -3$, denote by $a_{K_2'}(p)$ the number of copies of $\mathbb{Q}_p$ occurring in $K_2' \otimes \mathbb{Q}_p$ ($a_{K_2'}(p) = 0$ or 2 according to whether the number of prime ideals above p in K_2' is equal to 1 or 2). Then $M(\mathbb{Q}(\sqrt{D}), X) = C(\mathbb{Q}(\sqrt{D}))X + O(X^{2/3+\varepsilon})$, where*

$$C\big(\mathbb{Q}(\sqrt{D})\big) = g\big(K_2'\big)\frac{c_3(K_2')}{3^{3+r_2(K_2')}}\prod_{p\neq 3}\Big(1 + \frac{a_{K_2'}(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big),$$

and

$$c_3\big(K_2'\big) = \begin{cases} 11 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1^2, \\ 15 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1, \\ 21 & \text{if } 3\mathbb{Z}_{K_2'} = \mathfrak{p}_1\mathfrak{p}_2. \end{cases}$$

The result of (2) for $D = 1$ over $\mathbb{Q}$ (corresponding to cyclic cubic fields) is due to Cohn (see [6]), and over a general number field is due to the author and collaborators (see [5]). The result of (1) over $\mathbb{Q}$ is certainly also in the literature (at least its main term), but over a general number field it seems to be new, as are all the other results, whether over $\mathbb{Q}$ or over a general number field.

Note that the formula in (2) is given because of its elegance and for comparison with the quartic case, which we give below, but it should *not* be used for practical computation of the constants $C(\mathbb{Q}(\sqrt{D}))$; for this, use instead Corollary 7.6 below. We emphasize that (for D of reasonable size) all these constants can easily be computed to hundreds of decimals, using the folklore method explained in detail in Section 10.3.6 of [3].

1.3. Comparison with the quartic case

Because of its striking similarity, we recall the results of [2] in the *quartic* case. Let K_3 be a cubic number field, and set $g(K_3) = 3$ if K_3 is cyclic, $g(K_3) = 1$ otherwise. We let $\mathcal{F}(K_3)$ be the set of isomorphism classes of quartic number fields K whose cubic resolvent is isomorphic to K_3. If $K \in \mathcal{F}(K_3)$, its discriminant $d(K)$ is of the form $d(K) = d(K_3)f(K)^2$ for some integer $f(K)$, and as in our case we let

$$M(K_3, X) = \big|\big\{K \in \mathcal{F}(K_3),\ f(K) \leqslant X\big\}\big|.$$

The main result of [2] is then as follows:

Theorem 1.2. *Denote by $a_{K_3}(p)$ the number of copies of $\mathbb{Q}_p$ in $K_3 \otimes \mathbb{Q}_p$ ($a_{K_3}(p) = 0$, 1 or 3 according to whether the number of prime ideals above p in K_3 is equal to 1, 2, or 3). Then $M(K_3, X) = C(K_3)X + O(X^\alpha)$ for some $\alpha < 1$, with*

$$C(K_3) = \frac{1}{g(K_3)} \frac{c_2(K_3)}{2^{4+r_2(K_3)}} \prod_{p \neq 2} \left(1 + \frac{a_{K_3}(p)}{p}\right)\left(1 - \frac{1}{p}\right),$$

where

$$c_2(K_3) = \begin{cases} 11 & \text{if } 2\mathbb{Z}_{K_3} = \mathfrak{p}_1, \\ 14 & \text{if } 2\mathbb{Z}_{K_3} = \mathfrak{p}_1^3, \\ 15 & \text{if } 2\mathbb{Z}_{K_3} = \mathfrak{p}_1\mathfrak{p}_2, \\ 16 & \text{if } 2\mathbb{Z}_{K_3} = \mathfrak{p}_1^2\mathfrak{p}_2 \text{ and } v_2(d(K_3)) = 3, \\ 18 & \text{if } 2\mathbb{Z}_{K_3} = \mathfrak{p}_1^2\mathfrak{p}_2 \text{ and } v_2(d(K_3)) = 2, \\ 23 & \text{if } 2\mathbb{Z}_{K_3} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3. \end{cases}$$

The similarities are striking.

2. Galois theory

Definition 2.1. We denote by $\rho = \zeta_3$ a primitive cube root of unity and we set $L = K_2(\rho)$ and $k_z = k(\rho)$. We let τ be a generator of $\mathrm{Gal}(L/K_2)$, and we let τ_2 be a generator of $\mathrm{Gal}(K_2/k)$. We denote by $G = \mathrm{Gal}(L/k)$. Finally, we let σ be one of the two generators of the cyclic group of order 3 $\mathrm{Gal}(N/K_2) \simeq \mathrm{Gal}(N_z/L)$, where $N_z = N(\rho)$.

Remark 2.2. We have the following relations:

$$\tau^2 = \tau_2^2 = 1, \qquad \tau\tau_2 = \tau_2\tau, \qquad \tau\sigma = \sigma\tau.$$

We will need to distinguish five cases, according to the triviality or not of τ or τ_2, and to their action on ρ. We will order them as follows, and this numbering will be kept throughout the paper, so should be referred to.

(1) $\tau = \tau_2 = 1$: here K/k is a cyclic cubic extension; in other words $K_2 = k$, $\mathrm{Gal}(N_z/k) \simeq C_3$, and $\rho \in k$.
(2) $\tau_2 = 1$ and $\tau(\rho) = \rho^{-1}$: here K/k is a cyclic cubic extension, so that $K_2 = k$, $\mathrm{Gal}(N_z/k) \simeq C_6$; in other words $\tau\sigma = \sigma\tau$, and $\rho \notin k$ so $L = k(\rho)$.
(3) $\tau = 1$ and $\tau_2(\rho) = \rho$ but $\tau_2 \neq 1$: here K/k is noncyclic, $\rho \in k$, and in particular $L = K_2$, and $\mathrm{Gal}(N_z/k) \simeq D_3$; in other words $\tau_2\sigma = \sigma^{-1}\tau_2$.
(4) $\tau = 1$ and $\tau_2(\rho) = \rho^{-1}$: here again $L = K_2$, so that $\rho \in K_2$, but $\rho \notin k$, so $K_2 = k(\rho)$, and again $\mathrm{Gal}(N_z/k) \simeq D_3$; in other words $\tau_2\sigma = \sigma^{-1}\tau_2$.
(5) $\tau \neq 1$ and $\tau_2 \neq 1$: here $\rho \notin K_2$, so $\tau(\rho) = \rho^{-1}$ but $\tau_2(\rho) = \rho$, so that the fixed field of L under τ_2 is equal to $k_z = k(\rho)$, and $\mathrm{Gal}(N_z/k) \simeq D_3 \times C_2$; in other words $\tau\sigma = \sigma\tau$ and $\tau_2\sigma = \sigma^{-1}\tau_2$.

Definition 2.3.

(1) In cases (1) to (5) above, we set $T = \emptyset$, $\{\tau + 1\}$, $\{\tau_2 + 1\}$, $\{\tau_2 - 1\}$, $\{\tau + 1, \tau_2 + 1\}$, respectively, where T is considered as a subset of the group ring $\mathbb{Z}[\mathrm{Gal}(L/k)]$ or of $\mathbb{F}_3[\mathrm{Gal}(L/k)]$.
(2) We define $\iota(\tau \pm 1) = \tau \mp 1$ and $\iota(\tau_2 \pm 1) = \tau_2 \mp 1$.
(3) For any group M on which T acts, we denote by $M[T]$ the subgroup of elements of M annihilated by all the elements of T.

We will need the following trivial lemma (see [5], Lemma 2.4).

Lemma 2.4. *Let M be an $\mathbb{F}_3[G]$-module. For any $t \in T$ we have $M[t] = \iota(t)(M)$, and conversely $M[\iota(t)] = t(M)$.*

Proposition 2.5.

(1) *There exists a bijection between on the one hand isomorphism classes of extensions K/k having quadratic resolvent field isomorphic to K_2, and on the other hand classes of elements $\overline{\alpha} \in (L^*/L^{*3})[T]$ such that $\overline{\alpha} \neq \overline{1}$ modulo the equivalence relation identifying $\overline{\alpha}$ with its inverse.*
(2) *If $\alpha \in L^*$ is some representative of $\overline{\alpha}$, the extension K/k corresponding to α is the fixed field under $\mathrm{Gal}(L/k)$ of the field $N_z = L(\sqrt[3]{\alpha})$.*

Proof. Since $\rho \in L$, by Kummer theory, cyclic cubic extensions of L are of the form $N_z = L(\sqrt[3]{\alpha})$, where $\overline{\alpha} \neq \overline{1}$ is unique in (L^*/L^{*3}) modulo the equivalence relation identifying $\overline{\alpha}$ with its inverse. If $\theta^3 = \alpha$, then we may assume that $\sigma(\theta) = \rho\theta$. When τ is nontrivial (cases (2) and (5)) we have $\tau(\rho) = \rho^{-1}$. Thus,

$$\sigma\big(\theta\tau(\theta)\big) = \rho\theta\tau\big(\sigma(\theta)\big) = \rho\theta\tau(\rho\theta) = \theta\tau(\theta),$$

so by Galois theory $\theta\tau(\theta) \in L$, so $\alpha\tau(\alpha)$ is a cube, in other words $\alpha \in (L^*/L^{*3})[\tau+1]$.

Similarly when τ_2 is nontrivial we have either $\tau_2(\rho) = \rho$ (cases (3) and (5)) or $\tau_2(\rho) = \rho^{-1}$ (case (4)). A similar computation gives respectively $\alpha \in (L^*/L^{*3})[\tau_2+1]$ or $\alpha \in (L^*/L^{*3})[\tau_2-1]$.

Conversely, assume that these conditions are satisfied. The group conditions on τ and τ_2 are automatically satisfied, and the group conditions on σ are exactly those corresponding to the set T. It follows that N_z/k is Galois with suitable Galois group. The uniqueness statement comes from the corresponding statement of Kummer theory, since α and α^{-1} give the same extension. □

Definition 2.6. We denote by $V_3(L)$ the group of (3-)*virtual units* of L, in other words the group of $u \in L^*$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$ for some ideal $\mathfrak{q}$ of L. We define the (3-)*Selmer group* $S_3(L)$ of L by $S_3(L) = V_3(L)/L^{*3}$.

It is immediate that the Selmer group is finite.

Proposition 2.7.

(1) *There exists a bijection between isomorphism classes of cubic extensions K/k with given quadratic resolvent field K_2 and equivalence classes of triples $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$ modulo the equivalence relation $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u}) \sim (\mathfrak{a}_1, \mathfrak{a}_0, 1/\overline{u})$, where $\mathfrak{a}_0$, $\mathfrak{a}_1$, and $\overline{u}$ are as follows*:
   (a) *The $\mathfrak{a}_i$ are coprime integral squarefree ideals of L such that $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ and $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, where I is the group of fractionals ideals of L.*
   (b) *$\overline{u} \in S_3(L)[T]$, and $\overline{u} \neq 1$ when $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$.*

(2) *If $(\mathfrak{a}_0, \mathfrak{a}_1)$ is a pair of ideals satisfying* (a) *there exist an ideal $\mathfrak{q}_0$ and an element α_0 of L such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/L^{*3})[T]$. The cubic extensions K/k corresponding to such a pair $(\mathfrak{a}_0, \mathfrak{a}_1)$ are given as follows: for any $\overline{u} \in S_3(L)[T]$ the extension is the cubic subextension of $N_z = L(\sqrt[3]{\alpha_0 u})$ (for any lift u of $\overline{u}$).*

Proof. Let $N_z = L(\sqrt[3]{\alpha})$ as above. We can write uniquely $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ where the $\mathfrak{a}_i$ are coprime squarefree ideals of L. Since $\alpha \in (L^*/L^{*3})[T]$ and the class of $\mathfrak{a}_0\mathfrak{a}_1^2$ is equal to that of $\mathfrak{q}^{-3}$, we obtain (a). Now let $\mathfrak{a}_0, \mathfrak{a}_1$ be given satisfying (a). There exists an ideal $\mathfrak{q}$ and an element $\alpha \in L$ such that $(\mathfrak{a}_0\mathfrak{a}_1^2)\mathfrak{q}^3 = \alpha\mathbb{Z}_L$. Applying any $t \in T$, we deduce that $\mathfrak{q}_1^3 = t(\alpha)\mathbb{Z}_L$ for some ideal $\mathfrak{q}_1$, so that $t(\alpha)$ is a virtual unit. From $t \circ \iota(t) = 0$ and Lemma 2.4 we deduce that $t(\alpha) \in t(S_3(L))$, in other words that $t(\alpha) = \gamma^3 t(u)$, for some virtual unit u and some element γ. Thus, if we set $\alpha_0 = \alpha/u$, we have $\alpha_0 \in (L^*/L^{*3})[t]$, and $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$, for some ideal $\mathfrak{q}_0$.

The rest of the proof is immediate: $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ and $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3 = \alpha\mathbb{Z}_L$, with both $\alpha_0, \alpha \in (L^*/L^{*3})[T]$ if and only if $\alpha/\alpha_0 = (\mathfrak{q}/\mathfrak{q}_0)^3 \in V_3(L)[T]$, so $\alpha = \alpha_0 u$ for some lift u of $\overline{u} \in S_3(L)[T]$. Finally α and β give equivalent extensions if and only if either $\beta = \alpha\gamma^3$, which does not change the $\mathfrak{a}_i$ and the class $\overline{u}$, or if $\beta = \alpha^{-1}\gamma^3$. In this case

$$\beta\mathbb{Z}_L = \mathfrak{a}_0^{-1}\mathfrak{a}_1^{-2}\mathfrak{q}^{-3}\gamma^3 = \mathfrak{a}_1\mathfrak{a}_0^2\big(\gamma\,\mathfrak{a}_0^{-1}\mathfrak{a}_1^{-1}\mathfrak{q}^{-1}\big)^3,$$

which interchanges $\mathfrak{a}_0$ and $\mathfrak{a}_1$, and changes $\overline{u}$ into $1/\overline{u}$, finishing the proof. Note that the only fixed point of this involution on triples is obtained for $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$, and $\overline{u} = 1$. □

Lemma 2.8.

(1) *The condition $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ is equivalent to $\mathfrak{a}_1 = \tau(\mathfrak{a}_0)$, $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_0)$, $\mathfrak{a}_0 = \tau_2(\mathfrak{a}_0)$ and $\mathfrak{a}_1 = \tau_2(\mathfrak{a}_1)$, and $\mathfrak{a}_1 = \tau(\mathfrak{a}_0) = \tau_2(\mathfrak{a}_0)$ in cases* (2), (3), (4), *and* (5), *respectively.*

(2) *The ideal $\mathfrak{a}_0\mathfrak{a}_1$ of L comes from an ideal $\mathfrak{a}_\alpha$ of K_2 (in other words $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$), and in cases* (1), (2), *and* (3) *it comes from an ideal of k, while in cases* (4) *and* (5), *$\mathfrak{a}_\alpha$ is an ideal of K_2 invariant by τ_2.*

Proof. Just apply uniqueness of decomposition to $\tau(\mathfrak{a}_0\mathfrak{a}_1^2)$ and $\tau_2(\mathfrak{a}_0\mathfrak{a}_1^2)$. □

In case (5), which is the only case where $G = \mathrm{Gal}(L/k) \simeq V_4$, we define K_2' to be the quadratic subextension of L/k different from K_2 and k_z.

Definition 2.9. We define $\mathcal{D}$ (resp., $\mathcal{D}_3$) to be the set of all prime ideals p in k with $p \nmid 3\mathbb{Z}_k$ (resp., with $p \mid 3\mathbb{Z}_k$), such that:

- no other conditions in cases (1) and (4);
- p is split in L/k in case (2) and (3);
- the ideals above p are split in L/K_2 and L/k_z in case (5).

Proposition 2.10.

(1) *Let $\mathfrak{p}$ be a prime ideal of K_2 dividing $\mathfrak{a}_\alpha$ and let p be the prime ideal of k below $\mathfrak{p}$. Then $p \in \mathcal{D} \cup \mathcal{D}_3$.*
(2) *In cases* (2) *and* (3)*, set $K_2' = L$. Then in cases* (2)*,* (3)*, and* (5) *we have $p \in \mathcal{D} \cup \mathcal{D}_3$ if and only p is split in K_2'/k.*

Proof. (1) is immediate, for (2) use decomposition groups. □

3. Conductors

The discriminant (equivalently, the conductor) of a cyclic Kummer extension is given by an important theorem of Hecke (see [1], Section 10.2.9). We will mainly need it in the cubic case, but we also need it in the quadratic case, where it takes an especially nice form:

Theorem 3.1. *Let k be a number field, let $K_2 = k(\sqrt{D})$ be a quadratic extension with $D \in k^* \setminus k^{*2}$, and write uniquely $D\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$, where $\mathfrak{a}$ is an integral squarefree ideal. Then*

$$\mathfrak{d}(K_2/k) = \mathfrak{f}(K_2/k) = 4\mathfrak{a}/\mathfrak{c}^2,$$

where $\mathfrak{c}$ is the largest ideal (for divisibility) dividing $2\mathbb{Z}_k$ and coprime to $\mathfrak{a}$ such that the congruence $x^2/D \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ has a solution.

Corollary 3.2. *Let K be a number field such that $\rho \notin k$, where $\rho = \zeta_3$ is a primitive cube root of unity, and set $K_z = K(\rho)$. Then*

$$\mathfrak{d}(K_z/K) = \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_K \\ e(\mathfrak{p}/3) \text{ odd}}} \mathfrak{p}.$$

In particular, the ramified primes in K_z/K are those above 3 such that $e(\mathfrak{p}/3)$ is odd.

Proof. We have $K_z = K(\sqrt{-3})$, so $D = -3$. We have $D\mathbb{Z}_K = 3\mathbb{Z}_K = \mathfrak{a}\mathfrak{q}^2$ with $\mathfrak{a} = \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_K \\ e(\mathfrak{p}/3) \text{ odd}}} \mathfrak{p}$. On the other hand $\mathfrak{a}$ is coprime to 2 and the congruence $x^2 \equiv -3 \pmod 4$ has the solution $x = 1$, so $\mathfrak{c} = 2\mathbb{Z}_K$ and the corollary follows. □

If $\mathfrak{p}$ is a prime ideal of K_2, we will denote by $\mathfrak{p}_z$ any prime ideal of L above $\mathfrak{p}$. By the above corollary, we have $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ if and only if $L \neq K_2$ and $e(\mathfrak{p}/3)$ is odd, otherwise $e(\mathfrak{p}_z/\mathfrak{p}) = 1$.

In the case of cyclic cubic extensions, the result is more complicated, especially when $L \neq K_2$. We first need some definitions.

Definition 3.3. In the sequel, when p is a prime ideal of k we will denote by $\mathfrak{p}$ a prime ideal of K_2 above p, and by $\mathfrak{p}_z$ a prime ideal of L above $\mathfrak{p}$. In addition, to simplify notation:

- We set $p^{1/2}=\mathfrak{p}$ if p is ramified in K_2/k (i.e., $p\mathbb{Z}_{K_2}=\mathfrak{p}^2$), and similarly $\mathfrak{p}^{1/2}=\mathfrak{p}_z$ if $\mathfrak{p}$ is ramified in L/K_2 (i.e., $\mathfrak{p}\mathbb{Z}_L=\mathfrak{p}_z^2$).
- We say that $p\subset k$ divides some ideal $\mathfrak{b}$ of K_2 (resp., of L) when $(p\mathbb{Z}_{K_2})^{1/e(\mathfrak{p}/p)}$ (resp., $(p\mathbb{Z}_L)^{1/e(\mathfrak{p}_z/p)}$) does.

Note that $e(\mathfrak{p}_z/p)\leqslant 2$ (indeed, if for instance $e(\mathfrak{p}/p)=2$ then $e(\mathfrak{p}/3)$ is even so $\mathfrak{p}_z/\mathfrak{p}$ is unramified by Corollary 3.2), so we will never need to define "$p^{1/4}$".

Definition 3.4. Let $\overline{\alpha}\in(L^*/L^{*3})[T]$ be as above, let p be an ideal of k above 3, let $\mathfrak{p}$ and $\mathfrak{p}_z$ be as in Definition 3.3, and consider the congruence $x^3/\alpha\equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$ in L. If this congruence is soluble for $n=3e(\mathfrak{p}_z/3)/2$ we set $A_\alpha(p)=3e(\mathfrak{p}_z/3)/2+1$, otherwise, if $n<3e(\mathfrak{p}_z/3)/2$ is the largest exponent for which it has a solution, we set $A_\alpha(p)=n$. In both cases we define

$$a_\alpha(p)=\frac{A_\alpha(p)-1}{e(\mathfrak{p}_z/p)}.$$

It is clear that $A_\alpha(p)$ and $a_\alpha(p)$ do not depend on the ideal $\mathfrak{p}_z$ above p, whence the notation. We have the following properties:

Proposition 3.5. *We have $0\leqslant a_\alpha(p)<3e(p/3)/2-1/e(\mathfrak{p}/p)$ and $a_\alpha(p)e(\mathfrak{p}/p)\in\mathbb{Z}$, or $a_\alpha(p)=3e(p/3)/2$, which happens if and only if $A_\alpha(p)=3e(\mathfrak{p}_z/3)/2+1$, in which case it is only a half integer when $e(\mathfrak{p}_z/\mathfrak{p})=2$.*

Definition 3.6. To simplify notations, we set

$$\mathcal{P}_3=\left\{p \;\middle|\; 3\mathbb{Z}_k \text{ such that } e(\mathfrak{p}/3) \text{ odd}\right\}.$$

Theorem 3.7. *Let N correspond to α as above, write uniquely $\alpha\mathbb{Z}_L=\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$ with $\mathfrak{a}_0$ and $\mathfrak{a}_1$ integral coprime squarefree ideals, and let $\mathfrak{a}_\alpha$ be the ideal of K_2 such that $\mathfrak{a}_0\mathfrak{a}_1=\mathfrak{a}_\alpha\mathbb{Z}_L$ (see Lemma 2.8). Then*

$$\mathfrak{f}(N/K_2)=\frac{3\mathfrak{a}_\alpha\prod_{p\mid 3\mathbb{Z}_k}(p\mathbb{Z}_{K_2})^{e(p/3)/2}\prod_{p\in\mathcal{P}_3}(p\mathbb{Z}_{K_2})^{1/2}}{\prod_{\substack{p\mid 3\mathbb{Z}_k\\ p\nmid\mathfrak{a}_\alpha}}(p\mathbb{Z}_{K_2})^{\lceil a_\alpha(p)e(\mathfrak{p}/p)\rceil/e(\mathfrak{p}/p)}}.$$

Remark 3.8. Proposition 3.5 and Theorem 3.7 come from similar results in [5] where we have just replaced $a_\alpha(\mathfrak{p})$ by $a_\alpha(p)=a_\alpha(\mathfrak{p})/e(\mathfrak{p}/p)$. In particular, the fact that $a_\alpha(p)e(\mathfrak{p}/p)$ is an integer when $a_\alpha(p)<3e(p/3)/2$ is a rather subtle result, which follows from the use of higher ramification groups.

Definition 3.9. Let p, $\mathfrak{p}$ and $\mathfrak{p}_z$ be as in Definition 3.4, and let a be such that $0\leqslant a<3e(p/3)/2-1/e(\mathfrak{p}/p)$ and $ae(\mathfrak{p}/p)\in\mathbb{Z}$, or $a=3e(p/3)/2$. For $\varepsilon=0$ or 1 we define $h(\varepsilon,a,p)$ as follows:

- We set $h(0,a,p)=0$ if $a=3e(p/3)/2$ or $e(\mathfrak{p}_z/\mathfrak{p})=2$; in the other cases we set $h(0,a,p)=1/e(\mathfrak{p}/p)$.
- We set $h(1,a,p)=2/e(\mathfrak{p}_z/p)$.

Lemma 3.10. *Let $b=a+h(\varepsilon,a,p)$.*

(1) *Assume that $b\leqslant 3e(p/3)/2$. Then $h(\varepsilon,b,p)=h(\varepsilon,a,p)$, so that $a=b-h(\varepsilon,b,p)$.*
(2) *We have $b=0$ if and only if $a=0$, $\varepsilon=0$, and $e(\mathfrak{p}_z/\mathfrak{p})=2$. In particular, if $e(\mathfrak{p}_z/\mathfrak{p})=1$ we have $b>0$.*

Proof. Follows immediately from Definition 3.9. □

Lemma 3.11. *Let p be a prime ideal of k and denote by D_k the congruence $x^3/\alpha \equiv 1 \pmod{{}^* p^k}$ in L. If a is as in the above definition, then $a_\alpha(p) = a$ if and only if D_k is soluble for $k = a + h(0, a, p)$ and not soluble for $k = a + h(1, a, p)$, where this last condition is ignored if $a + h(1, a, p) > 3e(p/3)/2$.*

Proof. Just apply definitions 3.4 and 3.9 and Proposition 3.5. □

4. The Dirichlet series

To avoid having both the norm from $K_2/\mathbb{Q}$ and from $k/\mathbb{Q}$, and to emphasize the fact that we are mainly interested in the latter, we set explicitly the following definition:

Definition 4.1. If $\mathfrak{a}$ is an ideal of k, we set $\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{a})$, while if $\mathfrak{a}$ is an ideal of K_2, we set

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{K_2/\mathbb{Q}}(\mathfrak{a})^{1/[K_2:k]}.$$

This practical abuse of notation cannot create any problems since if $\mathfrak{a}$ is an ideal of k we have $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}\mathbb{Z}_{K_2})$. For instance, since $\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}$, we have $\mathcal{N}(\mathfrak{f}(K/k)) = \mathcal{N}(\mathfrak{f}(N/K_2))$. We emphasize that unless explicitly written otherwise, from now on we will only use the above notation.

Definition 4.2. The fundamental Dirichlet series is defined by

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s}.$$

Definition 4.3. For $\alpha_0 \in L^*$ and $\mathfrak{b}$ an ideal of L we introduce the function

$$f_{\alpha_0}(\mathfrak{b}) = \left|\left\{\overline{u} \in S_3(L)[T],\ x^3/(\alpha_0 u) \equiv 1 \left(\mathrm{mod}\ {}^*\mathfrak{b}\right) \text{ soluble in } L\right\}\right|,$$

with the convention that $f_{\alpha_0}(\mathfrak{b}) = 0$ if $\mathfrak{b} \nmid 3\sqrt{-3}$.

Definition 4.4.

(1) We let $\mathcal{B}$ be the set of formal products of the form $\prod_{\mathfrak{p}_i \mid 3\mathbb{Z}_k} (\mathfrak{p}_i \mathbb{Z}_{K_2})^{b_i}$, where the b_i are such that $0 \leqslant b_i \leqslant 3e(\mathfrak{p}_i/3)/2$ and $e(\mathfrak{p}_i/p_i)b_i \in \mathbb{Z} \cup \{3e(\mathfrak{p}_i/3)/2\}$.
(2) We will consider any $\mathfrak{b} \in \mathcal{B}$ as an ideal of K_2, where by abuse of language we accept to have half powers of prime ideals of K_2, and we set $\mathfrak{b}_z = \mathfrak{b}\mathbb{Z}_L$.
(3) If $\mathfrak{b} = \prod_{\mathfrak{p}_i \mid 3\mathbb{Z}_{K_2}} \mathfrak{p}_i^{b_i'} \in \mathcal{B}$, $b_i' = e(\mathfrak{p}_i/p_i)b_i$, we set $\lceil \mathcal{N} \rceil(\mathfrak{b}) = \prod_{\mathfrak{p}_i \mid \mathfrak{b}} \mathcal{N}(\mathfrak{p}_i)^{\lceil b_i' \rceil}$.
(4) For $\mathfrak{b} \in \mathcal{B}$ we define $\mathfrak{r}^e(\mathfrak{b}) = \prod_{\substack{\mathfrak{p} \mid 3\mathbb{Z}_{K_2},\ \mathfrak{p} \nmid \mathfrak{b} \\ e(\mathfrak{p}/3) \text{ even}}} \mathfrak{p}$.
(5) We set $\mathfrak{d}_3 = \prod_{p \in \mathcal{D}_3} p$.

Definition 4.5.

(1) Set $e = e(p/3)$, let $\mathfrak{p}$ an ideal of K_2 above p, let $\mathfrak{p}_z$ be an ideal of L above $\mathfrak{p}$, and define $s' = s/e(\mathfrak{p}/p)$. We define $Q((p\mathbb{Z}_{K_2})^{b_i}, s)$ as follows:

- if $e(\mathfrak{p}_z/\mathfrak{p}) = 1$, (so that $e(\mathfrak{p}/3)$ is even) we have

$$Q\left((p\mathbb{Z}_{K_2})^b, s\right) = \begin{cases} 0 & \text{if } b = 0, \\ 1/\mathcal{N}(p)^{s'} & \text{if } b = 1/e(\mathfrak{p}/p), \\ 1/\mathcal{N}(p)^{s'} - 1/\mathcal{N}(p)^{2s'} & \text{if } 2/e(\mathfrak{p}/p) \leqslant b \leqslant 3e/2 - 1/e(\mathfrak{p}/p), \\ 1 - 1/\mathcal{N}(p)^{2s'} & \text{if } b = 3e/2, \end{cases}$$

- if $e(\mathfrak{p}_z/\mathfrak{p}) = 2$ (so that $e(\mathfrak{p}/p) = 1$) we have

$$Q\left((p\mathbb{Z}_{K_2})^b, s\right) = \begin{cases} 1 & \text{if } b = 0 \text{ or } b = 3e/2, \\ 1 - 1/\mathcal{N}(p)^{s'} & \text{if } 1 \leqslant b \leqslant 3e/2 - 3/2, \\ -1/\mathcal{N}(p)^{s'} & \text{if } b = 3e/2 - 1/2. \end{cases}$$

(2) We set $P_{\mathfrak{b}}(s) = \prod_{p|\mathfrak{b}} Q\left((p\mathbb{Z}_{K_2})^{v_p(\mathfrak{b})}, s\right)$.

Proposition 4.6. *We have*

$$\Phi(s) = \frac{1}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]s} \prod_{\mathcal{P}_3} \mathcal{N}(p)^{s/2}} \sum_{\substack{\mathfrak{b} \in \mathcal{B} \\ \mathfrak{r}^e(\mathfrak{b}) | \mathfrak{d}_3}} \lceil \mathcal{N} \rceil(\mathfrak{b})^s P_{\mathfrak{b}}(s) \sum_{\substack{(\mathfrak{a}_0, \mathfrak{a}_1) \in J \\ (\mathfrak{a}_\alpha, 3\mathbb{Z}_{K_2}) = \mathfrak{r}^e(\mathfrak{b})}} \frac{f_{\alpha_0}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}.$$

Proof. This formula is obtained after some computations, applying in particular Proposition 2.7, Theorem 3.7 and an inclusion–exclusion argument. A complete proof of the analogous result in the (simpler) case of cyclic extensions can be found in [5]. □

5. Computation of $f_{\alpha_0}(\mathfrak{b})$

Recall that $\mathfrak{b}_z \mid 3\sqrt{-3}$ and that the $\mathfrak{a}_i$ are coprime squarefree ideals such that $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$ and $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$. We have also set $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \alpha_0\mathbb{Z}_L$ with $\alpha_0 \in (L^*/L^{*3})[T]$. Recall that

$$f_{\alpha_0}(\mathfrak{b}) = \left|\left\{\overline{u} \in S_3(L)[T],\ x^3 \equiv \alpha_0 u \pmod{{}^*\mathfrak{b}_z} \text{ soluble in } L\right\}\right|,$$

where we have replaced the congruence $x^3/(\alpha_0 u) \equiv 1 \pmod{{}^*\mathfrak{b}_z}$ by the above since we may assume α_0 coprime to $\mathfrak{b}_z$ (changing $\mathfrak{q}_0$ and α_0 if necessary).

Definition 5.1. Set

$$S_{\mathfrak{b}}(L)[T] = \left\{\overline{u} \in S_3(L)[T],\ x^3 \equiv u \pmod{{}^*\mathfrak{b}_z} \text{ soluble}\right\},$$

where u is any lift of $\overline{u}$ coprime to $\mathfrak{b}_z$, and the congruence is in L.

Lemma 5.2. *Let $\mathfrak{a}_0, \mathfrak{a}_1$ as in condition* (1) *of Proposition* 2.7. *Then*

$$f_{\alpha_0}(\mathfrak{b}) = \begin{cases} |S_{\mathfrak{b}}(L)[T]| & \text{if } \overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. First, assume that there exists an $u_0 \in S_3(L)[T]$ such that $x_0^3 \equiv \alpha_0 u_0 \pmod{{}^*\mathfrak{b}_z}$ for some $x_0 \in L$. The congruence $x^3 \equiv \alpha_0 u \pmod{{}^*\mathfrak{b}_z}$ is thus equivalent to $(x/x_0)^3 \equiv (u/u_0) \pmod{{}^*\mathfrak{b}_z}$, in other words to $u/u_0 \in S_{\mathfrak{b}}(L)[T]$, so the set of possible $\overline{u}$ is equal to $\overline{u_0}S_{\mathfrak{b}}(L)[T]$, whose cardinality is $|S_{\mathfrak{b}}(L)[T]|$. So if $f_{\alpha_0} \neq 0$ then it is equal to $|S_{\mathfrak{b}}(L)[T]|$.

Now let us prove that $f_{\alpha_0} \neq 0$ if and only if $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3$. The condition $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3$ is equivalent to the existence of $\mathfrak{q}_1$ and $\beta_1 \equiv 1 \pmod{{}^*\mathfrak{b}_z}$ such that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_1^3 = \beta_1\mathbb{Z}_L$. Assume first that u exists, so that $x_0^3 = \alpha_0 u\beta$ for some $\beta \equiv 1 \pmod{{}^*\mathfrak{b}_z}$ and $u\mathbb{Z}_L = \mathfrak{q}^3$. It follows that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3\mathfrak{q}^3 = \alpha_0 u\mathbb{Z}_L = (x_0^3/\beta)\mathbb{Z}_L$, so we can take $\mathfrak{q}_1 = \mathfrak{q}_0\mathfrak{q}/x_0$ and $\beta_1 = 1/\beta \equiv 1 \pmod{{}^*\mathfrak{b}_z}$. Conversely, assume that $\mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_1^3 = \beta_1\mathbb{Z}_L$ with $\beta_1 \equiv 1 \pmod{{}^*\mathfrak{b}_z}$. Since $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, we have $t(\beta_1) = \gamma^3$ for some $\gamma \in L^*$. It follows that $\alpha_0\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}_0^3 = \beta_1(\mathfrak{q}_0/\mathfrak{q}_1)^3$. Thus, $u = \alpha_0/\beta_1$ is a virtual unit, and $t(u)$ is a cube of L since this is true for α_0 and for β_1. Thus $\bar{u} \in S_3(L)[T]$ and $1^3 \equiv \beta_1 \equiv \alpha_0/u \pmod{{}^*\mathfrak{b}_z}$, so $f_{\alpha_0}(\mathfrak{b}) \neq 0$, proving the lemma. □

Note that when we assume $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl_{\mathfrak{b}}(L)^3$ we have automatically $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$, so we only need to assume that $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$.

To compute $|S_{\mathfrak{b}}(L)[T]|$ we will use the folling lemmas, which are similar to the ones proposed in [5], §2, so we will omit the proofs.

Lemma 5.3. *Set $Z_{\mathfrak{b}} = (\mathbb{Z}_L/\mathfrak{b}_z)^*$, $Cl = Cl(L)$, $Cl_{\mathfrak{b}} = Cl_{\mathfrak{b}}(L)$ and $U = U(L)$. Then*

$$\left|S_{\mathfrak{b}}(L)[T]\right| = \frac{|(U/U^3)[T]||(Cl_{\mathfrak{b}}/Cl_{\mathfrak{b}}^3)[T]|}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|}.$$

In particular

$$\left|S_3(L)[T]\right| = \left|\left(U/U^3\right)[T]\right|\left|\left(Cl/Cl^3\right)[T]\right|.$$

The quantity $|(Cl_{\mathfrak{b}}/Cl_{\mathfrak{b}}^3)[T]|$ will in fact disappear in subsequent computations, and in any case cannot be computed more explicitly.

Lemma 5.4. *For any number field K, denote by $\mathrm{rk}_3(K)$ the 3-rank of the group of units of K, in other words $\mathrm{rk}_3(K) = \dim_{\mathbb{F}_3}(U(K)/U(K)^3)$, so that $|U(K)/U(K)^3| = 3^{\mathrm{rk}_3(K)}$.*

(1) *With evident notation we have*

$$\mathrm{rk}_3(K) = \begin{cases} r_1(K) + r_2(K) - 1 & \text{if } \rho \notin K, \\ r_1(K) + r_2(K) & \text{if } \rho \in K. \end{cases}$$

(2) *We have $|(U/U^3)[T]| = 3^{r(U)}$, where*

$$r(U) = \begin{cases} \mathrm{rk}_3(k) & \text{in cases (1) and (4)}, \\ \mathrm{rk}_3(L) - \mathrm{rk}_3(k) & \text{in cases (2) and (3)}, \\ \mathrm{rk}_3(L) + \mathrm{rk}_3(k) - \mathrm{rk}_3(K_2) - \mathrm{rk}_3(k_z) & \text{in case (5)}. \end{cases}$$

Lemma 5.5. *Assume that $\mathfrak{b}$ is an ideal of $\mathcal{B}$, stable by τ_2 and such that $\mathfrak{b}_z \mid 3\sqrt{-3}$, and define*

$$\mathfrak{c}_z = \prod_{\substack{\mathfrak{p}_z \subset L \\ \mathfrak{p}_z \mid \mathfrak{b}_z}} \mathfrak{p}_z^{\lceil v_{\mathfrak{p}_z}(\mathfrak{b}_z)/3 \rceil}.$$

Then

$$\left|\left(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3\right)[T]\right| = \left|\frac{\mathfrak{c}_z}{\mathfrak{b}_z}[T]\right|.$$

Lemma 5.6.

$$\left|\left(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3\right)[T]\right| = \begin{cases} |\mathfrak{c}_z/\mathfrak{b}_z| & \text{in case (1)},\\ \frac{|\mathfrak{c}_z/\mathfrak{b}_z|}{|(\mathfrak{c}_z\cap k)/(\mathfrak{b}_z\cap k)|} & \text{in cases (2) and (3)},\\ |(\mathfrak{c}_z\cap k)/(\mathfrak{b}_z\cap k)| & \text{in case (4)},\\ \frac{|\mathfrak{c}_z/\mathfrak{b}_z||(\mathfrak{c}_z\cap k)/(\mathfrak{b}_z\cap k)|}{|(\mathfrak{c}_z\cap K_2)/(\mathfrak{b}_z\cap K_2)||(\mathfrak{b}_z\cap k_z)/(\mathfrak{c}_z\cap k_z)|} & \text{in case (5)}. \end{cases}$$

6. Final form of the Dirichlet series

We can now put together all the work that we have done. Recall that we have computed $|U/U^3[T]|$ in Lemma 5.4 and $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|$ in Lemma 5.6. Moreover, $\mathcal{B}$, $\lceil\mathcal{N}\rceil$ and $\mathfrak{d}_3$ are defined in Definition 4.4, and $P_{\mathfrak{b}}(s)$ is given by Definition 4.5. Finally, recall that we have

$$\Phi(s) = \frac{1}{2} + \sum_{K\in\mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s}.$$

Theorem 6.1. *For any ideal $\mathfrak{b}$, set $G_{\mathfrak{b}} = (Cl_{\mathfrak{b}}/Cl_{\mathfrak{b}}^3)[T]$. We have*

$$\Phi(s) = \frac{|(U/U^3)[T]|}{2\cdot 3^{(3/2)[k:\mathbb{Q}]s}\prod_{\mathcal{P}_3}\mathcal{N}(p)^{s/2}} \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})|\mathfrak{d}_3}} \left(\frac{\lceil\mathcal{N}\rceil(\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))}\right)^s \frac{P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} F(\mathfrak{b},\chi,s),$$

where

$$F(\mathfrak{b},\chi,s) = \prod_{\substack{p|\mathfrak{r}^e(\mathfrak{b})\\ p\in\mathcal{D}_3'(\chi)}} 2 \prod_{\substack{p|\mathfrak{r}^e(\mathfrak{b})\\ p\in\mathcal{D}_3\setminus\mathcal{D}_3'(\chi)}} (-1) \prod_{p\in\mathcal{D}'(\chi)} \left(1+\frac{2}{\mathcal{N}(p)^s}\right) \prod_{p\in\mathcal{D}\setminus\mathcal{D}'(\chi)} \left(1-\frac{1}{\mathcal{N}(p)^s}\right),$$

and $\mathcal{D}'(\chi)$ (resp. $\mathcal{D}_3'(\chi)$) is the set of $p\in\mathcal{D}$ (resp. $\mathcal{D}_3$) such that $\chi(p\mathbb{Z}_L)=1$ in cases (1) and (4), $\chi(\mathfrak{c}) = \chi(\tau'(\mathfrak{c}))$ in the other cases, where we write $p\mathbb{Z}_L = \mathfrak{c}\tau'(\mathfrak{c})$, $\tau'\in\{\tau,\tau_2\}$, and $\mathfrak{c}$ is not necessarily a prime ideal.

Proof. Let $\mathfrak{a}_0$ and $\mathfrak{a}_1$ be as in condition (a) of Proposition 2.7. We have $\mathfrak{a}_0\mathfrak{a}_1^2\in Cl_{\mathfrak{b}}(L)^3$ if and only if $\chi(\mathfrak{a}_0\mathfrak{a}_1^2)=1$ for all characters $\chi\in\widehat{G_{\mathfrak{b}}}$. The number of such characters being equal to $|G_{\mathfrak{b}}|$, by orthogonality of characters we have

$$\Phi(s) = \frac{|(U/U^3)[T]|}{2\cdot 3^{(3/2)[k:\mathbb{Q}]s}\prod_{\substack{p|3\mathbb{Z}_k,\\ e(\mathfrak{p}/3)\text{ odd}}}\mathcal{N}(p)^{s/2}} \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})|\mathfrak{d}_3}} \frac{\lceil\mathcal{N}\rceil(\mathfrak{b})^s P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} H(\mathfrak{b},\chi,s),$$

with $H(\mathfrak{b},\chi,s) = \sum_{\substack{(\mathfrak{a}_0,\mathfrak{a}_1)\in J'\\ (\mathfrak{a}_\alpha,3\mathbb{Z}_{K_2})=\mathfrak{r}^e(\mathfrak{b})}} \frac{\chi(\mathfrak{a}_0\mathfrak{a}_1^2)}{\mathcal{N}(\mathfrak{a}_\alpha)^s}$, where J' is the set of pairs of coprime squarefree ideals of L, satisfying condition (1) of Lemma 2.8, with no class group condition. Thus

$$H(\mathfrak{b},\chi,s) = \frac{\chi(\mathfrak{r}^e(\mathfrak{b}))}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s} \sum_{\substack{(\mathfrak{a},3\mathbb{Z}_L)=1\\ \mathfrak{a}\text{ squarefree}\\ \tau(\mathfrak{a})=\tau_2(\mathfrak{a})=\mathfrak{a}}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \sum_{\mathfrak{a}_1|\mathfrak{a}\mathfrak{r}^e(\mathfrak{b}),\ \mathfrak{a}_1\in J''} \chi(\mathfrak{a}_1),$$

where J'' is the set of squarefree ideals $\mathfrak{a}_1$ such that $\mathfrak{a}_1$ is stable by τ_2 in case (4), $\mathfrak{a}_1\tau'(\mathfrak{a}_1) = \mathfrak{a}\mathfrak{r}^e(\mathfrak{b})$ for each nontrivial $\tau'\in\{\tau,\tau_2\}$ in the other cases.

Let us define $G(\chi, p)$ by:

$$G(\chi, p) = \begin{cases} 1 + \chi(p\mathbb{Z}_L) & \text{in cases (1) and (4), and otherwise:} \\ \chi(\mathfrak{c}) + \chi(\tau'(\mathfrak{c})) & \text{when } p\mathbb{Z}_L = \mathfrak{c}\tau'(\mathfrak{c}) \ (\tau' \text{ and } \mathfrak{c} \text{ as above}). \end{cases}$$

Since $\mathfrak{a}$ is coprime to 3, by multiplicativity we have $H(\mathfrak{b}, \chi, s) = S_1 S_2$ with

$$S_1 = \frac{\chi(\mathfrak{r}^e(\mathfrak{b}))}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s} \prod_{p \mid \mathfrak{r}^e(\mathfrak{b})} G(\chi, p) \quad \text{and}$$

$$S_2 = \sum_{\substack{(\mathfrak{a}, 3\mathbb{Z}_L)=1 \\ \mathfrak{a} \text{ squarefree} \\ \tau(\mathfrak{a})=\tau_2(\mathfrak{a})=\mathfrak{a}}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} \prod_{p \mid \mathfrak{a}} G(\chi, p) = \prod_{p \in \mathcal{D}} \left(1 + \frac{\chi(p\mathbb{Z}_L) G(\chi, p)}{\mathcal{N}(p)^s}\right).$$

Now, looking at the possible values for $G(\chi, p)$, we conclude. □

Corollary 6.2. *In cases* (2) *and* (3)*, set* $K_2' = L$*, and in all cases denote by* $\mathfrak{d}(K_2'/k)$ *the relative discriminant of* K_2'/k*. Let us define*

$$c_1 = \frac{|(U/U^3)[T]|}{2 \cdot 3^{(3/2)[k:\mathbb{Q}]} \prod_{\substack{p \mid 3\mathbb{Z}_k \\ e(\mathfrak{p}/3) \text{ odd}}} \mathcal{N}(p)^{1/2}},$$

$$c_2 = \sum_{\substack{\mathfrak{b} \in \mathcal{B} \\ \mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3}} \frac{\lceil \mathcal{N} \rceil(\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))} \frac{P_{\mathfrak{b}}(1)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]|} 2^{\omega(\mathfrak{r}^e(\mathfrak{b}))},$$

$$c_3 = \prod_{p \subset k} \left(1 - \frac{3}{\mathcal{N}(p)^2} + \frac{2}{\mathcal{N}(p)^3}\right) \prod_{p \mid 3\mathbb{Z}_k} \left(1 + \frac{2}{\mathcal{N}(p)}\right)^{-1},$$

$$c_4 = \frac{1}{\zeta_k(2)} \prod_{p \in \mathcal{D}} \left(1 - \frac{2}{\mathcal{N}(p)(\mathcal{N}(p)+1)}\right) \prod_{p \mid \mathfrak{d}(K_2'/k)} \left(1 - \frac{1}{\mathcal{N}(p)+1}\right),$$

where $\omega(\mathfrak{r}^e(\mathfrak{b})) = \sum_{p \mid \mathfrak{r}^e(\mathfrak{b})} 1$.

- *In cases* (1) *and* (4)*, around* $s = 1$ *we have*

$$\Phi(s) = \frac{C_1(K_2/k)}{(s-1)^2} + \frac{C_1(K_2/k) C_2(K_2/k)}{s-1} + O(1),$$

with constants

$$C_1(K_2/k) = c_1 c_2 c_3 \left(\operatorname{Res}_{s=1} \zeta_k(s)\right)^2 \quad \text{and}$$

$$C_2(K_2/k) = 2\gamma_k + \lim_{s \to 1} \frac{G'(s)}{G(s)},$$

$$\text{where } G(s) = \frac{\Phi(s)}{\zeta_k(s)^2} \text{ and } \gamma_k = \lim_{s \to 1} \left(\frac{\zeta_k(s)}{\operatorname{Res}_{s=1} \zeta_k(s)} - \frac{1}{s-1}\right).$$

In addition, using the notation given at the beginning of this paper, as $X \to \infty$ we have

$$M(K_2/k, X) = C_1(K_2/k)X\big(\log(X) + C_2(K_2/k) - 1\big) + O\big(X^{\alpha}\big) \quad \text{for some } \alpha < 1.$$

- *In cases* (2), (3), *and* (5) *we have*

$$\Phi(s) = \frac{C(K_2/k)}{(s-1)} + O(1),$$

with

$$C(K_2/k) = c_1c_2c_4\big(\operatorname{Res}_{s=1}\zeta_{K_2'}(s)\big),$$

and

$$M(K_2/k, X) = C(K_2/k)X + O\big(X^{\alpha}\big) \quad \text{for some } \alpha < 1.$$

Proof. It is easy to see that when χ is not the trivial character, the functions $F(\mathfrak{b}, \chi, s)$ are holomorphic for $\Re(s) > 1/2$, so do not occur in the polar part at $s = 1$. On the other hand, since $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_3$, for $\chi = 1$ we have $F(\mathfrak{b}, 1, s) = 2^{\omega(\mathfrak{r}^e(\mathfrak{b}))}P(s)$, where $P(s) = \prod_{p\in\mathcal{D}}(1 + \frac{2}{\mathcal{N}(p)^s})$, so we just need to develop $P(s)$ to get the formula for the polar part of $\Phi(s)$.

Finally, since our Dirichlet series have nonnegative and polynomially bounded coefficients, the asymptotic results follow from a general (and in this case easy) Tauberian theorem. For the error term $O(X^{\alpha})$ with an explicit $\alpha < 1$, we refer to the following proposition and corollary. □

Proposition 6.3. *Let $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet series which is absolutely convergent for $\Re(s) > 1$, which can be extended meromorphically to $\Re(s) > 1/2$ with a pole of order $k \geqslant 1$ at $s = 1$ and no other pole in the strip $\frac{1}{2} < \Re(s) < 1$. In addition, assume the following*:

(1) *The coefficients a_n are nonnegative, and for all $\varepsilon > 0$ we have*

$$a_n \ll_{\varepsilon} n^{\varepsilon}.$$

(2) *$F(s)$ is a function of finite order in the vertical strip $\frac{1}{2} < \sigma \leqslant 1$: we have*

$$\big|F(\sigma + it)\big| \ll_{\varepsilon} |t|^{\mu(\sigma)+\varepsilon}, \quad \text{when } |t| \geqslant 1, \text{ for all } \varepsilon > 0,$$

where $\mu(1) = 0$, and $\mu(\sigma)$ is convex and decreasing in the strip.

(3) *The integral*

$$\int_0^1 \big|F(\sigma + it)\big|\,dt$$

is bounded independently of $\frac{1}{2} < \sigma < \frac{1}{2} + \delta$, for some $\delta > 0$.

Then for all $\varepsilon > 0$, we have

$$\sum_{n\leqslant x} a_n = \operatorname{Res}_{s=1}\left(F(s)\frac{x^s}{s}\right) + O\big(x^{\alpha+\varepsilon}\big),$$

where

$$\alpha = 1 - \frac{1}{2(1+\mu(1/2))}. \tag{1}$$

Proof. Apply Perron's formula, Cauchy's residue formula and use (1) and (2) to bound the error term. □

Corollary 6.4. *The error term in 6.2 is $O(x^{\alpha})$, where α is given by* (1)*.*

Proof. We only need to prove that $\Phi(s)$ satisfies the hypothesis of Proposition 6.3. For (1) we can simply refer to [7, Lemma 6.1] or look at the form of $F(\mathfrak{b}, \chi, s)$, and for (2) we apply the Phragmén–Lindelöf principle. □

Remark 6.5. In the case $k = \mathbb{Q}$ it is easy to show that $\mu(1/2) \leqslant 1/2$, so we obtain an error term $O(X^{2/3+\varepsilon})$. The previous bound on $\mu(1/2)$ is obtained by using only the convexity bound on the Riemann zeta function, but if we use subconvexity bounds we would get better results.

On the other hand, if we assume the Lindelöf hypothesis (which is for example implied by GRH), we obtain $\mu(1/2) = 0$, giving an error term $O(X^{1/2+\varepsilon})$.

7. Special cases: $k = \mathbb{Q}$, cases (2), (4), and (5)

We consider the case $k = \mathbb{Q}$, and since $\rho \notin k$ only cases (2), (4), and (5) occur.

7.1. Case (2): cyclic cubic extensions

Proposition 7.1. *We have*

$$\sum_{K/\mathbb{Q} \text{ cyclic cubic}} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{p \equiv 1 \pmod 3} \left(1 + \frac{2}{p^s}\right).$$

Corollary 7.2. *If, as above, $M(\mathbb{Q}, X)$ denotes the number of cyclic cubic fields K up to isomorphism with $f(K) \leqslant X$, we have*

$$M(\mathbb{Q}, X) = C(\mathbb{Q})X + O\left(X^{2/3+\varepsilon}\right), \quad \text{where}$$

$$C(\mathbb{Q}) = \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{2}{p(p+1)}\right) = 0.15852825839614206028350782035 75\ldots.$$

7.2. Case (4): pure cubic fields

In case (4), we have $K_2 = \mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$, so that $L = K_2$, and $K/\mathbb{Q}$ is a pure cubic field, in other words $K = \mathbb{Q}(\sqrt[3]{m})$.

Proposition 7.3. *We have*

$$\sum_{K/\mathbb{Q} \text{ pure cubic}} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{6}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{p \neq 3} \left(1 + \frac{2}{p^s}\right)$$
$$+ \frac{1}{3} \prod_{p \equiv \pm 1 \pmod 9} \left(1 + \frac{2}{p^s}\right) \prod_{p \not\equiv \pm 1 \pmod 9} \left(1 - \frac{1}{p^s}\right),$$

where $p \not\equiv \pm 1 \pmod 9$ includes $p = 3$.

Corollary 7.4. *If, as above, $M(\mathbb{Q}(\sqrt{-3}), X)$ denotes the number of pure cubic fields K up to isomorphism with $f(K) \leqslant X$, we have*

$$M\big(\mathbb{Q}(\sqrt{-3}), X\big) = C_1\big(\mathbb{Q}(\sqrt{-3})\big)X\big(\log(X) + C_2\big(\mathbb{Q}(\sqrt{-3})\big) - 1\big) + O\big(X^{2/3+\varepsilon}\big),$$

where

$$C_1\big(\mathbb{Q}(\sqrt{-3})\big) = \frac{7}{30}\prod_p\left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$
$$= 0.066907733301378371291841632984295637501344\ldots,$$

$$C_2\big(\mathbb{Q}(\sqrt{-3})\big) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2}$$
$$= 3.450222797830591962790711919671111041826885\ldots,$$

where γ is Euler's constant and the sum is over all primes including $p = 3$.

To check the validity of these constants, we note that for instance for $X = 10^{18}$ we have

$$M\big(\mathbb{Q}(\sqrt{-3}), X\big) = 2937032340990444425, \quad \text{while}$$
$$C_1\big(\mathbb{Q}(\sqrt{-3})\big)X\big(\log(X) + C_2\big(\mathbb{Q}(\sqrt{-3})\big) - 1\big) = 2937032340990158620\ldots.$$

As already mentioned, the error is of the order of $O(X^{1/4+\varepsilon})$ (in this case for instance $0.22 \cdot X^{1/4}\log(X)$), much smaller than $O(X^{2/3+\varepsilon})$ proved above, and even better than the error term $O(X^{1/2+\varepsilon})$ that we can prove under the Lindelöf conjecture.

7.3. Case (5): $K_2 = \mathbb{Q}(\sqrt{D})$ with $D \neq -3$

In case (5), we have $K_2 = \mathbb{Q}(\sqrt{D})$ with $D \neq -3$, so $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$.

Proposition 7.5. *Let D be a fundamental discriminant with $D \neq -3$, let $K_2 = \mathbb{Q}(\sqrt{D})$, and let $r_2(D) = 1$ for $D < 0$ and $r_2(D) = 0$ for $D > 0$. There exists a function $\phi_D(s)$ holomorphic for $\Re(s) > 1/2$ such that*

$$\sum_{K\in\mathcal{F}(K_2)} \frac{1}{f(K)^s} = \phi_D(s) + \frac{3^{r_2(D)}}{6}L_3(s)\prod_{(\frac{-3D}{p})=1}\left(1 + \frac{2}{p^s}\right), \quad \textit{where}$$

$$L_3(s) = \begin{cases} 1 + 2/3^{2s} & \text{if } 3 \nmid D, \\ 1 + 2/3^s & \text{if } D \equiv 3 \pmod 9, \\ 1 + 2/3^s + 6/3^{2s} & \text{if } D \equiv 6 \pmod 9. \end{cases}$$

Proof. If we denote by $\phi_D(s)$ the contribution of the nontrivial characters in Theorem 6.1 it is clear that $\phi_D(s)$ is a holomorphic function for $\Re(s) > 1/2$, so it is sufficient to consider the contribution of the trivial characters $\Phi_0(s)$. We consider the three cases separately and, with similar notations and computations as in the examples above, we get:

$$\Phi_0(s) = \frac{3^{r_2(D)}}{6}\left(1+\frac{2}{3^{2s}}\right)\prod_{(\frac{-3D}{p})=1}\left(1+\frac{2}{p^s}\right) \qquad \text{if } 3\nmid D,$$

$$\Phi_0(s) = \frac{3^{r_2(D)}}{6}\left(1+\frac{2}{3^{s}}\right)\prod_{(\frac{-3D}{p})=1}\left(1+\frac{2}{p^s}\right) \qquad \text{if } D\equiv 3 \pmod 9,$$

$$\Phi_0(s) = \frac{3^{r_2(D)}}{6}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{(\frac{-3D}{p})=1}\left(1+\frac{2}{p^s}\right) \quad \text{if } D\equiv 6 \pmod 9,\ D\neq -3. \qquad \square$$

Corollary 7.6. *Set $D' = -3D$ if $3\nmid D$ and $D' = -D/3$ if $3 \mid D$, and denote as usual by $\chi_{D'}$ the character $(\frac{D'}{\cdot})$. Then if $D \neq -3$ is a fundamental discriminant we have*

$$M\big(\mathbb{Q}(\sqrt{D}\,), X\big) = C\big(\mathbb{Q}(\sqrt{D}\,)\big)X + O\big(X^{2/3+\varepsilon}\big), \quad \textit{where}$$
$$C\big(\mathbb{Q}(\sqrt{D}\,)\big) = \frac{3^{r_2(D)}\ell_3 L(\chi_{D'},1)}{\pi^2}\prod_{p\mid D'}\left(1-\frac{1}{p+1}\right)\prod_{(\frac{D'}{p})=1}\left(1-\frac{2}{p(p+1)}\right),$$

where

$$\ell_3 = \begin{cases} 11/9 & \text{if } 3\nmid D,\\ 5/3 & \text{if } D\equiv 3 \pmod 9,\\ 7/5 & \text{if } D\equiv 6 \pmod 9.\end{cases}$$

Note that $L(\chi_{D'},1)$ is given by Dirichlet's class number formula, in other words with standard notation, $L(\chi_{D'},1) = 2\pi h(D')/(w(D')\sqrt{|D'|})$ if $D'<0$ and $L(\chi_{D'},1) = 2h(D')R(D')/\sqrt{D'}$ if $D'>0$.

Proof of Theorem 1.1(2). We now show how to modify the above formulas so as to obtain the formula given in the theorem. By Propositions 7.1 and 7.5 we can write

$$\Phi_D(s) = \phi_D(s) + g\big(K_2'\big)\frac{3^{r_2(D)}}{6}L_3(s)\prod_{p\neq 3}\left(1+\frac{a_{K_2'}(p)}{p^s}\right),$$

where $g(K_2') = 1$ unless $D=1$, in other words $K_2' = \mathbb{Q}(\sqrt{-3}\,)$, in which case $g(K_2') = 3$. Thus,

$$\frac{\Phi_D(s)}{(1-1/3^s)\zeta(s)} = \psi_D(s) + g\big(K_2'\big)\frac{3^{r_2(D)}}{6}L_3(s)\prod_{p\neq 3}\left(1+\frac{a_{K_2'}(p)}{p^s}\right)\left(1-\frac{1}{p^s}\right),$$

where $\psi_D(s) = \phi_D(s)/((1-1/3^s)\zeta(s))$. When s tends to 1, $\psi_D(s)$ tends to 0, the left-hand side tends to a limit, and it is easy to see that the right-hand side tends to a semi-convergent Euler product. Thus, if we set $P(K_2') = \prod_{p\neq 3}((1+a_{K_2'}(p)/p)(1-1/p))$, we have

$$C\big(\mathbb{Q}(\sqrt{D}\,)\big) = \operatorname{Res}_{s=1}\Phi_D(s) = g\big(K_2'\big)\frac{1}{3^{2-r_2(D)}}L_3(1)P\big(K_2'\big) = g\big(K_2'\big)\frac{c_3(K_2')}{3^{3+r_2(K_2')}}P\big(K_2'\big),$$

where $c_3(K_2')$ is given in the theorem, since the different cases for $L_3(1)$ correspond to the different splittings of 3 in $K_2'/\mathbb{Q}$. $\square$

7.4. An exact result when $D < 0$ and $3 \nmid h(D)$

It is interesting to note that when $D < 0$ and $3 \nmid h(D)$, one can prove that nontrivial characters do not occur in the above formulas, so that $\phi_D(s) = 0$, thus giving exact formulas for the Dirichlet series.

Proposition 7.7. *Assume that $K_2 = \mathbb{Q}(\sqrt{D})$ with $D < 0$, $D \neq -3$, and $3 \nmid h(D) = |Cl(K_2)|$. Then for any ideal $\mathfrak{b} \in \mathcal{B}$ occurring in the sum of Theorem* 6.1*, the group $G_{\mathfrak{b}} = (Cl_{\mathfrak{b}}(L)/Cl_{\mathfrak{b}}(L)^3)[T]$ is trivial.*

Proof. An important theorem of Scholz [9] says that if $D < 0$ is a negative fundamental discriminant different from -3 we have

$$0 \leqslant \mathrm{rk}_3\big(Cl\big(\mathbb{Q}(\sqrt{D})\big)\big) - \mathrm{rk}_3\big(Cl\big(\mathbb{Q}(\sqrt{-3D})\big)\big) \leqslant 1$$

and that $\mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{D}))) = \mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{-3D})))$ if and only if the fundamental unit ε of $\mathbb{Q}(\sqrt{3D})$ is not 3-primary, in other words if and only if ε is not a cube modulo $3\sqrt{-3}\mathbb{Z}_L$, where $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$. Since in our case we assume that $\mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{D}))) = 0$, it follows that we also have $\mathrm{rk}_3(Cl(\mathbb{Q}(\sqrt{-3D}))) = 0$ and that ε is not a cube modulo $3\sqrt{-3}\mathbb{Z}_L$.

We now consider the exact sequence of $\mathbb{F}_3[G]$-modules already used above in the computation of $f_{\alpha_0}(\mathfrak{b})$:

$$1 \to S_{\mathfrak{b}}(L)[T] \to S_3(L)[T] \to \frac{Z_{\mathfrak{b}}}{Z_{\mathfrak{b}}^3}[T] \to \frac{Cl_{\mathfrak{b}}(L)}{Cl_{\mathfrak{b}}(L)^3}[T] \to \frac{Cl(L)}{Cl(L)^3}[T] \to 1.$$

By Hasse's formula giving the class number of biquadratic number fields [8], we have $|Cl(L)| = 2^{-j}|Cl(K_2)||Cl(K_2')|$ with $j = 0$ or 1, so in particular by Scholz's theorem we deduce that $3 \nmid |Cl(L)|$. We thus have the exact sequence

$$1 \to S_{\mathfrak{b}}(L)[T] \to S_3(L)[T] \to \frac{Z_{\mathfrak{b}}}{Z_{\mathfrak{b}}^3}[T] \to G_{\mathfrak{b}} \to 1.$$

In addition, also since $3 \nmid |Cl(L)|$, $S_3(L)$ is an $\mathbb{F}_3$-vector space of dimension $r_1(L) + r_2(L) = 2$, generated by the classes modulo cubes of ρ and a fundamental unit ε of $K_2' = \mathbb{Q}(\sqrt{-3D})$. The action of τ and τ_2 is given by $\tau(\rho) = \rho^{-1}$, $\tau_2(\rho) = \rho$, $\tau(\varepsilon) = \pm\varepsilon^{-1}$, $\tau_2(\varepsilon) = \pm\varepsilon^{-1}$ (where $\pm = \mathcal{N}_{K_2'/\mathbb{Q}}(\varepsilon)$), and modulo cubes the $\pm$ signs disappear. Since $T = \{\tau + 1, \tau_2 + 1\}$, it follows that $S_3(L)[T]$ is a 1-dimensional $\mathbb{F}_3$-vector space generated by the class of ε.

Since $G_{\mathfrak{b}}$ maps surjectively onto $G_{\mathfrak{b}'}$ for $\mathfrak{b}' \mid \mathfrak{b}$, it is sufficient to consider $\mathfrak{b} = 3\sqrt{-3}$. In that case, we have seen that $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]| = 3$ in all cases, and since we have just shown that $|S_3(L)[T]| = 3$, by the above exact sequence it follows that $G_{\mathfrak{b}}$ is trivial if and only if $S_{\mathfrak{b}}(L)[T]$ is trivial, hence by definition if and only if ε is not congruent to a cube modulo $\mathfrak{b}_z = 3\sqrt{-3}\mathbb{Z}_L$, which is exactly the second statement of Scholz's theorem, proving the proposition. □

Remark 7.8. The same proof shows the following result for $D > 0$: if $D > 0$ and $3 \nmid h(D')$, where as usual $D' = -3D$ if $3 \nmid D$ and $D' = -D/3$ if $3 \mid D$, then $G_{\mathfrak{b}}$ is canonically isomorphic to $(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[T]$, hence has order 1 unless $\mathfrak{b} = 3\sqrt{-3}$ or $3 \nmid D$ and $\mathfrak{b} = 3\mathbb{Z}_L$, in which case it has order 3.

Corollary 7.9. *Under the same assumptions, we have the following simple result*:

$$\sum_{K \in \mathcal{F}(K_2)} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}L_3(s) \prod_{(\frac{-3D}{p})=1} \left(1 + \frac{2}{p^s}\right),$$

where

$$L_3(s) = \begin{cases} 1 + 2/3^{2s} & \text{if } 3 \nmid D, \\ 1 + 2/3^{s} & \text{if } D \equiv 3 \pmod 9, \\ 1 + 2/3^{s} + 6/3^{2s} & \text{if } D \equiv 6 \pmod 9. \end{cases}$$

References

[1] H. Cohen, Advanced Topics in Computational Number Theory, Grad. Texts in Math., vol. 193, Springer-Verlag, 2000.
[2] H. Cohen, Counting A_4 and S_4 number fields with given resolvent cubic, Fields Inst. Commun. 41 (2004) 159–168.
[3] H. Cohen, Number Theory II, Analytic and Modern Tools, Grad. Texts in Math., vol. 240, Springer-Verlag, 2007.
[4] H. Cohen, F. Diaz y Diaz, M. Olivier, Cyclotomic extensions of number fields, Indag. Math. 14 (2003) 183–196.
[5] 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.
[6] H. Cohn, The density of abelian cubic fields, Proc. Amer. Math. Soc. 5 (1954) 476–477.
[7] B. Datskovsky, D.J. Wright, Density of discriminants of cubic extensions, J. Reine Angew. Math. 386 (1988) 116–138.
[8] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, Berlin, 1952.
[9] A. Scholz, Über die Beziehung der Klassenzahlen quadratischen Körper zveinander, J. Reine Angew. Math. 166 (1931) 201–203.