ON D_ℓ-EXTENSIONS OF ODD PRIME DEGREE ℓ

HENRI COHEN AND FRANK THORNE

Abstract. Generalizing the work of A. Morra and the authors, we give explicit formulas for the Dirichlet series generating function of D_ℓ-extensions of odd prime degree ℓ with given quadratic resolvent. Over the course of our proof, we explain connections between our formulas and the Ankeny-Artin-Chowla conjecture, the Ohno–Nakagawa relation for binary cubic forms, and other topics.

1. Introduction

The theory of cubic number fields is, in many respects, well understood. One reason for this is that the *Delone-Faddeev* [17] and *Davenport-Heilbronn* [16] *correspondences* parametrize cubic fields in terms of binary cubic forms, up to equivalence by an action of $\mathrm{GL}_2(\mathbb{Z})$, and satisfying certain local conditions. Therefore questions about counting cubic fields can be reduced to questions about counting lattice points, and this idea has led to asymptotic density theorems as well as other interesting results.

In more recent work, Bhargava [5, 6] obtained similar parametrization and counting results for S_4-quartic and S_5-quintic fields. However, generalizing this work to number fields of arbitrary degree ℓ seems difficult, if not impossible: the parametrizations of S_3-cubic, S_4-quartic, and S_5-quintic fields are all by *prehomogeneous vector spaces*, and for higher degree fields there is no apparent prehomogeneous vector space for which one could hope to establish a parametrization theorem.

In [12] and [14], A. Morra and the authors contributed to the cubic theory by giving explicit formulas for the Dirichlet generating series of discriminants of cubic fields having *given* resolvent. For example, writing

$$\Phi_{-107}(s) = \sum_{\substack{[K:\mathbb{Q}]=3 \\ \mathrm{Disc}(K)=-107n^2}} n^{-s}\ , \tag{1.1}$$

we have the explicit formula

$$\Phi_{-107}(s) = -\frac{1}{2} + \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{321}{p}\right)=1}\left(1+\frac{2}{p^s}\right) + \left(1+\frac{2}{3^{2s}}\right)\prod_p\left(1+\frac{\omega(p)}{p^s}\right), \tag{1.2}$$

where $\omega(p)$ is equal to 2 or -1 if p is totally split or inert in the unique cubic field of discriminant 321, determined by the polynomial x^3-x^2-4x+1, and $\omega(p)=0$ otherwise. Similar formulas hold when -107 is replaced by any other fundamental discriminant D; the formula has one main term, and one additional Euler product for each cubic field of discriminant $-D/3$, $-3D$, and $-27D$.

The proofs involve class field theory and Kummer theory; see also work of Bhargava and Shnidman [7] obtaining related results through a study of binary cubic forms.

The object of the present paper is to generalize the theory developed in [12] and [14] to degree ℓ extensions having Galois group D_ℓ, for any odd prime ℓ. In particular, our work shows that the existence of formulas such as (1.2) is not tied to the existence of parametrizations by prehomogeneous vector spaces.

Date: August 6, 2014.
1991 *Mathematics Subject Classification.* 11R16.

Let L/k be an extension[1] of odd prime degree ℓ, let $N = \widetilde{L}$ be a Galois closure of L, and assume that $\mathrm{Gal}(N/k) \simeq D_\ell$, the dihedral group with 2ℓ elements. We will simply call L a *D_ℓ-extension* of k (or a *D_ℓ-field* when $k = \mathbb{Q}$), the assumption that L/k is of degree ℓ being understood, and similarly when D_ℓ is replaced by F_ℓ (see below).

There exists a unique quadratic subextension K/k of N/k, called the *quadratic resolvent* of L, with $\mathrm{Gal}(N/K) \simeq C_\ell$, and a nontrivial theorem of J. Martinet involving the computation of higher ramification groups (see Propositions 10.1.25 and 10.1.28 of [8]) tells us that its conductor $f(N/K)$ is of the form $f(N/K) = f(L)\mathbb{Z}_K$, where $f(L)$ is an ideal of the base field k, and that the relative discriminant $\mathfrak{d}(L/k)$ of L/k is given by the formula $\mathfrak{d}(L/k) = \mathfrak{d}(K/k)^{(\ell-1)/2} f(L)^{\ell-1}$.

We study the set $\mathcal{F}_\ell(K)$ of D_ℓ-extensions of k whose quadratic resolvent field is isomorphic to K. (Here and in the sequel, extensions are always considered up to k-isomorphism). More precisely, we want to compute as explicitly as possible the Dirichlet series[2]

$$\Phi_\ell(K, s) = \frac{1}{\ell - 1} + \sum_{L \in \mathcal{F}_\ell(K)} \frac{1}{\mathcal{N}(f(L))^s} ,$$

where $\mathcal{N}(f(L)) = \mathcal{N}_{k/\mathbb{Q}}(f(L))$ is the absolute norm of the ideal $f(L)$.

Since our formulas are complicated to state, we postpone an exact statement of our results until later in the paper. Our most general result is Theorem 6.1, and in the case $k = \mathbb{Q}$ we specialize this to a more explicit version in Theorem 7.3. Finally, in Section 9 we prove for $k = \mathbb{Q}$ that our formulas can always be brought into a form similar to (1.2).

In a companion paper, joint with Rubinstein-Salzedo [13], we investigate a curious twist to this story. Taking the $n = 1$ term of formula (1.2) (or, rather, its generalization to any D) yields the nontrivial identity

$$N_3(D^*) + N_3(-27D) = \begin{cases} N_3(D) & \text{if } D < 0, \\ 3N_3(D) + 1 & \text{if } D > 0, \end{cases} \tag{1.3}$$

for any fundamental discriminant D, where $D^* = -3D$ if $3 \nmid D$ and $D^* = -D/3$ if $3 \mid D$. (Note that there are no cubic fields of discriminant $-3D$ if $3 \mid D$.) This identity was previously conjectured by Ohno [31] and then proved by Nakagawa [30], as a consequence of an 'extra functional equation' for the Shintani zeta function associated to the lattice of binary cubic forms. Our generalization of (1.2) thus subsumes the Ohno–Nakagawa theorem (1.3).

Our proof there *used* the Ohno–Nakagawa theorem, but in [13] we further develop some of the techniques of this paper (in particular, of Section 8) to give another proof of (1.3) and give a generalization to any prime $\ell \geq 3$. For $\ell > 3$ our work relates counts of D_ℓ-fields (the right-hand side of (1.3)) to counts of F_ℓ-fields ℓ (the left-hand side), where F_ℓ is the *Frobenius group* of order $\ell(\ell - 1)$, whose definition is recalled in Section 9. (Note that $S_3 = D_3 = F_3$.) The result involves a technical (Galois theoretic) condition on the F_ℓ-fields which is not automatically satisfied for $\ell > 3$, and we defer to [13] for a complete statement of the results. That said, one interesting and easily stated consequence is that for any negative fundamental discriminant $-D$ coprime to 5, we have

$$N_{F_5}\big((-1)^0 5^3 D^2\big) + N_{F_5}\big((-1)^0 5^5 D^2\big) + N_{F_5}\big((-1)^0 5^7 D^2\big) = N_{D_5}\big((-D)^2\big) + N_{D_5}\big((-5D)^2\big) , \tag{1.4}$$

[1] A remark on our choice of notation: Readers familiar with [14] or [12] should note that by and large we adopt the notation of [14] and the progression of [12]; the reader knowledgeable with the latter paper can immediately see the similarities and differences. (See also Morra's thesis [28] for a version of [12] with more detailed proofs.) What was called (K_2, K, L, K_2') in [12] will now be called (K, L, K_z, K') (so that the main number field in which most computations take place is K_z), and the field names (k, k_z, N, N_z) stay unchanged. The primitive cube root of unity ρ is replaced by a primitive ℓth root of unity ζ_ℓ.

[2] The series also depends on the base field k, which we do not include explicitly in the notation.

and if $D \neq 1$ is instead positive, then we have

$$N_{F_5}\big((-1)^2 5^3 D^2\big) + N_{F_5}\big((-1)^2 5^5 D^2\big) + N_{F_5}\big((-1)^2 5^7 D^2\big) = 5\Big(N_{D_5}\big(D^2\big) + N_{D_5}\big((5D)^2\big)\Big) + 2\,. \tag{1.5}$$

In the above, $N_G(X)$ denotes the number of G-fields with discriminant exactly equal to X, and $(-1)^r$ specifies the number of pairs of complex embeddings.

If we want an identity counting D_5-fields of discriminant $(\pm D)^2$ *or* $(\pm 5D)^2$ alone, then the left side of (1.4) and (1.5) becomes more complicated, and involves the Galois condition mentioned above. The relevance to the present paper is that it is *precisely those F_ℓ-fields counted by this identity that yield Euler products.* We describe this in more detail in Section 9.

There is one further curiosity that emerges in our work: a connection to a well-known conjecture attributed to[3] Ankeny, Artin, and Chowla [1] which states that if $\ell \equiv 1 \pmod 4$ is prime and $\epsilon = (a + b\sqrt{\ell})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{\ell})$, then $\ell \nmid b$. As we will see, the truth or falsity of the conjecture will be reflected in our explicit formula for D_ℓ-extensions having quadratic resolvent $\mathbb{Q}(\sqrt{\ell})$. Note that the conjecture is known to be true for $\ell < 2 \cdot 10^{11}$, but on heuristic grounds it should be false.

Our work follows several other papers studying dihedral field extensions. Much of the theory (such as Martinet's theorem) is described in the first author's book [8]. Another reference is Jensen and Yui [22], who studied D_ℓ-extensions from multiple points of view. They proved that if $\ell \equiv 1 \pmod 4$ is a regular prime, then no D_ℓ-extension of $\mathbb{Q}$ has discriminant a power of ℓ; our proof uses similar ideas, and we will recover and strengthen their result. Jensen and Yui also studied the problem of constructing D_ℓ-extensions, and gave several examples.

Another relevant work is the paper of Louboutin, Park, and Lefeuvre [27], who developed a general class field theory method to construct real D_ℓ-extensions. These problems have also been addressed in the function field setting by Weir, Scheidler, and Howe [36].

Since some of the proofs are quite technical, we give a detailed overview of the contents of this paper.

We begin in Section 2 with a characterization of the fields $L \in \mathcal{F}_\ell(K)$ using Galois and Kummer theory. These fields are in bijection with elements of $K_z := K(\zeta_\ell)$ modulo ℓth powers, satisfying certain restrictions which guarantee that the associated Kummer extensions of K_z descend to degree ℓ extensions of k. Writing such an extension as $K_z(\sqrt[\ell]{\alpha})$ with $\alpha\mathbb{Z}_{K_z} = \prod_{0 \le i \le \ell-2} \mathfrak{a}_i^{g^i}\mathfrak{q}^\ell$, we further characterize these fields in terms of conditions on the $\mathfrak{a}_i$ and an associated member $\overline{u}$ of a Selmer group associated to K_z.

These conditions are described in terms of the group ring $\mathbb{F}_\ell[G]$, where $G = \mathrm{Gal}(K_z/k)$. Groups such as $K_z^*/K_z^{*\ell}$, $\mathrm{Cl}(K_z)[\ell]$, and the Selmer group are naturally $\mathbb{F}_\ell[G]$-modules, and our conditions correspond to being annihilated by certain elements of $\mathbb{F}_\ell[G]$ (see Definition 2.2).

In Section 2 we also study the subfields of K_z/k, with particular attention to a degree $\ell-1$ extension K'/k called the *mirror field* of K; we will see that much of the arithmetic of prime splitting in various extensions can be conveniently expressed in terms of K'.

In Section 3, we give an expression for the 'conductor' $f(L)$ in terms of the quantities $\mathfrak{a}_i$ and $\overline{u}$ defined in Section 2. The main result, Theorem 3.8, was proved by the first author, Diaz y Diaz, and Olivier in [11] in their study of cyclic extensions of degree ℓ, and we also prove a few additional related lemmas and propositions. Unfortunately the results of that section are rather complicated to state, and oblige us to introduce a fair amount of notation.

In Section 4 we begin to study the fundamental Dirichlet series using the results proved in Section 3. That section is mostly elementary and combinatorial (but messy), and in Section 5 we study the size of a

[3]Ankeny, Artin, and Chowla did not conjecture this in [1], although they did explicitly ask if it is true. Mordell [29] attributed the conjecture to them in followup work, where he proved the conjecture for regular primes.

certain Selmer group appearing in our formulas. That section is heavily algebraic and again appeals heavily to the results of [11].

In Section 6, we put everything together to obtain our most general formula (Theorem 6.1 for $\Phi_\ell(K,s)$, a generalization of the main theorem of [12].

In the remainder of the paper we further study this formula with the aim of making everything more explicit; for the most part we now specialize to the case $k=\mathbb{Q}$. In Section 7 we compute various quantities appearing in Theorem 6.1 for $k=\mathbb{Q}$, leading to Theorem 7.3, a more explicit specialized version of Theorem 6.1. This also allows us to obtain asymptotics for the number of D_ℓ-extensions of $\mathbb{Q}$, proved in Corollary 7.5.

The formula of Theorem 7.3 falls short of being explicit in one important aspect: it involves a sum (of Euler products) over the character group of a somewhat complicated group $G_{\mathfrak{b}}$. So in Section 8 we further study its size. The main result is the Kummer pairing of Theorem 8.2, familiar from (for example) the proof of the Scholz reflection principle, and fairly simple to prove. One important input (Proposition 8.1) is a very nice relationship, due essentially to Kummer and Hecke, between the conductor of Kummer extensions of K_z, and congruence properties of the ℓth roots used to generate them. This section culminates in an explicit formula for the size of $G_{\mathfrak{b}}$.

Some of our work in Section 8 (including Theorem 8.2) is also critical in [13], and to avoid redundancy we only sketch a few results whose complete proofs are given there.

In Section 8 we also explore the connection to the conjecture of Ankeny, Artin, and Chowla mentioned above. The truth or falsity of this conjecture will then be reflected in our explicit formula (Proposition 9.2) for $\Phi_\ell(\mathbb{Q}(\sqrt{\ell}),s)$, and in Corollary 9.4 we will give a proof of an observation of Lemmermeyer, that the existence of D_ℓ-fields ramified only at ℓ is equivalent to the falsity of the Ankeny-Artin-Chowla conjecture.

In Section 9 we further study the characters of the group $G_{\mathfrak{b}}$, and prove (in Theorem 9.1) that each such character corresponds to an F_ℓ-extension E/k, such that the values of χ correspond to the splitting types of primes in E. This was done for $\ell=3$ and $k=\mathbb{Q}$ in [14], but in Theorem 9.1 we do not require $k=\mathbb{Q}$.

It is here that the connection to the Ohno–Nakagawa theorem emerges; for $\ell=3$ and $k=\mathbb{Q}$, we established in [14] (using Ohno–Nakagawa) that the set of characters of $G_{\mathfrak{b}}$ corresponds precisely to a suitable and easily described set of fields E. For $\ell>3$ we require the generalization of Ohno–Nakagawa established in [13], and so in Section 9 we say a bit more about the results of [13] and explain their relevance. We also prove an explicit formula valid for the 'special case' $K=\mathbb{Q}(\sqrt{\ell})$.

Acknowledgements

We would like to thank Michael Filaseta, David Harvey, Franz Lemmermeyer, Hendrik Lenstra, David Roberts, and John Voight for helpful comments and suggestions.

2. Galois and Kummer Theory

2.1. Galois and Kummer theory, and the Group Ring. We will use the results of [11], but before stating them we need some notation. We denote as usual by ζ_ℓ a primitive ℓth root of unity, we set $K_z=K(\zeta_\ell)$, $k_z=k(\zeta_\ell)$, $N_z=N(\zeta_\ell)$, and we denote by τ, τ_2, and σ generators of k_z/k, K/k, and N/K respectively, with $\tau^{\ell-1}=\tau_2^2=\sigma^\ell=1$.

The number ζ_ℓ could belong to k, or to K, or generate a nontrivial extension of K of degree dividing $\ell-1$. These essentially correspond respectively to cases (3), (4), and (5) of [12] (cases (1) and (2) correspond to cyclic extensions of k of degree ℓ, which have been treated in [11]). Cases (3) and (4) are considerably simpler since we do not have to adjoin ζ_ℓ to K to apply Kummer theory.

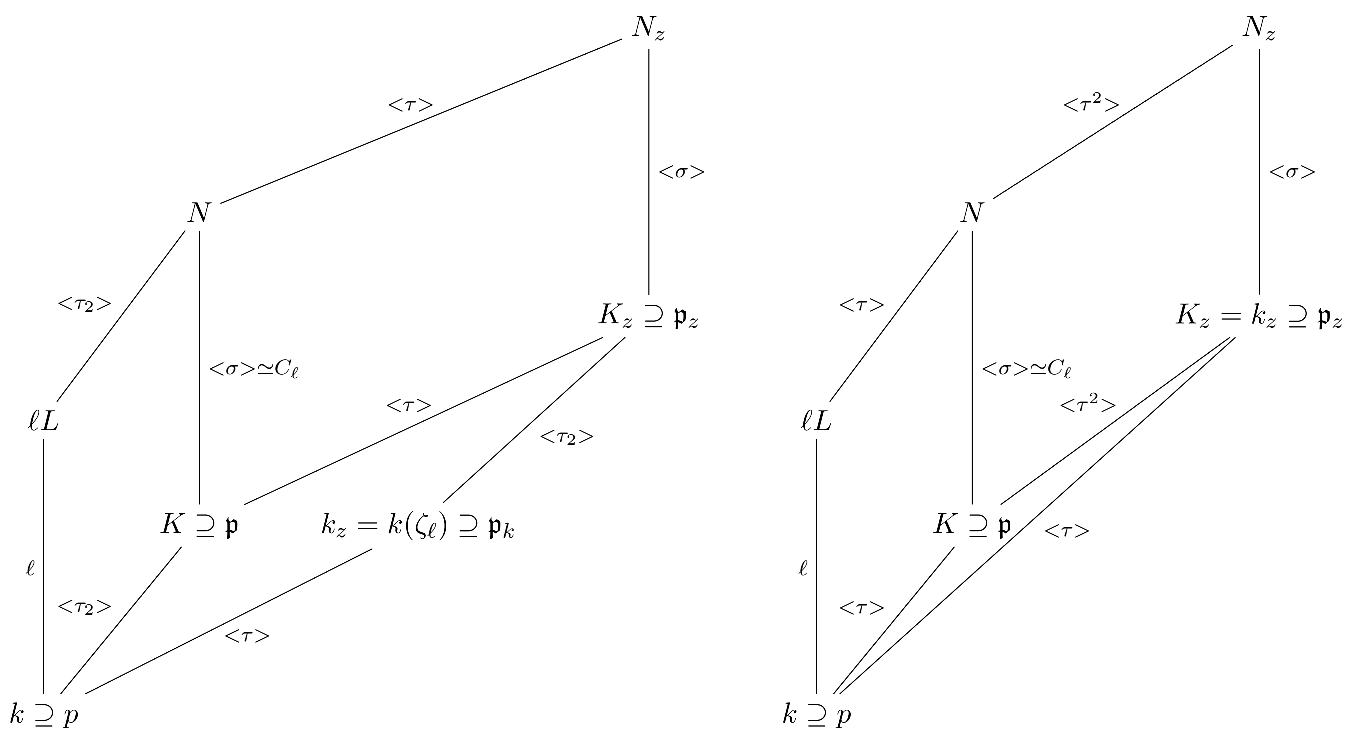
We are particularly interested in the case $k=\mathbb{Q}$, in which case either $[K_z:K]=\ell-1$, or $[K_z:K]=(\ell-1)/2$, i.e., $K\subset k_z$, which is equivalent to $K=\mathbb{Q}(\sqrt{\ell^*})$ with $\ell^*=(-1)^{(\ell-1)/2}\ell$. To balance generality and simplicity, *we assume that k is any number field for which* $[k_z : k] = \ell - 1$. Then, as for $k = \mathbb{Q}$ there are two possible cases: either $[K_z : K] = \ell - 1$, which we call the *general case*, or $K \subset k_z = K_z$ and $[K_z : K] = (\ell-1)/2$, which we will call the *special case*. Note that if $\ell = 3$ this means that $\zeta_\ell \in K$, so we are in case (4), but there is no reason to treat this case separately. It should not be particularly difficult to extend our results to any base field k, as was done in [11].

We set the following notation:

- We let g be a primitive root modulo ℓ, and also denote by g its image in $\mathbb{F}_\ell^* = (\mathbb{Z}/\ell\mathbb{Z})^*$.
- We let $G = \mathrm{Gal}(K_z/k)$. Thus in the general case $G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})^*$, while in the special case $G = \mathrm{Gal}(k_z/k) \simeq (\mathbb{Z}/\ell\mathbb{Z})^*$. We denote by τ the unique element of $\mathrm{Gal}(k_z/k)$ such that $\tau(\zeta_\ell) = \zeta_\ell^g$, so that τ generates $\mathrm{Gal}(k_z/k)$, and we again denote by τ its lift to K_z or N_z.

The composite extension $N_z = NK_z$ is Galois over k, and σ and τ naturally lift to N_z. In the general case, τ and σ commute; in the special case, τ^2 is a generator of $\mathrm{Gal}(K_z/K)$ and τ_2 can be taken to be any odd power of τ, for instance τ itself, so that $\tau\sigma\tau^{-1} = \sigma^{-1}$.

This information is summarized in the two Hasse diagrams below, depicting the general and special cases respectively.



In the above $p, \mathfrak{p}, \mathfrak{p}_k, \mathfrak{p}_z$ indicate our typical notation (to be used later) for primes of k, K, k_z, K_z respectively.

Lemma 2.1. *For $a \bmod (\ell-1)$ and $b \bmod 2$, set*

$$e_a = \frac{1}{\ell-1} \sum_{j \bmod (\ell-1)} g^{aj}\tau^{-j} \in \mathbb{F}_\ell[G] \quad \textit{and, in the general case,} \quad e_{2,b} = \frac{1}{2}\sum_{j \bmod 2} (-1)^{bj}\tau_2^{-j}\ .$$

The e_a form a complete set of orthogonal idempotents in $\mathbb{F}_\ell[G]$, as do the $e_{2,b}$ in the general case, so in the general case any $\mathbb{F}_\ell[G]$-module M has a canonical decomposition $M = \sum_{a \bmod (\ell-1),\ b \bmod 2} e_a e_{2,b} M$, while in the special case we simply have $M = \sum_{a \bmod (\ell-1)} e_a M$.

Proof. Immediate and classical; see, e.g., Section 7.3 of [18]. $\square$

We set the following definitions:

Definition 2.2. *In the group ring $\mathbb{F}_\ell[G]$, we set*

$$T = \begin{cases} \{\tau_2 + 1, \tau - g\} & \text{in the general case ,} \\ \{\tau + g\} & \text{in the special case .} \end{cases}$$

(1) We define $\iota(\tau_2 + 1) = e_{2,1} = \frac{1}{2}(1 - \tau_2)$, and for any a we define $\iota(\tau - g^a) = e_a$, so that for instance $\iota(\tau + g) = e_{(\ell+1)/2}$.
(2) For any $\mathbb{F}_\ell[G]$ module M, we denote as usual by $M[T]$ the subgroup annihilated by all the elements of T.

Lemma 2.3. *Let M be an $\mathbb{F}_\ell[G]$-module.*
(1) For any $t \in T$ we have $t \circ \iota(t) = \iota(t) \circ t = 0$, where the action of t and $\iota(t)$ is on M.
(2) For all $t \in T$ we have $M[t] = \iota(t)M$ and $M[\iota(t)] = t(M)$.
(3) If $x \in M[t]$ then $\iota(t)(x) = x$.

Proof. This follows from Lemma 2.1. In particular, $\tau e_a = g^a e_a$, so that the image of $\tau - g^a$ is $\sum_{b \neq a} e_a M$. $\square$

2.2. **The Bijections.**

Proposition 2.4. *(1) There exists a bijection between elements $L \in \mathcal{F}_\ell(K)$ and classes of elements $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[T]$ such that $\overline{\alpha} \neq \overline{1}$, modulo the equivalence relation identifying $\overline{\alpha}$ with $\overline{\alpha^j}$ for all j with $1 \le j \le \ell - 1$.*
(2) If $\alpha \in K_z^*$ is some representative of $\overline{\alpha}$, the extension L/k corresponding to α is the field $K_z(\sqrt[\ell]{\alpha})^G$, i.e., the fixed field of $K_z(\sqrt[\ell]{\alpha})$ by $G = \mathrm{Gal}(K_z/k)$.

Proof. In the first place, observe that there is a bijection between $L \in \mathcal{F}_\ell(K)$ and cyclic degree ℓ extensions of K_z which are Galois over k. Now, since $\zeta_\ell \in K_z$, by Kummer theory cyclic extensions of degree ℓ of K_z are of the form $N_z = K_z(\sqrt[\ell]{\alpha})$, where $\overline{\alpha} \neq \overline{1}$ is unique in $K_z^*/K_z^{*\ell}$ modulo the equivalence relation mentioned in the proposition. Therefore, it remains only to prove that $\overline{\alpha}$ is annihilated by T if and only if N_z is Galois over k.

Given such an extension $N_z = K_z(\theta)$ with $\theta^\ell = \alpha$, we may assume the generator σ chosen so that $\sigma(\theta) = \zeta_\ell \theta$. Set $\varepsilon = 1$ if we are in the general case, $\varepsilon = -1$ if we are in the special case, so that $\tau\sigma\tau^{-1} = \sigma^\varepsilon$. We have $\tau(\zeta_\ell) = \zeta_\ell^g$, so that

$$\sigma(\tau(\theta)) = \tau(\sigma^\varepsilon(\theta)) = \tau(\zeta_\ell^\varepsilon)\tau(\theta) = \zeta_\ell^{\varepsilon g}\tau(\theta) \ ,$$

hence if we set $\eta = \tau(\theta)/\theta^{\varepsilon g}$ we have $\sigma(\eta) = \zeta_\ell^{\varepsilon g}\tau(\theta)/\zeta_\ell^{\varepsilon g}\theta^{\varepsilon g} = \eta$. It follows by Galois theory that $\eta \in K_z$, so that $\tau(\alpha)/\alpha^{\varepsilon g} = \eta^\ell \in K_z^{*\ell}$, hence that $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[\tau - \varepsilon g]$.

Concerning τ_2 (in the general case only), the relation $\tau_2\sigma\tau_2^{-1} = \sigma^{-1}$ similarly shows that $\sigma(\theta\tau_2(\theta)) = \theta\tau_2(\theta)$ so that $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[\tau_2 + 1]$, in other words $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[T]$.

Conversely, assume that $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[T]$, and again write $\theta = \sqrt[\ell]{\alpha}$ with $\sigma(\theta) = \zeta_\ell\theta$ and $N_z = K_z(\theta)$. Define an automorphism $\overline{\tau}$ of N_z, agreeing with τ on K_z, by writing $\overline{\tau}(\theta) = \eta\theta^{\varepsilon g}$ ($\varepsilon = \pm 1$ as before), where $\eta^\ell = \tau(\alpha)/\alpha^{\varepsilon g} \in K_z^\ell$, so that $\eta \in K_z$ is well-defined up to an ℓth root of unity, and we make an arbitrary such choice.

Computations show that $\overline{\tau}\sigma^{\varepsilon}(\theta)=\sigma\overline{\tau}(\theta)$ and that $\overline{\tau}^{\ell-1}(\theta)$ is a root of unity. Each $\overline{\tau}\sigma^i$ is also a lift of τ. In the general case, we check that there is a unique such lift, which we denote simply by τ, for which $\tau^{\ell-1}(\theta)=\theta$, establishing that N_z/K is Galois with Galois group $C_{\ell-1}\times C_\ell$.

We now write $\overline{\tau_2}(\theta)=\eta_2/\theta$ with $\eta_2^\ell=\alpha\tau_2(\alpha)$, which is an element of K_z and indeed k_z. We check that $\overline{\tau_2}^2(\theta)=\theta$ and $\overline{\tau_2}\sigma(\theta)=\sigma^{-1}\overline{\tau_2}$, so that by rewriting $\overline{\tau_2}$ as τ_2 we see that N_z/k is Galois with Galois group $C_{\ell-1}\times D_\ell$, as required. Here the choice of lift τ_2 is not uniquely determined: D_ℓ has ℓ elements of order 2, corresponding to the ℓ conjugate subextensions L/k of degree ℓ.

In the special case, $(\overline{\tau}\sigma^i)^{\ell-1}=(\overline{\tau})^{\ell-1}$, so we write τ for an arbitrary choice of lift and must check that $\tau^{\ell-1}(\theta)=\theta$. Because $\tau(\theta)\theta^g=\eta$, we have $\tau^{\ell-1}(\theta)/\theta^{g^{\ell-1}}=\eta^u$ with $u=\frac{\tau^{\ell-1}-g^{\ell-1}}{\tau+g}$ (in group ring notation), and thus

$$\tau^{\ell-1}(\theta)=\eta^u\theta\alpha^b,$$

with $b=\frac{g^{\ell-1}-1}{\ell}$ and $(\eta^u)^{\tau+g}=\xi^\ell$ for some $\xi\in K_z$, so that $(\eta^u\alpha^b)^{\tau+g}=x^\ell$ for some $x\in K_z$. But we also know that $\eta^u\alpha^b=\zeta_\ell^j$ for some j, so that $x=\zeta_\ell^{2gj}$, hence $j=0\pmod{\ell}$. Therefore $\tau^{\ell-1}(\theta)=\theta$ and N_z/k is Galois over $\mathbb{Q}$ with Galois group $C_\ell\rtimes C_{\ell-1}$, as required.

□

Recall from [8] the following definition:

Definition 2.5. *We denote by $V_\ell(K_z)$ the group of (ℓ-)*virtual units *of K_z, in other words the group of $u\in K_z^*$ such that $u\mathbb{Z}_{K_z}=\mathfrak{q}^\ell$ for some ideal $\mathfrak{q}$ of K_z, or equivalently such that $\ell\mid v_{\mathfrak{p}_z}(u)$ for any prime ideal $\mathfrak{p}_z$ of K_z. We define the (ℓ-)*Selmer group *$S_\ell(K_z)$ of K_z by $S_\ell(K_z)=V_\ell(K_z)/{K_z^*}^\ell$.*

The following lemma shows in particular that the Selmer group is finite.

Lemma 2.6. *We have a split exact sequence of $\mathbb{F}_\ell[G]$-modules*

$$1\longrightarrow\frac{U(K_z)}{U(K_z)^\ell}\longrightarrow S_\ell(K_z)\longrightarrow \mathrm{Cl}(K_z)[\ell]\longrightarrow 1\ ,$$

where the last nontrivial map sends $\overline{u}$ to the ideal class of $\mathfrak{q}$ such that $u\mathbb{Z}_{K_z}=\mathfrak{q}^\ell$.

Proof. The splitting is the only nontrivial claim, for which see Lemma 3.1 of [10] (among other sources). □

From Lemma 2.3 we extract the following technical result.

Lemma 2.7. *Given $t\in T$ and $\alpha\in K_z^*$ such that $t(\alpha)$ is a virtual unit, we have $t(\alpha)=\gamma^\ell t(u)$ for some $\gamma\in K_z^*$ and some virtual unit u.*

Moreover, if α is annihilated modulo ${K_z^*}^\ell$ by $t'\neq t\in T$, we may choose u to be annihilated by t' in $S_\ell(K_z)$.

Proof. Given t and α, (1) of Lemma 2.3 applied to $M=K_z^*/{K_z^*}^\ell$ implies that $\iota(t)(t(\alpha))\in{K_z^*}^\ell$. Since $t(\alpha)$ is a virtual unit, its image $\overline{t(\alpha)}$ is annihilated by $\iota(t)$ in the Selmer group. By Lemma 2.3 applied to $M=S_\ell(K_z)$, we have $\overline{t(\alpha)}=t(\overline{\beta})$ for some $\overline{\beta}\in S_\ell(K_z)$, giving the first result. For the second, we replace each of the modules M by $M[t']$: since t and t' commute, if $\alpha\in M$ is annhilated by t', so is $t(\alpha)$. □

Proposition 2.8. *(1) There exists a bijection between elements $L\in\mathcal{F}_\ell(K)$ and equivalence classes of ℓ-tuples $(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2},\overline{u})$ modulo the equivalence relation*

$$(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2},\overline{u})\sim(\mathfrak{a}_{-i},\dots,\mathfrak{a}_{\ell-2-i},\overline{u^{g^i}})$$

for all i (with the indices of the ideals $\mathfrak{a}$ considered modulo $\ell-1$), where the $\mathfrak{a}_i$ and $\overline{u}$ are as follows:

(a) The $\mathfrak{a}_i$ are coprime integral squarefree ideals of K_z such that if we set $\mathfrak{a}=\prod_{0\le i\le\ell-2}\mathfrak{a}_i^{g^i}$ then the ideal class of $\mathfrak{a}$ belongs to $\mathrm{Cl}(K_z)^\ell$, and $\overline{\mathfrak{a}}\in(I(K_z)/I(K_z)^\ell)[T]$, where as usual $I(K_z)$ denotes the group of (nonzero) fractional ideals of K_z.

(b) $\overline{u} \in S_\ell(K_z)[T]$*, and in addition* $\overline{u} \neq \overline{1}$ *when* $\mathfrak{a}_i = \mathbb{Z}_{K_z}$ *for all* i*.*

(2) Given $(\mathfrak{a}_0, \dots, \mathfrak{a}_{\ell-2})$*,* $\mathfrak{a}$*, and* $\overline{u}$ *as in (a), the field* $L \in \mathcal{F}_\ell(K)$ *is determined as follows: There exist an ideal* $\mathfrak{q}_0$ *and an element* $\alpha_0 \in K_z$ *such that* $\mathfrak{a}\mathfrak{q}_0^\ell = \alpha_0\mathbb{Z}_{K_z}$ *with* $\overline{\alpha_0} \in (K_z^*/K_z^{*\ell})[T]$*. Then* L *is any of the* ℓ *conjugate degree* ℓ *subextensions of* $N_z = K_z(\sqrt[\ell]{\alpha_0 u})$*, where* u *is an arbitrary lift of* $\overline{u}$*.*

Proof. Given L, associate $N_z = K_z(\sqrt[\ell]{\alpha})$ as in Proposition 2.4. We may write uniquely $\alpha\mathbb{Z}_{K_z} = \prod_{0 \leq i \leq \ell-2} \mathfrak{a}_i^{g^i}\mathfrak{q}^\ell$, where the $\mathfrak{a}_i$ are coprime integral squarefree ideals of K_z, and they must satisfy the conditions of (a).

Given $\mathfrak{a}\mathfrak{q}^\ell = \alpha\mathbb{Z}_{K_z}$, we obtain $\overline{u}$ by writing $\mathfrak{a}\mathfrak{q}_0^\ell = \alpha_0\mathbb{Z}_{K_z}$ with $\overline{\alpha_0} \in (K_z^*/K_z^{*\ell})[T]$ as in (2), and setting $u = \alpha/\alpha_0$. To write $\mathfrak{a}\mathfrak{q}_0^\ell = \alpha_0\mathbb{Z}_{K_z}$, we apply any $t \in T$ to the equation $\mathfrak{a}\mathfrak{q}^\ell = \alpha\mathbb{Z}_{K_z}$, obtaining $\mathfrak{q}_1^\ell = t(\alpha)\mathbb{Z}_{K_z}$ for some $\mathfrak{q}_1$, so that $t(\alpha)$ is a virtual unit. By Lemma 2.7, $t(\alpha) = \gamma^\ell t(u_1)$ where u_1 is a virtual unit; writing $\alpha_1 = \alpha/u_1$, we have $\overline{\alpha_1} \in (K_z^*/K_z^{*\ell})[t]$ and $\mathfrak{a}\mathfrak{q}_2^\ell = \alpha_1\mathbb{Z}_{K_z}$ for some ideal $\mathfrak{q}_2$. In the special case we are done with $\alpha_0 = \alpha_1$ and $u = u_1$; in the general case, we use the second conclusion of Lemma 2.7, repeat the argument with the remaining element of T, obtain $\mathfrak{a}\mathfrak{q}_2^\ell = \alpha_2\mathbb{Z}_{K_z}$ for some ideal $\mathfrak{q}_3$ with $\overline{\alpha_0} \in (K_z^*/K_z^{*\ell})[T]$, and take $\alpha_0 = \alpha_2$. In both cases note that that both $\overline{\alpha}$ and $\overline{\alpha_0}$ are annihilated by T, and so u must be as well. [4]

This establishes the bijection, and we conclude by observing the following:

- The elements α and β give equivalent extensions if and only if $\beta = \alpha^{g^i}\gamma^\ell$ for some element γ and some i modulo $\ell - 1$, and then if $\alpha_0\mathbb{Z}_{K_z} = \prod_j \mathfrak{a}_j^{g^j}\mathfrak{q}^\ell$ and $\alpha = \alpha_0 u$, we have on the one hand $\beta\mathbb{Z}_{K_z} = \prod_j \mathfrak{a}_{j-i}^{g^j}\mathfrak{q}_1^\ell$ for some ideal $\mathfrak{q}_1$, so the ideals $\mathfrak{a}_j$ are permuted cyclically, and on the other hand $\beta = (\alpha_0 u)^{g^i}\gamma^\ell = \alpha_0^{g^i}u^{g^i}\gamma^\ell$, so $\overline{u}$ is changed into $\overline{u}^{g^i}$, giving the equivalence described in (1).
- The only fixed point of the transformation $(\mathfrak{a}_0, \dots, a_{\ell-2}, \overline{u}) \mapsto (\mathfrak{a}_{\ell-2}, \mathfrak{a}_0, \dots, \mathfrak{a}_{\ell-3}, \overline{u^g})$ is obtained with all the $\mathfrak{a}_i$ equal and $\overline{u} = \overline{u^g}$, but since the $\mathfrak{a}_i$ are pairwise coprime this means that they are all equal to $\mathbb{Z}_{K_z}$, and $\overline{u} = \overline{u^{g^i}}$ for all i, and so $\overline{u} = 1$.

∎

Remark 2.9. *Note that condition (a) implies (but is not equivalent to the fact) that* $\overline{\mathfrak{a}} \in (\mathrm{Cl}(K_z)/\mathrm{Cl}(K_z)^\ell)[T]$*, and for any modulus* $\mathfrak{m}$ *coprime to* $\mathfrak{a}$ *also that* $\overline{\mathfrak{a}} \in (\mathrm{Cl}_\mathfrak{m}(K_z)/\mathrm{Cl}_\mathfrak{m}(K_z)^\ell)[T]$*.*

Lemma 2.10. *Keep the above notation, and in particular recall that* $\mathfrak{a} = \prod_{0 \leq i \leq \ell-2} \mathfrak{a}_i^{g^i}$*. The condition* $\overline{\mathfrak{a}} \in (I(K_z)/I(K_z)^\ell)[T]$ *is equivalent to the following:*

(1) In the general case $\tau(\mathfrak{a}_i) = \mathfrak{a}_{i-1}$ *(equivalently,* $\mathfrak{a}_i = \tau^{-i}(\mathfrak{a}_0)$*), and* $\tau^{(\ell-1)/2}(\mathfrak{a}_0) = \tau_2(\mathfrak{a}_0)$*.*

(2) In the special case $\tau(\mathfrak{a}_i) = a_{i+(\ell-3)/2}$*, so that* $\mathfrak{a}_{2i} = \tau^{-2i}(\mathfrak{a}_0)$ *and* $\mathfrak{a}_{2i+1} = \tau^{-2i}(\mathfrak{a}_1)$*, with the following conditions on* $(\mathfrak{a}_0, \mathfrak{a}_1)$*:*
  - *If* $\ell \equiv 1 \pmod 4$ *then* $\mathfrak{a}_1 = \tau^{(\ell-3)/2}(\mathfrak{a}_0)$*, or equivalently* $\mathfrak{a}_0 = \tau^{(\ell+1)/2}(\mathfrak{a}_1)$*.*
  - *If* $\ell \equiv 3 \pmod 4$ *then* $\tau^{(\ell-1)/2}(\mathfrak{a}_0) = \mathfrak{a}_0$ *and* $\tau^{(\ell-1)/2}(\mathfrak{a}_1) = \mathfrak{a}_1$*.*

Proof. Since $\tau(\mathfrak{a}) = \prod_i \tau(\mathfrak{a}_i)^{g^i}$ and the $\tau(\mathfrak{a}_i)$ are integral, squarefree and coprime ideals, this is the canonical decomposition of $\tau(\mathfrak{a})$ (up to ℓth powers). On the other hand $\mathfrak{a}^g = \prod_i \mathfrak{a}_{i-1}^{g^i}$. Assume first that we are in the general case. Since $\tau(\mathfrak{a})/\mathfrak{a}^g$ is an ℓth power, by uniqueness of the decomposition we deduce that $\tau(\mathfrak{a}_i) = \mathfrak{a}_{i-1}$. A similar proof using that $g^{(\ell-1)/2} \equiv -1 \pmod{\ell}$ shows that $\tau_2(\mathfrak{a}_i) = \mathfrak{a}_{i+(\ell-1)/2}$, and putting everything together proves (1). Assume now that we are in the special case, so that $\tau(\mathfrak{a})/\mathfrak{a}^{-g}$ is an ℓth power. Since $-g \equiv g^{(\ell+1)/2} \pmod{\ell}$, the same reasoning shows that $\tau(\mathfrak{a}_i) = \mathfrak{a}_{i-(\ell+1)/2} = \mathfrak{a}_{i+(\ell-3)/2}$, so in particular $\tau^2(\mathfrak{a}_i) = \mathfrak{a}_{i-(\ell+1)} = \mathfrak{a}_{i-2}$, and the other formulas follow immediately. ∎

[4] This detailed reasoning was omitted from [12], so the proof given there is incomplete.

Corollary 2.11. *Let $\mathfrak{p}_z$ be a prime ideal of K_z dividing some $\mathfrak{a}_i$, denote by $\mathfrak{p}$ the ideal of K below $\mathfrak{p}_z$, and in the general case denote by $\mathfrak{p}_k$ the ideal of k_z below $\mathfrak{p}_z$.*

1. *In all cases $\mathfrak{p}$ is totally split in the extension K_z/K. In addition:*
2. *In the general case $\mathfrak{p}_k$ is split in the quadratic extension K_z/k_z.*
3. *In the special case with $\ell \equiv 1 \pmod 4$, if we denote by p the ideal of k below $\mathfrak{p}$, then p is totally split in the extension K_z/k (equivalently p is split in the quadratic extension K/k).*

Proof. Assume first that we are in the general case. Then τ acts transitively on the $\mathfrak{a}_i$, all of which are squarefree and coprime, and so any $\mathfrak{p}$ dividing $\mathfrak{a}_i$ must have $\ell-1$ nontrivial conjugates (including $\mathfrak{p}$ itself), establishing (1). Similarly, $\tau_2(\mathfrak{a}_i) = \mathfrak{a}_{i+(\ell-1)/2}$, and for the same reason the prime ideals of K_z dividing the $\mathfrak{a}_i$ come from prime ideals $\mathfrak{p}_k$ of k_z which split in K_z/k_z.

In the special case, if p splits as a product of h conjugate ideals in K_z, the decomposition group $D(\mathfrak{p}_z/p)$ has cardinality $ef = (\ell-1)/h$ hence is the subgroup of $\mathrm{Gal}(K_z/k)$ generated by τ^h since $[K_z : k] = \ell - 1$. Since $\tau^h(\mathfrak{a}_i) = \mathfrak{a}_{(\ell-3)h/2+i}$ and τ^h fixes $\mathfrak{p}_z$, it follows as before that $(\ell-1) \mid (\ell-3)h/2$. Now evidently $(\ell-1, (\ell-3)/2)$ is equal to 1 if $\ell \equiv 1 \pmod 4$ and to 2 if $\ell \equiv 3 \pmod 4$. Thus when $\ell \equiv 1 \pmod 4$ we deduce as above that $(\ell-1) \mid h$ hence that $e = f = 1$, so that p is totally split in K_z/k. On the other hand if $\ell \equiv 3 \pmod 4$ we only have $(\ell-1)/2 \mid h$. If $h = \ell-1$ then p is again totally split. On the other hand, if $h = (\ell-1)/2$ then $ef = 2$, so p is either inert or ramified in the quadratic extension K/k, so $\mathfrak{p}$ is totally split in K_z/K. □

Note that in the special case with $\ell \equiv 3 \pmod 4$ the ideal p can be inert, split, or ramified in the quadratic extension K/k.

This leads to the following definition:

Definition 2.12. *We define $\mathcal{D}$ (resp., $\mathcal{D}_\ell$) to be the set of all prime ideals p of k with $p \nmid \ell$ (resp., with $p \mid \ell$) such that the prime ideals $\mathfrak{p}_z$ of K_z above p satisfy the above conditions (in other words $\mathfrak{p}$ totally split in K_z/K, and in addition in the general case $\mathfrak{p}_k$ split in K_z/k_z, and in the special case with $\ell \equiv 1 \pmod 4$, p split in K/k).*

Thus the above corollary says that the prime ideals p of k below prime ideals of K_z dividing one of the $\mathfrak{a}_i$ belong to $\mathcal{D} \cup \mathcal{D}_\ell$.

2.3. **The Mirror Field.** We now introduce the *mirror field* of K. When $\ell = 3$ this notion is classical and well-known; the mirror field of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Q}(\sqrt{-3D})$ and the *Scholz reflection principle* establishes that the 3-ranks of their class groups differ by at most 1.

In the case $\ell > 3$ this notion is less well known but does appear in the literature (see for instance the works of G. Gras [19] and [20]), and in particular Scholz's theorem can be generalized to this context, see for instance [24] for the case $\ell = 5$.

Definition 2.13. *In the general case, we define the* mirror field *K' of K (implicitly, with respect to the prime ℓ) to be the degree $\ell-1$ subextension of K_z/k fixed by $\tau^{(\ell-1)/2}\tau_2$.*

We do not define the mirror field for the special case, although we could say that it is $k_z = K_z$, so in this subsection we assume that we are in the general case.

Lemma 2.14. *Write $K = k(\sqrt{D})$ for some $D \in k^* \setminus k^{*2}$.*

1. *We have $K' = k\big(\sqrt{D}(\zeta_\ell - \zeta_\ell^{-1})\big)$.*
2. *The field K' is a quadratic extension of $k(\zeta_\ell + \zeta_\ell^{-1})$, more precisely*
$$K' = k(\zeta_\ell + \zeta_\ell^{-1})\Big(\sqrt{-D(4-\alpha^2)}\Big)\ ,$$
where $\alpha = \zeta_\ell + \zeta_\ell^{-1}$.

(3) *The extension K'/k is cyclic of degree $\ell-1$, and if $k=\mathbb{Q}$ we have*
$$\zeta_{K'}(s)=\prod_{0\le j<\ell-1}L((\omega\chi_D)^j,s)\ ,$$
where ω is a generator of the group of characters modulo ℓ, $\chi_D(n)=\left(\frac{D}{n}\right)$, and $(\omega\chi_D)^j$ is an abuse of notation for the primitive character equivalent to it.

Proof. Straightforward; for (2), note that $-D(4-\alpha^2)=D(\zeta_\ell-\zeta_\ell^{-1})^2$, and for (3) see Theorem 4.3 of [35]. □

The point of introducing the mirror field is the following result:

Proposition 2.15. *Assume that we are in the general case. As before, let p be a prime ideal of k, $\mathfrak{p}_z$ an ideal of K_z above p, and $\mathfrak{p}_k$ and $\mathfrak{p}$ the prime ideals below $\mathfrak{p}_z$ in k_z and K respectively. The following are equivalent:*

(1) *The ideals $\mathfrak{p}_k$ and $\mathfrak{p}$ are both totally split in K_z/k_z and K_z/K respectively (in other words $p\in\mathcal{D}\cup\mathcal{D}_\ell$).*
(2) *The ideal p is totally split in K'/k.*
(3) *Exactly one of following is true:*
   (a) *p is split in K/k and totally split in k_z/k.*
   (b) *p is inert in K/k and split in k_z/k as a product of $(\ell-1)/2$ prime ideals of degree 2.*
   (c) *p is above ℓ, is ramified in K/k, and its absolute ramification index $e(p/\ell)$ is an odd multiple of $(\ell-1)/2$ (equivalently $e(\mathfrak{p}/\ell)$ is an odd multiple of $\ell-1$).*

In particular (by Corollary 2.11), (1)-(3) are all true if $\mathfrak{p}_z$ divides some $\mathfrak{a}_i$.

Proof. (1) if and only if (2): We see that any nontrivial elements of $D(\mathfrak{p}_z/p)$ must be of the form $\tau^i\tau_2$ with $i\not\equiv 0 \pmod{\ell-1}$, and squaring we have $\tau^{2i}\in D(\mathfrak{p}_z/p)$, so $2i\equiv 0\pmod{\ell-1}$, so $D(\mathfrak{p}_z/p)\subset\{1,\tau^{(\ell-1)/2}\tau_2\}$, yielding (2). The converse is proved similarly.

(2) implies (3): We first recall from [10] the following result:

Lemma 2.16. *Let K be any number field and $K_z=K(\zeta_\ell)$. The conductor of the extension K_z/K is given by the formula*
$$\mathfrak{f}(K_z/K)=\prod_{\substack{\mathfrak{p}\mid\ell\\ (\ell-1)\nmid e(\mathfrak{p}/\ell)}}\mathfrak{p}\ .$$

It follows in particular that if $p\nmid\ell$, or if $p\mid\ell$ and $(\ell-1)\mid e(p/\ell)$ then p is unramified in k_z/k, and therefore also (arguing via inertia groups) in K/k, since otherwise the ideal $\mathfrak{p}_k$ would be ramified in K_z/k_z. Thus, assuming (2), the only prime ideals p which can be ramified in K/k are with $p\mid\ell$ and $(\ell-1)\nmid e(p/\ell)$.

If p is split or inert in K/k, we check that $e(\mathfrak{p}_z|p)$ equals 1 or 2 respectively, showing (a) and (b). To check the last statement of (c) for ramified p, recall from [10] that $e(\mathfrak{p}_z/\mathfrak{p})=(\ell-1)/(\ell-1,e(\mathfrak{p}/\ell))$ which is equal to 1 by (1), hence $(\ell-1)\mid e(\mathfrak{p}/\ell)=e(\mathfrak{p}/p)e(p/\ell)$. Since $(\ell-1)\nmid e(p/\ell)$ we conclude that $e(p/\ell)=n(\ell-1)/2$ with n odd.

The converse is similarly proved and we omit the details. □

Corollary 2.17. *Let p be a prime ideal of k below a prime ideal $\mathfrak{p}_z$ dividing some $\mathfrak{a}_i$. If p is ramified in the quadratic extension K/k then p is above ℓ.*

Proof. The general case has already been proved and used above. In the special case, K/k is a subextension of k_z/k, and the only prime ideals of k ramified in k_z/k are above ℓ. □

Corollary 2.18. *In both the general and special cases, assume that for any prime ideal p of k above ℓ the absolute ramification index $e(p/\ell)$ is not divisible by $(\ell-1)/2$. Then all the ideals $\mathfrak{a}_i$ defined above are coprime to ℓ.*

Proof. With notation as above, Corollary 2.11 implies that $\mathfrak{p}$ is unramified in K_z/K, hence $\mathfrak{p}\nmid\mathfrak{f}(K_z/K)$, so by Lemma 2.16 $(\ell-1)\mid e(\mathfrak{p}/\ell)=e(\mathfrak{p}/p)e(p/\ell)$. Since $e(\mathfrak{p}/p)=1$ or 2 this implies that $(\ell-1)/2\mid e(p/\ell)$, a contradiction. ☐

Note that for $\ell=3$ this corollary is empty, but the conclusion of the corollary always holds when $\ell>2[k:\mathbb{Q}]+1$, and in particular when $k=\mathbb{Q}$ and $\ell\geq 5$.

Proposition 2.19. *There exists an ideal $\mathfrak{a}_\alpha$ of K such that $\prod_{0\leq i\leq\ell-2}\mathfrak{a}_i=\mathfrak{a}_\alpha\mathbb{Z}_{K_z}$. In addition:*

1. *In the general (resp., special) case, $\mathfrak{a}_\alpha$ is stable by τ_2 (resp., by τ).*
2. *If either the assumption of Corollary 2.18 is satisfied (for instance when $\ell>2[k:\mathbb{Q}]+1$), or we are in the special case with $\ell\equiv 1\pmod 4$, then $\mathfrak{a}_\alpha=\mathfrak{a}'_\alpha\mathbb{Z}_K$ for some ideal $\mathfrak{a}'_\alpha$ of k.*

Proof. (1). In the general case, since $\tau(\mathfrak{a}_i)=\mathfrak{a}_{i-1}$ we have $\prod_{0\leq i\leq\ell-2}\mathfrak{a}_i=\mathfrak{a}_\alpha\mathbb{Z}_{K_z}$ with $\mathfrak{a}_\alpha=\mathcal{N}_{K_z/K}(\mathfrak{a}_0)$, and since $\tau_2(\mathfrak{a}_i)=\mathfrak{a}_{i+(\ell-1)/2}$, $\mathfrak{a}_\alpha$ is stable by τ_2. In the special case, since $\tau^2(\mathfrak{a}_i)=\mathfrak{a}_{i-2}$ we have $\prod_{0\leq i<(\ell-1)/2}\mathfrak{a}_{2i}=\mathcal{N}_{K_z/K}(\mathfrak{a}_0)\mathbb{Z}_{K_z}$ and $\prod_{0\leq i<(\ell-1)/2}\mathfrak{a}_{2i+1}=\mathcal{N}_{K_z/K}(\mathfrak{a}_1)\mathbb{Z}_{K_z}$, so that $\prod_{0\leq i<\ell-1}\mathfrak{a}_i=\mathfrak{a}_\alpha\mathbb{Z}_{K_z}$ with $\mathfrak{a}_\alpha=\mathcal{N}_{K_z/K}(\mathfrak{a}_0\mathfrak{a}_1)$ an ideal of K, and since $\tau(\mathfrak{a}_i)=\mathfrak{a}_{i+(\ell-3)/2}$, $\mathfrak{a}_\alpha$ is stable by τ.

(2). In the special case with $\ell\equiv 1\pmod 4$ then $(\ell-3)/2$ is odd, so since $\mathfrak{a}_1=\tau^{(\ell-3)/2}(\mathfrak{a}_0)$ it follows that $\tau(\mathcal{N}_{K_z/K}(\mathfrak{a}_0))=\mathcal{N}_{K_z/K}(\mathfrak{a}_1)$, so that $\prod_{0\leq i\leq\ell-2}\mathfrak{a}_i=\mathcal{N}_{K_z/k}(\mathfrak{a}_0)\mathbb{Z}_{K_z}=\mathfrak{a}'_\alpha\mathbb{Z}_{K_z}$ with $\mathfrak{a}'_\alpha$ an ideal of the base field k. On the other hand, if the assumption of Corollary 2.18 is satisfied then $\mathfrak{a}_\alpha$ is coprime to ℓ, hence by Corollary 2.17 it is not divisible by any prime ramified in K/k, and since it is stable by $\mathrm{Gal}(K/k)$ it comes from an ideal $\mathfrak{a}'_\alpha$ of k. ☐

3. Hecke Theory: Conductors

Our goal (see Theorem 3.8) is to give a usable expression for the "conductor" $f(L)$ in terms of the fundamental quantities $(\mathfrak{a}_0,\cdots,\mathfrak{a}_{\ell-2},\overline{u})$ given by Proposition 2.8, where we recall that the conductor of the C_ℓ-extension N/K is equal to $f(N/K)=f(L)\mathbb{Z}_K$ and that $\mathfrak{d}(L/k)=\mathfrak{d}(K/k)^{(\ell-1)/2}f(L)^{\ell-1}$.

As above, we will usually denote by p a prime ideal of k, by $\mathfrak{p}$ a prime ideal of K above p, by $\mathfrak{p}_z$ a prime ideal of K_z above $\mathfrak{p}$, and in the general case, by $\mathfrak{p}_k$ a prime ideal of k_z below $\mathfrak{p}_z$.

We first recall from [10] and [11] some results concerning the cyclotomic extensions k_z/k and K_z/K.

Remark 3.1. *By and large we stick to the notation of* [11]. *When we quote results proved in* [11] *for the extension denoted K_z/K there, we always apply them to our K_z/K except when otherwise noted.*

The notations $e(\mathfrak{p})$, $A_\alpha(\mathfrak{p})$, $a_\alpha(\mathfrak{p})$, and C_n have the same meaning in both papers, except that $A_\alpha(\mathfrak{p})$ is written $A_\alpha(\mathfrak{p}_z)$ in [11]. *The notation $h(\epsilon,a,\mathfrak{p})$ has the same meaning as $h(\epsilon,a,e(\mathfrak{p}))$ of* [11] *(**confirm**), except possibly when $\epsilon=0$, $(\ell-1)\mid e$, and $\ell\mid a$. The notation $m(\mathfrak{p})$ of* [11] *is the same as $M(\mathfrak{p})$ here.*

Proposition 3.2. *Keep the above notation, assume that p lies over ℓ, and write $e(\mathfrak{p})$ and $e(p)$ for the respective absolute ramification indices over ℓ. Then we have*

$$e(\mathfrak{p}_z/\mathfrak{p})=\frac{\ell-1}{(\ell-1,e(\mathfrak{p}))}\quad\text{and}\quad\frac{e(\mathfrak{p}_z/\ell)}{\ell-1}=\frac{e(\mathfrak{p})}{(\ell-1,e(\mathfrak{p}))}\,. \tag{3.1}$$

Proof. Immediate from Theorem 2.1 of [11]. ☐

Definition 3.3. *Suppose that p, $\mathfrak{p}$, and $\mathfrak{p}_z$ are ideals as above, and that they lie over ℓ, so that $e(\mathfrak{p}_z/p)\mid(\ell-1)$. Moreover, let $\overline{\alpha}\in(K_z^*/K_z^{*\ell})[T]$ be as in Proposition 2.4.*

1. *If $p\mathbb{Z}_K=\mathfrak{p}^2$ in K/k we set $p^{1/2}=\mathfrak{p}$, and if $\mathfrak{p}\mathbb{Z}_{K_z}=\mathfrak{p}_z^{e(\mathfrak{p}_z/\mathfrak{p})}$ in K_z/K, we set $\mathfrak{p}_z=\mathfrak{p}^{1/e(\mathfrak{p}_z/\mathfrak{p})}$.*
2. *We say that an ideal p of k divides some $\mathrm{Gal}(K_z/k)$-invariant ideal $\mathfrak{b}$ of K (resp., of K_z) when $(p\mathbb{Z}_K)^{1/e(\mathfrak{p}/p)}$ (resp., $(p\mathbb{Z}_K)^{1/e(\mathfrak{p}_z/p)}$) does, or equivalently when $\mathfrak{p}$ (resp., $\mathfrak{p}^{1/e(\mathfrak{p}_z/\mathfrak{p})}$) does, where this last condition is independent of the choice of ideal $\mathfrak{p}$ of K above p.*

(3) *If e is an integer, write $r(e)$ for the unique integer such that $e \equiv r(e) \pmod{\ell-1}$ and $1 \le r(e) \le \ell-1$.*
(4) *We write*

$$M(\mathfrak{p}) = \frac{\ell e(\mathfrak{p}_z/\ell)}{\ell-1} = \frac{\ell e(\mathfrak{p})}{(\ell-1,e(\mathfrak{p}))} \in \mathbb{Z}\ , \quad m(\mathfrak{p}) = \frac{M(\mathfrak{p})}{e(\mathfrak{p}_z/\mathfrak{p})} = \frac{\ell e(\mathfrak{p})}{\ell-1}\ .$$

(5) *Denote by D_n the congruence $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$ in K_z.*
(6) *Define quantities $A_\alpha(p)$ and $a_\alpha(p)$ as follows:*
   - *If D_n is soluble for $n = M(\mathfrak{p})$, we set $A_\alpha(\mathfrak{p}) = M(\mathfrak{p})+1$ and $a_\alpha(\mathfrak{p}) = m(\mathfrak{p})$.*
   - *Otherwise, if $n < M(\mathfrak{p})$ is the largest exponent for which it is soluble, we set $A_\alpha(\mathfrak{p}) = n$ and we define*

$$a_\alpha(\mathfrak{p}) = \frac{A_\alpha(\mathfrak{p}) - r(e(\mathfrak{p}))/(\ell-1,e(\mathfrak{p}))}{e(\mathfrak{p}_z/\mathfrak{p})} = \left\lceil \frac{A_\alpha(\mathfrak{p})}{e(\mathfrak{p}_z/\mathfrak{p})} \right\rceil - 1 \in \mathbb{Z}\ .$$

Remarks 3.4. *(1) The quantity $r(e(\mathfrak{p}))/(\ell-1,e(\mathfrak{p})) = r(e(\mathfrak{p}))/(\ell-1,r(e(\mathfrak{p})))$ is easily seen to be an integer, and equals $q=1$ when $\ell=3$ or when $k=\mathbb{Q}$ for instance.*
(2) The notation $A_\alpha(\mathfrak{p})$ and $a_\alpha(\mathfrak{p})$ (instead of $A_\alpha(\mathfrak{p}_z)$ and $a_\alpha(\mathfrak{p}_z)$) is justified by the following lemma:

Lemma 3.5. *With the above assumptions, the solubility of D_n (the congruence $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$) is independent of the ideal $\mathfrak{p}_z$ of K_z above p. In other words, using the notation of Definition 3.3, it is equivalent to $x^\ell/\alpha \equiv 1 \pmod{{}^*p^{n/e(\mathfrak{p}_z/p)}}$ or to $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}^{n/e(\mathfrak{p}_z/p)}}$.*

Proof. If $\mathfrak{p}_z'$ is another ideal above p, there exists $h = \tau^i\tau_2^j \in \mathrm{Gal}(K_z/k)$ with $\mathfrak{p}_z' = h(\mathfrak{p}_z)$ (resp., simply $h = \tau^i$ in the special case). Thus if $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$ we have $h(x)^\ell/h(\alpha) \equiv 1 \pmod{{}^*\mathfrak{p}_z'^n}$. However, since $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[T]$, modulo ℓth powers we have $\overline{\tau(\alpha)} = \overline{\alpha^g}$ and $\overline{\tau_2(\alpha)} = \overline{\alpha^{-1}}$ (resp., $\overline{\tau(\alpha)} = \overline{\alpha^{-g}}$), hence $h(\alpha) = \alpha^{(-1)^j g^i}\gamma^\ell$ (resp., $h(\alpha) = \alpha^{(-1)^i g^i}\gamma^\ell$) for some $\gamma \in K_z^*$. We deduce that $y^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z'^n}$, with $y = (h(x)/\gamma)^{(-1)^j g^{-i} \bmod \ell}$ (resp., $y = (h(x)/\gamma)^{(-1)^i g^{-i} \bmod \ell}$), proving the lemma. ☐

Note that thanks to this lemma we could even write $A_\alpha(p)$ and $a_\alpha(p)$ instead of $A_\alpha(\mathfrak{p})$ and $a_\alpha(\mathfrak{p})$, but since it is the ideal $\mathfrak{p}$ of K which occurs in most formulas, we have preferred the latter notation, keeping in mind that these quantities are independent of the ideal $\mathfrak{p}$ of K above p.

Proposition 3.6. *(1) We have $\ell \nmid A_\alpha(\mathfrak{p})$, and if $A_\alpha(\mathfrak{p}) < M(\mathfrak{p})$ (equivalently, if $A_\alpha(\mathfrak{p}) < M(\mathfrak{p})-1$) then*

$$A_\alpha(\mathfrak{p}) \equiv \frac{e(\mathfrak{p})}{(\ell-1,e(\mathfrak{p}))} \left(\bmod\ \frac{\ell-1}{(\ell-1,e(\mathfrak{p}))}\right)\ .$$

(2) We have $a_\alpha(\mathfrak{p}) = m(\mathfrak{p})$ if $A_\alpha(\mathfrak{p}) = M(\mathfrak{p})+1$, and otherwise

$$0 \le a_\alpha(\mathfrak{p}) \le \frac{\ell e(\mathfrak{p})}{\ell-1} - \frac{\ell-1+r(e(\mathfrak{p}))}{\ell-1} < \frac{\ell e(\mathfrak{p})}{\ell-1} - 1 = m(\mathfrak{p}) - 1\ .$$

Proof. (1) follows from Proposition 3.8 of [11], and follows from the definitions and from (3.1). ☐

Remark 3.7. *As mentioned in* [12]*, the congruence (1), or equivalently the integrality of $a_\alpha(\mathfrak{p})$ (when $A_\alpha(\mathfrak{p}) < M(\mathfrak{p})$) comes from a subtle although very classical computation involving higher ramification groups; see Proposition 3.6 of* [11] *along with Chapter 4 of* [34].

We can now quote the crucial result from [11] which gives the conductor of the extension N/K:

Theorem 3.8. [11, Theorem 3.15] *Assume that $(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})$ are as in Proposition 2.8, so that $\prod_{0\le i\le \ell-2}\mathfrak{a}_i = \mathfrak{a}_\alpha\mathbb{Z}_{K_z}$ with $\mathfrak{a}_\alpha$ an ideal of K stable by τ_2 (resp., by τ in the special case), and sometimes coming from k (see Proposition 2.19). Then the conductor of the associated field extension N/K is given as follows:*

$$f(N/K) = \ell\mathfrak{a}_\alpha \frac{\prod_{\mathfrak{p}\mid\ell}\mathfrak{p}^{\lceil e(\mathfrak{p})/(\ell-1)\rceil}}{\prod_{\mathfrak{p}\mid\ell,\ \mathfrak{p}\nmid\mathfrak{a}_\alpha}\mathfrak{p}^{\lceil a_\alpha(\mathfrak{p})\rceil}}\ .$$

Remark 3.9. *One can now draw additional conclusions about the $a_\alpha(\mathfrak{p})$. For example, suppose that p is a prime ideal k above ℓ with $p\mathbb{Z}_K = \mathfrak{p}^2$, $\mathfrak{p} \nmid \mathfrak{a}_\alpha$ and $a_\alpha(\mathfrak{p}) < m(\mathfrak{p})$. Then $v_\mathfrak{p}(f(N/K)/\ell) \equiv 0 \pmod 2$, as $f(N/K) = f(L)\mathbb{Z}_K$ for an ideal $f(L)$ of k, and it follows from the theorem and Proposition 3.6 that*

$$a_\alpha(\mathfrak{p}) \equiv \lceil e(\mathfrak{p})/(\ell-1)\rceil \pmod 2. \tag{3.2}$$

Definition 3.10. *Recall that $m(\mathfrak{p}) = \ell e(\mathfrak{p})/(\ell-1)$. Let $a \in \mathbb{Q}$ be such that either $a = m(\mathfrak{p})$ or a is an integer such that $0 \le a \le m(\mathfrak{p}) - (\ell - 1 + r(e(\mathfrak{p})))/(\ell-1)$. For $\varepsilon = 0$ or 1 we define $h(\varepsilon, a, \mathfrak{p})$ as follows:*

(1) When $a = m(\mathfrak{p})$ we set $h(0, a, \mathfrak{p}) = 0$.

(2) When $a < m(\mathfrak{p})$, we set

$$h(0,a,\mathfrak{p}) = \begin{cases} 0 & \text{if } (\ell-1) \nmid e(\mathfrak{p}) \ , \\ 1 & \text{if } (\ell-1) \mid e(\mathfrak{p}) \ . \end{cases}$$

(3) We set for all a

$$h(1,a,\mathfrak{p}) = \begin{cases} 1 & \text{if } (\ell-1) \nmid e(\mathfrak{p}) \ , \\ 2 & \text{if } (\ell-1) \mid e(\mathfrak{p}) \ . \end{cases}$$

Remarks 3.11. *(1) Note the trivial but important fact $h(1, a, \mathfrak{p})$ is independent of a and that $h(0, a, \mathfrak{p})$ depends on whether $a = m(\mathfrak{p})$. As usual these quantities in fact depend on the ideal $\mathfrak{p}$ only via the prime p of k below $\mathfrak{p}$.*

(2) Note that if $\ell > 2[k : \mathbb{Q}]+1$, for instance when $k = \mathbb{Q}$ and $\ell \ge 5$, we have $e(\mathfrak{p}) < \ell-1$ so $(\ell-1) \nmid e(\mathfrak{p})$. Thus in this case we simply have $h(\varepsilon, a, \mathfrak{p}) = \varepsilon$, independently of a and $\mathfrak{p}$. We will also see in Remark 4.7 that a number of other formulas simplify.

Lemma 3.12. *Let $\mathfrak{p}$ be a prime ideal of K above ℓ and denote by C_n the congruence $x^\ell/\alpha \equiv 1 \pmod{^*\mathfrak{p}^n}$ in K_z. Then $a_\alpha(\mathfrak{p})$ is equal to the unique value of a as in the previous definition such that C_n is soluble for $n = a + h(0, a, \mathfrak{p})$ and not soluble for $n = a + h(1, a, \mathfrak{p})$, where this last condition is ignored if $a + h(1, a, \mathfrak{p}) > M(\mathfrak{p})$.*

Proof. By Lemma 3.5 the solubility of D_n is equivalent to that of $C_{n/e(\mathfrak{p}_z/\mathfrak{p})}$. If $a = a_\alpha(\mathfrak{p}) = m(\mathfrak{p})$, then D_n is soluble for $n = \ell e(\mathfrak{p}_z/\ell)/(\ell-1)$, which is equivalent to $C_{m(\mathfrak{p})} = C_a$ as desired.

If $a = a_\alpha(\mathfrak{p}) < m(\mathfrak{p})$, we have $A_\alpha(\mathfrak{p}) = ae(\mathfrak{p}_z/\mathfrak{p}) + r(e(\mathfrak{p}))/(\ell-1, e(\mathfrak{p}))$, and Proposition 3.6 (1) implies that the solubility of D_n for $n = A_\alpha(\mathfrak{p})$ is equivalent to that of $D_{n'}$ when $A_\alpha(\mathfrak{p}) - (\ell-1)/(\ell-1, e(\mathfrak{p})) < n' \le A_\alpha(\mathfrak{p})$. If $(\ell-1) \nmid e(\mathfrak{p})$ we have $r(e(\mathfrak{p})) < \ell - 1$ and choose $n' = ae(\mathfrak{p}_z/\mathfrak{p})$, while if $(\ell-1) \mid e(\mathfrak{p})$ we choose $n' = n = ae(\mathfrak{p}_z/\mathfrak{p}) + 1$. Thus the solubility of $D_{A_\alpha(\mathfrak{p})}$ and $D_{n'}$ is equivalent to that of $C_{n''}$, where $n'' = n'/e(\mathfrak{p}_z/\mathfrak{p}) = a + h(0, a, \mathfrak{p})$ by definition of $h(0, a, \mathfrak{p})$. (Recall that $e(\mathfrak{p}_z/\mathfrak{p}) = 1$ when $(\ell-1) \mid e(\mathfrak{p})$.)

Furthermore the nonsolubility of D_n for $n = A_\alpha(\mathfrak{p}) + 1$ is equivalent to that of $D_{n'}$ when $A_\alpha(\mathfrak{p}) < n' \le A_\alpha(\mathfrak{p}) + (\ell-1)/(\ell-1, e(\mathfrak{p}))$ (when the upper bound is less than $M(\mathfrak{p})$). If $(\ell-1) \nmid e(\mathfrak{p})$ we have $1 \le r(e(\mathfrak{p})) < \ell - 1$ and choose $n' = ae(\mathfrak{p}_z/\mathfrak{p}) + (\ell-1)/(\ell-1, e(\mathfrak{p}))$, while if $(\ell-1) \mid e(\mathfrak{p})$ we choose $n' = A_\alpha(\mathfrak{p}) + 1 = ae(\mathfrak{p}_z/\mathfrak{p}) + 2$. Thus the nonsolubility of $D_{A_\alpha(\mathfrak{p})+1}$ and $D_{n'}$ are equivalent to that of $C_{n''}$, where $n'' = n'/e(\mathfrak{p}_z/\mathfrak{p}) = a + h(1, a, \mathfrak{p})$, proving the lemma. $\square$

The above proof shows that the definition of $h(\varepsilon, a, \mathfrak{p})$ is unique if we require that $h(\varepsilon, a, \mathfrak{p}) \in \mathbb{Z}$ and that the above lemma be satisfied.

4. The Dirichlet Series

Since $f(N/K) = f(L)\mathbb{Z}_K$ for some ideal $f(L)$ of k, we have $\mathcal{N}_{K/\mathbb{Q}}(f(N/K)) = \mathcal{N}_{k/\mathbb{Q}}(f(L))^2$. To emphasize the fact that we are mainly interested in the norm from $k/\mathbb{Q}$, we set the following definition (norms from extensions other than $k/\mathbb{Q}$ will always indicate the field extension explicitly):

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, we set*
$$\mathcal{N}(\mathfrak{a})=\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})^{1/2}\ .$$
In particular, for each ideal $\mathfrak{a}$ of k we have $\mathcal{N}(\mathfrak{a})=\mathcal{N}(\mathfrak{a}\mathbb{Z}_K)$.

Recall that we set
$$\Phi_\ell(K,s)=\frac{1}{\ell-1}+\sum_{L\in\mathcal{F}_\ell(K)}\frac{1}{\mathcal{N}(f(L))^s}\ ,$$
and $f(N/K)=f(L)\mathbb{Z}_K$ is given by Theorem 3.8. By Proposition 2.4, we have
$$(\ell-1)\Phi_\ell(K,s)=\sum_{\overline{\alpha}\in(K_z^*/{K_z^*}^\ell)[T]}\frac{1}{\mathcal{N}(f(L))^s}\ ,$$
where $L=K_z(\sqrt[\ell]{\alpha})^G$ (including $\overline{\alpha}=1$ corresponding to $L=K_z^G=k$ with $f(L)=\mathbb{Z}_k$ and $\mathcal{N}(f(L))=1$), so by Proposition 2.8, we have
$$(\ell-1)\Phi_\ell(K,s)=\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\ \sum_{\overline{u}\in S_\ell(K_z)[T]}\frac{1}{\mathcal{N}(f(L))^s}\ ,$$
where J is the set of $(\ell-1)$uples of ideals satisfying condition (a) of Proposition 2.8, and $f(L)$ is the conductor of the extension corresponding to $(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2},\overline{u})$. Thus, replacing $f(L)$ by the formula given by Theorem 3.8, recalling that $\prod_{\mathfrak{p}\mid\ell}\mathcal{N}(\mathfrak{p})^{e(\mathfrak{p})}=\ell^{[k:\mathbb{Q}]}$, and writing
$$e(\mathfrak{p})=(\lceil e(\mathfrak{p})/(\ell-1)\rceil-1)(\ell-1)+r(e(\mathfrak{p}))\ ,$$
we obtain
$$(\ell-1)\Phi_\ell(K,s)=\ell^{-\frac{\ell}{\ell-1}[k:\mathbb{Q}]s}\prod_{\mathfrak{p}\mid\ell}\mathcal{N}(\mathfrak{p})^{-\frac{\ell-1-r(e(\mathfrak{p}))}{\ell-1}s}\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,\tag{4.1}$$
where
$$S_\alpha(s)=\sum_{\overline{u}\in S_\ell(K_z)[T]}\ \prod_{\substack{\mathfrak{p}\mid\ell\\ \mathfrak{p}\nmid\mathfrak{a}_\alpha}}\mathcal{N}(\mathfrak{p})^{\lceil a_{\alpha u}(\mathfrak{p})\rceil s}\ ,$$
and where α is any element of K_z^* such that $\overline{\alpha}\in(K_z^*/{K_z^*}^\ell)[T]$ and $\mathfrak{q}_0^\ell\prod_{0\le i\le\ell-2}\mathfrak{a}_i^{g^i}=\alpha\mathbb{Z}_{K_z}$ for some ideal $\mathfrak{q}_0$.

Definition 4.2. *For $\alpha\in K_z^*$ and an ideal $\mathfrak{b}$ of K_z, we introduce the function*
$$f_\alpha(\mathfrak{b})=|\{\overline{u}\in S_\ell(K_z)[T],\ x^\ell/(\alpha u)\equiv 1\pmod{^*\mathfrak{b}}\quad\textit{soluble in }K_z\}|\ ,$$
with the convention that $f_\alpha(\mathfrak{b})=0$ if $\mathfrak{b}\nmid(1-\zeta_\ell)^\ell\mathbb{Z}_{K_z}$.

Let p_i for $1\le i\le g$ be the prime ideals of k above ℓ and not dividing $\mathfrak{a}_\alpha$, and for each i let a_i be such that either $a_i=m(\mathfrak{p}_i)$, or $0\le a_i\le m(\mathfrak{p}_i)-\frac{(\ell-1)+r(e(\mathfrak{p}_i))}{\ell-1}=\lceil m(\mathfrak{p}_i)\rceil-2$ with $a_i\in\mathbb{Z}$, where as usual $\mathfrak{p}_i$ is an ideal of K above p_i, and let A be the set of such $(a_1,\dots,a_g)$. Noting that thanks to the convention of Definition 4.1 we have $\prod_{\mathfrak{p}_i\mid p_i}\mathcal{N}(\mathfrak{p}_i)=\mathcal{N}(p_i)^{1/e(\mathfrak{p}_i/p_i)}$, we thus have
$$S_\alpha(s)=\sum_{(a_1,\dots,a_g)\in A}\ \prod_{1\le i\le g}\mathcal{N}(p_i)^{\lceil a_i\rceil s/e(\mathfrak{p}_i/p_i)}\sum_{\substack{\overline{u}\in S_\ell(K_z)[T]\\ \forall i,\ a_{\alpha u}(\mathfrak{p}_i)=a_i}}1\ .$$

Note that there are conditions on the a_i, e.g. (3.2), such that the inner sum vanishes for impossible choices of the a_i.

By Lemma 3.12, we have $a_{\alpha u}(\mathfrak{p}_i) \ge a_i$ if and only if $\overline{u}$ is counted by $f_\alpha(\mathfrak{p}_i^{b_i})$, where $b_i = a_i + h(0, a, \mathfrak{p}_i)$, and we rewrite $\mathfrak{p}_i^{b_i} = p_i^{b_i/e(\mathfrak{p}_i/p_i)}$. By inclusion-exclusion the inner sum is equal to

$$S_\alpha(s) = \sideset{}{'}\sum_{\substack{(b_1,\dots,b_g)\in B\\(\varepsilon_1,\dots,\varepsilon_g)\in\{0,1\}^g}} \prod_{1\le i\le g} \mathcal{N}(p_i)^{\lceil v(b_i,\varepsilon_i)\rceil s/e(\mathfrak{p}_i/p_i)}(-1)^{\sum_i \varepsilon_i} f_\alpha\left(\prod_{1\le i\le g} p_i^{b_i/e(\mathfrak{p}_i/p_i)}\right) ,$$

where: B is the set of g-uples $(b_1,\dots,b_g)$ with $0 \le b_i \le m(\mathfrak{p}_i)$, $b_i \in \mathbb{Z}\cup\{m(\mathfrak{p}_i)\}$; $v(b_i,\varepsilon_i) = b_i - h(\varepsilon_i, b_i, p_i)$; and the sum is restricted to those b_i and ε_i for which $(v(b_1,\varepsilon_i),\dots,v(b_g,\varepsilon_g)) \in A$.

Lemma 4.3. *We have*

$$S_\alpha(s) = \sum_{(b_1,\dots,b_g)\in B} f_\alpha\left(\prod_{1\le i\le g} p_i^{b_i/e(\mathfrak{p}_i/p_i)}\right) \prod_{1\le i\le g}\left(\mathcal{N}(p_i)^{\lceil b_i\rceil s/e(\mathfrak{p}_i/p_i)} Q(p_i^{b_i/e(\mathfrak{p}_i/p_i)}, s)\right) ,$$

where $Q(p^{b/e(\mathfrak{p}/p)}, s)$ is defined as follows. Let as usual $\mathfrak{p}$ be an ideal of K above p and define $q = \mathcal{N}(p)^{1/e(\mathfrak{p}/p)}$. Then if $b = m(\mathfrak{p})$ or $0 \le b < m(\mathfrak{p})$ with $b \in \mathbb{Z}$:

(1) If $(\ell-1)\nmid e(\mathfrak{p})$ we set

$$Q(p^{b/e(\mathfrak{p}/p)}, s) = \begin{cases} 1 & \text{if} \quad b = 0\ , \\ 1 - 1/q^s & \text{if} \quad 1 \le b \le \lceil m(\mathfrak{p})\rceil - 2\ , \\ -1/q^s & \text{if} \quad b = \lceil m(\mathfrak{p})\rceil - 1\ , \\ 1 & \text{if} \quad b = m(\mathfrak{p})\ . \end{cases}$$

(2) If $(\ell-1)\mid e(\mathfrak{p})$ we set

$$Q(p^{b/e(\mathfrak{p}/p)}, s) = \begin{cases} 1 & \text{if} \quad b = 0\ , \\ 1/q^s & \text{if} \quad b = 1\ , \\ 1/q^s - 1/q^{2s} & \text{if} \quad 2 \le b \le m(\mathfrak{p}) - 1\ , \\ 1 - 1/q^{2s} & \text{if} \quad b = m(\mathfrak{p})\ . \end{cases}$$

Proof. Since the indices are independent, it is enough to prove the formulas for $g = 1$, and this is easily done just by expanding the sum over ε, and using Definition 3.10 to check the condition $v(b,\varepsilon) \in A$. Note (as was mentioned in [14]) that the corresponding value for $b = 0$ was mistakenly written as 0 in [12]; it must be 1, so that the corresponding factor Q is omitted from the product. $\square$

Definition 4.4. *(1) We let $\mathcal{B}$ be the set of formal products of the form $\mathfrak{b} = \prod_{p_i\mid\ell} p_i^{b_i/e(\mathfrak{p}_i/p_i)}$, where the b_i are such that $0 \le b_i \le m(\mathfrak{p}_i)$ and $b_i \in \mathbb{Z}\cup\{m(\mathfrak{p}_i)\}$.*

(2) We will consider any $\mathfrak{b} \in \mathcal{B}$ as an ideal of K, where by abuse of language we accept to have fractional powers of prime ideals of K, and we will set $\mathfrak{b}_z = \mathfrak{b}\mathbb{Z}_{K_z}$, which is a true ideal of K_z stable by τ, and also by τ_2 in the general case.

(3) If $\mathfrak{b} \in \mathcal{B}$ as above, we set

$$\lceil\mathcal{N}\rceil(\mathfrak{b}) = \prod_{p_i\mid\mathfrak{b}} \mathcal{N}(p_i)^{\lceil b_i\rceil/e(\mathfrak{p}_i/p_i)} \quad \text{and} \quad P(\mathfrak{b}, s) = \prod_{p_i\mid\mathfrak{b}} Q(p_i^{b_i/e(\mathfrak{p}_i/p_i)}, s) = \prod_{p\mid\mathfrak{b}} Q(p^{v_p(\mathfrak{b})}, s)\ .$$

Remark 4.5. *The ideals $\mathfrak{b}_z$ for $\mathfrak{b} \in \mathcal{B}$ nearly, but not exactly, correspond to the ideals $\mathfrak{b}_z$ considered at the beginning of Section 2.2 of [11]. In the general case, the correspondence is exact, with K_z/K having the same meaning, except that here we additionally demand that $\mathfrak{b}_z$ be invariant by τ_2. In particular, all of the results of Section 2.2 carry over without change.*

In the special case, we can interpret the field extension K_z/K of [11] *to be either K_z/K or K_z/k here. Generally speaking, and in particular when quoting* (3.8)*, we use the former interpretation, so that the notation matches up and the set of $\mathfrak{b}_z$ considered is the same. One difference is that τ in* [11] *is τ^2 here.*

In Theorem 5.4 we rely on the latter interpretation. In this case, our bounds on b_i still correspond to the bounds on $v_{\mathfrak{p}}$ (with $\mathfrak{p}$ there corresponding to p here), but $v_{\mathfrak{p}}$ is now allowed to be a half-integer. Most but not all of the results of Section 2.2 remain valid in this case, so we must be careful when quoting them.

(This makes me uneasy....)

We set $E = \{p_1, \dots, p_g\} \subset \{p \mid \ell\mathbb{Z}_k\}$ to be the set of prime ideals of k above ℓ not dividing $\mathfrak{a}_\alpha$, so that [5]

$$(\mathfrak{a}_\alpha, \ell\mathbb{Z}_K) = \prod_{\substack{p_i\mid\ell,\ p_i\notin E\\ \mathfrak{p}_i\mid p_i}} \mathfrak{p}_i\ .$$

We obtain

$$\begin{aligned}\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} &= \sum_{E\subset\{p\mid\ell\}}\ \sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p\mid\ell,p\nmid\mathfrak{a}_\alpha\}=E}}\frac{1}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ \times\\ &\quad \sum_{(b_1,\dots,b_g)\in B} f_\alpha\left(\prod_{1\le i\le g} p_i^{b_i/e(\mathfrak{p}_i/p_i)}\right)\prod_{p_i\in E}\left(Q(p_i^{b_i/e(\mathfrak{p}_i/p_i)},s)\mathcal{N}(p_i)^{\lceil b_i\rceil s/e(\mathfrak{p}_i/p_i)}\right)\\ &= \sum_{E\subset\{p\mid\ell\}}\ \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ p\mid\mathfrak{b}\Rightarrow p\in E}}\lceil\mathcal{N}\rceil(\mathfrak{b})^s\prod_{p_i\in E}Q(p_i^{b_i/e(\mathfrak{p}_i/p_i)},s)\sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p\mid\ell,p\nmid\mathfrak{a}_\alpha\}=E}}\frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ .\end{aligned}$$

As can be seen from Definition 3.10, when $(\ell-1)\mid e(\mathfrak{p})$ we have $b_i>0$, so the terms with $b_i=0$ can be omitted in the product.

Thus we can write

$$\begin{aligned}\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} &= \sum_{E\subset\{p\mid\ell\}}\ \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ p\mid\mathfrak{b}\Rightarrow p\in E\\ p\in E\text{ and }(\ell-1)\mid e(\mathfrak{p})\Rightarrow p\mid\mathfrak{b}}}\lceil\mathcal{N}\rceil(\mathfrak{b})^s\prod_{p\mid\mathfrak{b}}Q(p^{v_p(\mathfrak{b})},s)\sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p\mid\ell,\ p\nmid\mathfrak{a}_\alpha\}=E}}\frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\\ &= \sum_{\mathfrak{b}\in\mathcal{B}}\lceil\mathcal{N}\rceil(\mathfrak{b})^s P(\mathfrak{b},s)\sum_{\substack{E\subset\{p\mid\ell\}\\ p\mid\mathfrak{b}\Rightarrow p\in E\\ p\nmid\mathfrak{b}\text{ and }(\ell-1)\mid e(\mathfrak{p})\Rightarrow p\notin E}}\ \sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p\mid\ell,\ p\nmid\mathfrak{a}_\alpha\}=E}}\frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,\end{aligned}$$

so that

$$\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\mathfrak{b}\in\mathcal{B}}\lceil\mathcal{N}\rceil(\mathfrak{b})^s P(\mathfrak{b},s)\sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ (\mathfrak{a}_\alpha,\mathfrak{b})=1\\ \mathfrak{p}\nmid\mathfrak{b}\text{ and }(\ell-1)\mid e(\mathfrak{p})\Rightarrow\mathfrak{p}\mid\mathfrak{a}_\alpha}}\frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ . \tag{4.2}$$

[5]There is an unimportant misprint in [12], where the left-hand side of this formula is given as $\mathfrak{a}_\alpha$, but it should be $(\mathfrak{a}_\alpha, 3\mathbb{Z}_K)$. The rest of the computation is unchanged.

Definition 4.6. *(1) For $\mathfrak{b}$ as above we define*

$$\mathfrak{r}^e(\mathfrak{b}) = \prod_{\substack{\mathfrak{p}\mid \ell\mathbb{Z}_K,\ \mathfrak{p}\nmid\mathfrak{b} \\ (\ell-1)\mid e(\mathfrak{p})}} \mathfrak{p}\ .$$

(2) We set $\mathfrak{d}_\ell = \prod_{p\in\mathcal{D}_\ell} p$ (see Definition 2.12).

Remark 4.7. *The nontriviality of $\mathfrak{r}^e(\mathfrak{b})$ will introduce a few complications in our computations. Since $e(\mathfrak{p}) = e(\mathfrak{p}/p)e(p) \le 2[k:\mathbb{Q}]$, we note that if $\ell > 2[k:\mathbb{Q}]+1$ then $\mathfrak{r}^e(\mathfrak{b})$ is always trivial. This will in particular be the case for $k=\mathbb{Q}$ and $\ell \ge 5$, which we will study later. In particular, in view of the next lemma, when $\mathfrak{r}^e(\mathfrak{b})$ is trivial all ideals $\mathfrak{a}_i$ and $\mathfrak{a}_\alpha$ are coprime to ℓ.*

Lemma 4.8. *For each $\mathfrak{a}_\alpha$ appearing in the inner sum of (4.2) we have*

$$(\mathfrak{a}_\alpha, \ell\mathbb{Z}_K) = \mathfrak{r}^e(\mathfrak{b}) = \prod_{\substack{p\in D_\ell \\ (p,\mathfrak{b})=1}} \prod_{\mathfrak{p}\mid p} \mathfrak{p}\ , \tag{4.3}$$

so that $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_\ell$.

Additionally, in the special case with $\ell \equiv 1 \pmod 4$ we have $\mathfrak{r}^e(\mathfrak{b}) = \prod_{\substack{p\in D_\ell \\ (p,\mathfrak{b})=1}} p$.

Proof. If $\mathfrak{p} \nmid \mathfrak{b}$ and $(\ell-1) \mid e(\mathfrak{p})$ then clearly $\mathfrak{p} \mid \mathfrak{a}_\alpha$. Conversely, let $\mathfrak{p} \mid \mathfrak{a}_\alpha$ be above ℓ. Since $(\mathfrak{a}_\alpha, \mathfrak{b}) = 1$ we know that $\mathfrak{p} \nmid \mathfrak{b}$. If we had $(\ell-1) \nmid e(\mathfrak{p})$, Proposition 3.2 would imply that $e(\mathfrak{p}_z/\mathfrak{p}) > 1$, contradicting Corollary 2.11. This proves the first equality of (4.3), and the second equality follows in essentially the same way.

That $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_\ell$, and the formula in the special case, again follows by Corollary 2.11. □

Thus we obtain

$$\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J} \frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\substack{\mathfrak{b}\in\mathcal{B} \\ \mathfrak{r}^e(\mathfrak{b})\mid\mathfrak{d}_\ell}} \lceil\mathcal{N}\rceil(\mathfrak{b})^s P(\mathfrak{b},s) \sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J \\ (\mathfrak{a}_\alpha,\ell\mathbb{Z}_K)=\mathfrak{r}^e(\mathfrak{b})}} \frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}. \tag{4.4}$$

To compute $f_\alpha(\mathfrak{b})$ we set the following definition:

Definition 4.9. *For any ideal $\mathfrak{b}\in\mathcal{B}$, and for any subset T of $\mathbb{F}_\ell[G]$, we set*

$$S_\mathfrak{b}(K_z)[T] = \{\overline{u} \in S_\ell(K_z)[T],\ x^\ell/u \equiv 1 \pmod{{}^*\mathfrak{b}_z} \text{ soluble}\}\ ,$$

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

Lemma 4.10. *Let $(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})$ satisfy condition (a) of Proposition 2.8, suppose that α satisfies the condition described before Definition 4.2, and recall that we set $\mathfrak{a} = \prod_i \mathfrak{a}_i^{g^i}$. We have*

$$f_\alpha(\mathfrak{b}) = \begin{cases} |S_\mathfrak{b}(K_z)[T]| & \text{if } \overline{\mathfrak{a}} \in \mathrm{Cl}_\mathfrak{b}(K_z)^\ell\ , \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The lemma and its proof are a direct generalization of Lemma 5.3 of [12], and we omit the details. □

5. Computation of $|S_{\mathfrak{b}}(K_z)[T]|$

In this section we compute the size of the group $S_{\mathfrak{b}}(K_z)[T]$ appearing in Lemma 4.10, as well as several related quantities.

Lemma 5.1. *Set $Z_{\mathfrak{b}} = (\mathbb{Z}_{K_z}/\mathfrak{b})^*$. Then*

$$|S_{\mathfrak{b}}(K_z)[T]| = \frac{|(U(K_z)/U(K_z)^{\ell})[T]||(\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^{\ell})[T]|}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|}\ ,$$

and in particular

$$|S_{\ell}(K_z)[T]| = |(U(K_z)/U(K_z)^{\ell})[T]||(\mathrm{Cl}(K_z)/\mathrm{Cl}(K_z)^{\ell})[T]|\ .$$

Proof. This is a minor variant of Corollary 2.13 of [11], proved in the same way. ☐

The quantity $|(U(K_z)/U(K_z)^{\ell})[T]|$ is given by the following lemma.

Lemma 5.2. *For any number field M, write $\mathrm{rk}_{\ell}(U(M)) := \dim_{\mathbb{F}_{\ell}}(U(M)/U(M)^{\ell})$, and denote by $r_1(M)$ and $r_2(M)$ the number of real and pairs of complex embeddings of M.*

(1) For any number field M we have

$$\mathrm{rk}_{\ell}(U(M)) = \begin{cases} r_1(M) + r_2(M) - 1 & \text{if } \zeta_{\ell} \notin M, \\ r_1(M) + r_2(M) & \text{if } \zeta_{\ell} \in M. \end{cases}$$

(2) We have $|(U(K_z)/U(K_z)^{\ell})[T]| = \ell^{RU(K)}$, where

$$RU(K) := \begin{cases} r_2(K) - r_2(k) & \text{in the general case,} \\ r_1(k) + r_2(k) & \text{in the special case with } \ell \equiv 3 \pmod 4\ , \\ r_2(k) & \text{in the special case with } \ell \equiv 1 \pmod 4\ . \end{cases}$$

(3) In particular, if $k = \mathbb{Q}$ we have $RU(K) = r_2(K)$ in all cases.

Proof. (1) is Dirichlet's theorem, and (3) is a consequence of (2). To prove (2) in the general case, where $T = \{\tau_2 + 1, \tau - g\}$, we apply the exact sequence

$$1 \longrightarrow \frac{U(k_z)}{U(k_z)^{\ell}}[\tau - g] \longrightarrow \frac{U(K_z)}{U(K_z)^{\ell}}[\tau - g] \longrightarrow \frac{U(K_z)}{U(K_z)^{\ell}}[\tau_2 + 1, \tau - g] \longrightarrow 1\ , \tag{5.1}$$

where the last nontrivial map sends ε to $\tau_2(\varepsilon)/\varepsilon$. Surjectivity follows from Lemma 2.3, and $(\tau_2+1)(\tau_2-1) = 0$ implies that the two nontrivial maps compose to zero. Finally, suppose $\varepsilon \in U(K_z)$ satisfies $\tau_2(\varepsilon) = \varepsilon\eta^{\ell}$ for some $\eta \in K_z$. Applying τ_2 to both sides we see that $\eta\tau_2(\eta) = \zeta_{\ell}^a$ for some a, and replacing η with $\eta_1 = \eta\zeta_{\ell}^b$ with $a + 2b \equiv 0 \pmod{\ell}$, we obtain $\eta_1\tau_2(\eta_1) = 1$ and $\tau_2(\varepsilon) = \varepsilon\eta_1^{\ell}$. By Hilbert 90 there exists η_2 with $\eta_1 = \eta_2/\tau_2(\eta_2)$, so that $\varepsilon_1 = \varepsilon\eta_2^{\ell}$ satisfies $\tau_2(\varepsilon_1) = \varepsilon_1$, in other words $\varepsilon_1 \in k_z$, proving exactness of (5.1).

By a nontrivial theorem of Herbrand (see Theorem 2.3 of [11]), we have $|(U(K_z)/U(K_z)^{\ell})[\tau - g]| = \ell^{r_2(K)+1}$ and $|(U(k_z)/U(k_z)^{\ell})[\tau - g]| = \ell^{r_2(k)+1}$, establishing (2) in the general case.

In the special case, with $T = \{\tau + g\} = \{\tau - g^{(\ell+1)/2}\}$, (2) follows directly from Herbrand's theorem applied to the extension $k_z/k = K_z/k$, for which τ generates the Galois group. ☐

Note that the formula given in Lemma 5.4 of [12] is different: here we have made the simplifying assumption that $[K_z : K] = [k_z : k] = \ell - 1$ or $K \subset k_z$, and it is immediate to check that the formulas of loc. cit. give the ones given above.

Finally, we need to compute $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|$.

Lemma 5.3. *Let $\mathfrak{b}\in\mathcal{B}$ satisfy $\mathfrak{b}_z \mid (1-\zeta_\ell)^\ell$, and define $\mathfrak{c}_z=\prod_{\substack{\mathfrak{p}_z\subset K_z\\ \mathfrak{p}_z\mid\mathfrak{b}_z}}\mathfrak{p}_z^{\lceil v_{\mathfrak{p}_z}(\mathfrak{b}_z)/\ell\rceil}$. We have*

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]|=|(\mathfrak{c}_z/\mathfrak{b}_z)[T]|\;,$$

the latter being considered as an additive group.

Proof. See Proposition 2.6 and Theorem 2.7 of [11], or Lemma 1.5.6 of [28]. $\square$

Theorem 5.4. *In the general case, we have*

$$|(\mathfrak{c}_z/\mathfrak{b}_z)[\tau-g]|=\prod_{\mathfrak{p}\mid\mathfrak{b}_z}\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})^{x(\mathfrak{p})}\;,$$

where

$$x(\mathfrak{p})=\lceil v_{\mathfrak{p}}(\mathfrak{b})\rceil-\left\lceil\frac{v_{\mathfrak{p}}(\mathfrak{b})-r_0(e(\mathfrak{p}))}{\ell}\right\rceil\;, \tag{5.2}$$

where $r_0(e)$ is the remainder of e modulo $\ell-1$ with $0\le r_0(e)\le\ell-2$.

In the special case, we have, for any j with $0\le j<\ell-1$,

$$|(\mathfrak{c}_z/\mathfrak{b}_z)[\tau-g^j]|=\prod_{p\mid\mathfrak{b}_z}\mathcal{N}_{k/\mathbb{Q}}(p)^{x(p)}\;,$$

where

$$x(p)=\left\lceil v_p(\mathfrak{b})-\frac{je(p)}{\ell-1}\right\rceil-\left\lceil\frac{\lceil e(\mathfrak{p}_z/p)v_p(\mathfrak{b})/\ell\rceil-\frac{je(p)}{(\ell-1,e(p))}}{e(\mathfrak{p}_z/p)}\right\rceil\;. \tag{5.3}$$

Proof. This is essentially Theorem 2.7 of [11]. The equation (5.2) is Corollary 2.8 of [11], and (5.3) is the third displayed equation of p. 178 of [11], occurring in the proof. As mentioned in Remark 4.5, we require the result of Theorem 2.7 for $\mathfrak{b}_z$ which do not satisfy the hypotheses given there, and so we check that the condition $v_{\mathfrak{p}_z}(\mathfrak{p})|v_{\mathfrak{p}_z}(\mathfrak{b}_z)$ described in [11] is not required of $\mathfrak{b}_z$, except in the simplification subsequent to (5.3).

Indeed, a careful reading of [11] demonstrates that the equation (5.3) is valid under the following hypotheses: $K_z=k(\zeta_\ell)/k$ is an extension of degree $\ell-1$, where τ and g are as described earlier; p is a prime of k above ℓ and $\mathfrak{p}_z$ is a prime of K above p; and $\mathfrak{b}_z$ is a τ-invariant integral ideal of K_z dividing $(1-\zeta_\ell)^\ell$. $\square$

It may be possible to simplify (5.3) in general, but it is not obvious how, and in any case the equation is quite suitable for computing $(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]$ in particular examples.

In the special case, this theorem together with Lemma 5.3 gives the cardinality of $(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]$ by choosing $j=(\ell+1)/2$. In the general case we require the following additional lemma:

Lemma 5.5. *Assume that we are in the general case and set $\mathfrak{c}_k=\mathfrak{c}_z\cap k_z$ and $\mathfrak{b}_k=\mathfrak{b}_z\cap k_z$. We have*

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]|=|(\mathfrak{c}_z/\mathfrak{b}_z)[\tau-g]|/|(\mathfrak{c}_k/\mathfrak{b}_k)[\tau-g]|\;,$$

where the two terms on the right-hand side are given by (5.2) *and* (5.3) *respectively.*

Proof. We have an exact sequence of $\mathbb{F}_\ell[G]$-modules

$$1\longrightarrow\frac{\mathfrak{c}_z}{\mathfrak{b}_z}[\tau_2-1][\tau-g]\longrightarrow\frac{\mathfrak{c}_z}{\mathfrak{b}_z}[\tau-g]\longrightarrow\frac{\mathfrak{c}_z}{\mathfrak{b}_z}[T]\longrightarrow 1\;,$$

the last map sending x to $x-\tau_2(x)$. It therefore suffices to argue that $(\mathfrak{c}_z/\mathfrak{b}_z)[\tau_2-1]=(\mathfrak{c}_z\cap k_z)/(\mathfrak{b}_z\cap k_z)$: if $x\in\mathfrak{c}_z$ satisfies $\tau_2(x)=x+y$ for some $y\in\mathfrak{b}_z$, then applying τ_2 we see that $\tau_2(y)=-y$, hence $\tau_2(x+y/2)=x+y/2$. Moreover $x+y/2\equiv x\pmod{\mathfrak{b}_z}$, because 2 is invertible modulo ℓ hence modulo $\mathfrak{b}$. $\square$

Definition 5.6. *We set* $G_{\mathfrak{b}} = (\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell)[T]$.

Lemma 5.7. *In the general case set* $u = \iota(\tau_2+1)\iota(\tau-g)$ *and in the special case set* $u = \iota(\tau+g)$.

(1) *The map* $I \mapsto u(I)$ *induces a surjective map from* $\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$ *to* $G_{\mathfrak{b}}$, *of which a section is the natural inclusion from* $G_{\mathfrak{b}}$ *to* $\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$.

(2) *Any character* $\chi \in \widehat{G_{\mathfrak{b}}}$ *can be naturally extended to a character of* $\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$ *by setting* $\chi(\overline{I}) = \chi(\overline{u(I)})$, *which we again denote by* χ *by abuse of notation.*

(3) *Let as usual* $\mathfrak{a} = \prod_{0\le i\le \ell-2} \mathfrak{a}_i^{g^i}$ *with the* $(\mathfrak{a}_i)$ *satifying condition (a) of Proposition 2.8.*
- *In the general case and in the special case when* $\ell \equiv 1 \pmod 4$, *we have* $\chi(\overline{\mathfrak{a}}) = \chi(\overline{\mathfrak{a}_0})^{-1}$;
- *In the special case when* $\ell \equiv 3 \pmod 4$, *we have* $\chi(\overline{\mathfrak{a}}) = \chi(\overline{\mathfrak{a}_0\mathfrak{a}_1^g})^{(\ell-1)/2}$,

where χ *on the right-hand side is defined in (2).*

Proof. (1) and (2) are immediate from Lemma 2.3. For (3), assume that we are in the special case. Using Lemma 2.10 we have $\mathfrak{a}_{2i} = \tau^{-2i}(\mathfrak{a}_0)$, $\mathfrak{a}_{2i+1} = \tau^{-2i}(\mathfrak{a}_1)$, and $\chi(\overline{\tau^2(I)}) = \chi(\overline{I})^{g^2}$, so that

$$\chi(\overline{\mathfrak{a}}) = \prod_{0\le i<(\ell-1)/2} \chi(\overline{\tau^{-2i}(\mathfrak{a}_0\mathfrak{a}_1^g)})^{g^2 i} = \prod_{0\le i<(\ell-1)/2} \chi(\overline{\mathfrak{a}_0\mathfrak{a}_1^g}) = \chi(\overline{\mathfrak{a}_0\mathfrak{a}_1^g})^{(\ell-1)/2}\ .$$

If in addition $\ell \equiv 1 \pmod 4$ we have $\mathfrak{a}_1 = \tau^{(\ell-3)/2}(\mathfrak{a}_0)$ and $\chi(\tau(I)) = \chi(I^{-g})$, giving $\chi(\mathfrak{a}_1) = \chi(\mathfrak{a}_0)^{(-g)^{(\ell-3)/2}} = \chi(\mathfrak{a}_0)^{-g^{(\ell-3)/2}}$ and $\chi(\mathfrak{a}_1^g) = \chi(\mathfrak{a}_0)$, so $\chi(\overline{\mathfrak{a}_0\mathfrak{a}_1^g})^{(\ell-1)/2} = \chi(\overline{\mathfrak{a}_0})^{\ell-1} = \chi(\overline{\mathfrak{a}_0})^{-1}$.

The general case of (3) is proved similarly, with $\mathfrak{a}_i = \tau^{-i}(\mathfrak{a}_0)$. □

6. Semi-Final Form of the Dirichlet Series

We can now put everything together, and obtain a complete analogue of the main theorem of [12]:

Theorem 6.1. *Recall that for any (true or formal) ideal* $\mathfrak{b}$ *of* K *as above we set* $G_{\mathfrak{b}} = (\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell)[T]$. *We have*

$$\Phi_\ell(K,s) = \frac{\ell^{RU(K)}}{(\ell-1)\ell^{\frac{\ell}{\ell-1}[k:\mathbb{Q}]s}} \prod_{\mathfrak{p}\mid\ell} \mathcal{N}(\mathfrak{p})^{-\frac{(\ell-1-r(e(\mathfrak{p}))}{\ell-1}s}\ .$$
$$\cdot \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})\mid\mathfrak{d}_\ell}} \left(\frac{\lceil\mathcal{N}\rceil(\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))}\right)^s \frac{P(\mathfrak{b},s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]|} \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} F(\mathfrak{b},\chi,s)\ ,$$

where

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

and $\mathcal{D}'(\chi)$ *(resp.* $\mathcal{D}'_\ell(\chi)$*) is the set of* $p\in\mathcal{D}$ *(resp.* $\mathcal{D}_\ell$*) such that* $\chi(\mathfrak{p}_z) = 1$, *where* $\mathfrak{p}_z$ *is any prime ideal of* K_z *above* p.

Proof. We begin with the formula for $\Phi_\ell(K,s)$ given by (4.1) and (4.4). By Remark 2.9 we have $\overline{\mathfrak{a}} \in (\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell)[T]$ with $\mathfrak{a} = \prod_{0\le i\le\ell-2}\mathfrak{a}_i^{g^i}$. Thus $\overline{\mathfrak{a}} \in \mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$ if and only if $\chi(\overline{\mathfrak{a}}) = 1$ for all characters $\chi \in \widehat{G_{\mathfrak{b}}}$. The number of such characters being equal to $|G_{\mathfrak{b}}|$, by orthogonality of characters and Lemmas 5.1 and 5.2 we obtain

$$\Phi_\ell(K,s) = \frac{\ell^{RU(K)}}{(\ell-1)\ell^{\frac{\ell}{\ell-1}[k:\mathbb{Q}]s}} \prod_{\mathfrak{p}\mid\ell} \mathcal{N}(\mathfrak{p})^{-\frac{\ell-1-r(e(\mathfrak{p}))}{\ell-1}s} \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})\mid\mathfrak{d}_\ell}} \frac{\lceil\mathcal{N}\rceil(\mathfrak{b})^s P(\mathfrak{b},s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]|} \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} H(\mathfrak{b},\chi,s)\ ,$$

with

$$H(\mathfrak{b},\chi,s)=\sum_{\substack{(\mathfrak{a}_0,\cdots,\mathfrak{a}_{\ell-2})\in J'\\(\mathfrak{a}_\alpha,\ell\mathbb{Z}_K)=\mathfrak{r}^e(\mathfrak{b})}}\frac{\chi(\overline{\mathfrak{a}})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,$$

where $\mathfrak{a}_\alpha$ was defined in Proposition 2.19, and J' is the set of $(\ell-1)$uples of coprime squarefree ideals of K_z, satisfying condition (a) of Proposition 2.8, but now without the condition that the ideal class of $\mathfrak{a}$ belongs to $\mathrm{Cl}(K_z)^\ell$, so satisfying the condition of Lemma 2.10.

Assume first that we are in the general case. By Lemma 2.10 we can replace the sum over J' by a sum over ideals $\mathfrak{a}_0$ of K_z. The conditions and quantities linked to $\mathfrak{a}_0$ are then as follows:

(a) The ideal $\mathfrak{a}_0$ is a squarefree ideal of K_z such that $\tau^{(\ell-1)/2}(\mathfrak{a}_0)=\tau_2(\mathfrak{a}_0)$.
(b) The ideals $\mathfrak{a}_0$ and $\tau^i(\mathfrak{a}_0)$ are coprime for $(\ell-1)\nmid i$.
(c) If $\mathfrak{p}_z$, is a prime ideal of K_z dividing $\mathfrak{a}_0$, $\mathfrak{p}$ the prime ideal of K below $\mathfrak{p}_z$, and p the prime ideal of k below $\mathfrak{p}_z$ then by Corollary 2.11 we have $p\in\mathcal{D}\cup\mathcal{D}_\ell$. Conversely, if this is satisfied then the ideals $\mathfrak{a}_i=\tau^{-i}(\mathfrak{a}_0)$ must be pairwise coprime since otherwise $\mathfrak{a}_\alpha$ would be divisible by some $\mathfrak{p}_z^2$ which is impossible since $\mathfrak{p}$ is unramified in K_z/K.
(d) We have $\mathcal{N}_{K_z/K}(\mathfrak{a}_0)=\mathfrak{a}_\alpha$.
(e) By Lemma 5.7 we have $\chi(\overline{\mathfrak{a}})=\chi^{-1}(\overline{\mathfrak{a}_0})$.

Thus if we denote temporarily by J'' the set of ideals $\mathfrak{a}_0$ of K_z satisfying the first three conditions above, we have

$$H(\mathfrak{b},\chi,s)=\sum_{\substack{\mathfrak{a}_0\in J''\\(\mathcal{N}_{K_z/K}(\mathfrak{a}_0),\ell\mathbb{Z}_K)=\mathfrak{r}^e(\mathfrak{b})}}\frac{\chi^{-1}(\overline{\mathfrak{a}_0})}{\mathcal{N}(\mathcal{N}_{K_z/K}(\mathfrak{a}_0))^s}\ .$$

So that we can use multiplicativity, write $\mathfrak{a}_0=\mathfrak{c}\mathfrak{d}$, where $\mathfrak{c}$ is the ℓ-part of $\mathfrak{a}_0$ and $\mathfrak{d}$ is the prime to ℓ part (recall that $\mathfrak{a}_0$ is squarefree). The condition $(\mathcal{N}_{K_z/K}(\mathfrak{a}_0),\ell\mathbb{Z}_K)=\mathfrak{r}^e(\mathfrak{b})$ is thus equivalent to $\mathcal{N}_{K_z/K}(\mathfrak{c})=\mathfrak{r}^e(\mathfrak{b})$. Thus $H(\mathfrak{b},\chi,s)=S_cS_d$ with

$$S_c=\sum_{\substack{\mathfrak{c}\in J''\\\mathcal{N}_{K_z/K}(\mathfrak{c})=\mathfrak{r}^e(\mathfrak{b})}}\frac{\chi^{-1}(\overline{\mathfrak{c}})}{\mathcal{N}(\mathcal{N}_{K_z/K}(\mathfrak{c}))^s}\quad\text{and}\quad S_d=\sum_{\substack{\mathfrak{d}\in J''\\(\mathcal{N}_{K_z/K}(\mathfrak{d}),\ell\mathbb{Z}_K)=1}}\frac{\chi^{-1}(\overline{\mathfrak{d}})}{\mathcal{N}(\mathcal{N}_{K_z/K}(\mathfrak{d}))^s}\ .$$

Consider first the sum S_d. By multiplicativity we have $S_d=\prod_{p\in\mathcal{D}}S_{d,p}$ with

$$S_{d,p}=\sum_{\substack{\mathfrak{d}\mid p\mathbb{Z}_{K_z}\\\tau^{(\ell-1)/2}(\mathfrak{d})=\tau_2(\mathfrak{d})}}\frac{\chi^{-1}(\overline{\mathfrak{d}})}{\mathcal{N}(\mathcal{N}_{K_z/K}(\mathfrak{d}))^s}\ .$$

We consider three cases.

(1) Assume that $p\mathbb{Z}_K=\mathfrak{p}$, i.e, that p is inert in K/k. Since $\mathfrak{p}$ is totally split in K_z/K we have $\mathfrak{p}\mathbb{Z}_{K_z}=\prod_{0\le i\le\ell-2}\tau^i(\mathfrak{p}_z)$ for some prime ideal $\mathfrak{p}_z$ of K_z. Furthermore, since $\mathfrak{p}_z/\mathfrak{p}_k$ (with our usual notation) is split we have $\tau_2(\mathfrak{p}_z)\neq\mathfrak{p}_z$, and since $\mathfrak{p}$ is stable by τ_2, $\tau_2(\mathfrak{p}_z)$ is again above $\mathfrak{p}$, so $\tau_2(\mathfrak{p}_z)=\tau^j(\mathfrak{p}_z)$ for some $j\not\equiv 0\pmod{\ell-1}$. Applying τ_2 once again we obtain $\mathfrak{p}_z=\tau^{2j}(\mathfrak{p}_z)$, and since $\mathfrak{p}$ is totally split this means that $2j\equiv 0\pmod{\ell-1}$, hence that $j\equiv(\ell-1)/2\pmod{\ell-1}$ since $j\not\equiv 0\pmod{\ell-1}$. We deduce that $\tau^{(\ell-1)/2}(\mathfrak{p}_z)=\tau_2(\mathfrak{p}_z)$.

Now we must have $\mathfrak{d}=\prod_i\tau^i(\mathfrak{p}_z)^{\varepsilon_i}$ with $\varepsilon_i=0$ or 1, but since $\mathfrak{d}$ is coprime to $\tau^i(\mathfrak{d})$ for $i\not\equiv 0\pmod{\ell-1}$ this means that at most one ε_i is nonzero. In other words $\mathfrak{d}=\mathbb{Z}_{K_z}$ or $\mathfrak{d}=\tau^i(\mathfrak{p}_z)$ for some i. Now note that $\mathcal{N}_{K_z/K}(\mathfrak{p}_z)=\mathfrak{p}$, hence $\mathcal{N}(\mathcal{N}_{K_z/K}(\mathfrak{p}_z))=\mathcal{N}(p)^s$ (with our definition of $\mathcal{N}$).

Furthermore, we have $\chi(\tau^i(\mathfrak{p}_z))=\chi(\mathfrak{p}_z)^{g^i}$. Thus

$$S_{d,p}=1+\sum_{0\le i\le \ell-2}\frac{\chi(\mathfrak{p}_z)^{-g^i}}{\mathcal{N}(p)^s}=1+\sum_{1\le j\le \ell-1}\frac{\chi(\mathfrak{p}_z)^j}{\mathcal{N}(p)^s}\ , \tag{6.1}$$

so that $S_{d,p}=1+(\ell-1)/\mathcal{N}(p)^s$ if $\chi(\mathfrak{p}_z)=1$, and $S_{d,p}=1-1/\mathcal{N}(p)^s$ otherwise.

(2) Assume that $p\mathbb{Z}_K=\mathfrak{p}\tau_2(\mathfrak{p})$, i.e., that p is split in K/k. If $\mathfrak{p}_z$ is a prime ideal above $\mathfrak{p}$ then $\tau_2(\mathfrak{p}_z)$ is above $\tau_2(\mathfrak{p})$. Thus if we set

$$\mathfrak{d}=\prod_i \tau^i(\mathfrak{p}_z)^{\varepsilon_i}\prod_i \tau_2(\tau^i(\mathfrak{p}_z))^{\varepsilon'_i}\ ,$$

the fact that $\mathfrak{d}$ is coprime to $\tau^i(\mathfrak{d})$ for $(\ell-1)\nmid i$ implies that at most one of the ε_i and one of the ε'_i is nonzero, and since $\tau^{(\ell-1)/2}(\mathfrak{d})=\tau_2(\mathfrak{d})$ this means that the only possibilities are $\mathfrak{d}=\mathbb{Z}_{K_z}$ and $\mathfrak{d}=\tau^i((\mathfrak{p}_z)\tau^{(\ell-1)/2}(\tau_2(\mathfrak{p}_z)))$. Since

$$\chi(\tau^{(\ell-1)/2}(\tau_2(\mathfrak{p}_z)))=\chi^{-1}(\tau_2(\mathfrak{p}_z))=\chi(\mathfrak{p}_z)\ ,$$

and since when $\mathfrak{d}\ne\mathbb{Z}_{K_z}$ we have $\mathcal{N}(\mathcal{N}_{K_z/K}(\mathfrak{d}))=\mathcal{N}(p)$, we obtain the same result as above.

(3) Finally note that since p is not above ℓ the case where p is ramified in K/k is excluded by Proposition 2.15.

Consider now the sum S_c. By multiplicativity, since $\mathfrak{b}$ is stable by τ_2, and applying Lemma 4.8 we have

$$S_c=\frac{1}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s}\sum_{\substack{\mathfrak{c}\in J''\\ \mathcal{N}_{K_z/K}(\mathfrak{c})=\mathfrak{r}^e(\mathfrak{b})}}\chi^{-1}(\bar{\mathfrak{c}})=\frac{1}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))^s}\prod_{\substack{p\in\mathcal{D}_\ell\\ (p,\mathfrak{b})=1}}S_{c,p}\ ,$$

with

$$S_{c,p}=\sum_{\substack{\mathfrak{c}\mid p\mathbb{Z}_{K_z}\\ \tau^{(\ell-1)/2}(\mathfrak{c})=\tau_2(\mathfrak{c})\\ \mathcal{N}_{K_z/K}(\mathfrak{c})=\prod_{\mathfrak{p}\mid p}\mathfrak{p}}}\chi^{-1}(\bar{\mathfrak{c}})\ .$$

As above we consider three cases.

(1) Assume that $p\mathbb{Z}_K=\mathfrak{p}$. As before, the condition $\tau^{(\ell-1)/2}(\mathfrak{p}_z)=\tau_2(\mathfrak{p}_z)$ is automatically satisfied, and we must have $\mathfrak{c}=\mathbb{Z}_{K_z}$ or $\mathfrak{c}=\tau^i(\mathfrak{p}_z)$. The additional condition $\mathcal{N}_{K_z/K}(\mathfrak{c})=\prod_{\mathfrak{p}\mid p}\mathfrak{p}=\mathfrak{p}$ is satisfied if and only if $\mathfrak{c}=\tau^i(\mathfrak{p}_z)$, hence as above $S_{c,p}=\ell-1$ if $\chi(\mathfrak{p}_z)=1$ and -1 otherwise.

(2) Assume that $p\mathbb{Z}_K=\mathfrak{p}\tau_2(\mathfrak{p})$. Then once again $\mathfrak{c}=\mathbb{Z}_{K_z}$ is excluded and the only possibilities are $\mathfrak{c}=\tau^i((\mathfrak{p}_z)\tau^{(\ell-1)/2}(\tau_2(\mathfrak{p}_z)))$ and we obtain the same result as in (1).

(3) Assume that $p\mathbb{Z}_K=\mathfrak{p}^2$, i.e., that p is ramified in K/k, case which could not occur when p is not above ℓ. Once again since $\tau_2(\mathfrak{p})=\mathfrak{p}$ we have $\tau^{(\ell-1)/2}(\mathfrak{p}_z)=\tau_2(\mathfrak{p}_z)$, hence we have $\mathfrak{c}=\tau^i(\mathfrak{p}_z)$, and we again obtain the same result as in (1) and (2).

Putting everything together proves the theorem in the general case.

In the special case with $\ell\equiv 1\pmod 4$**,** a similar proof applies. The definition of $H(\mathfrak{b},\chi,s)$ is the same, and we replace the sum over J' by a sum over ideals $\mathfrak{a}_0$ of K_z satisfying similar conditions to those above, except:

- Condition (a) is absent. The replacement condition $\mathfrak{a}_1=\tau^{(\ell-3)/2}(\mathfrak{a}_0)$ is formally similar, but it will only be relevant insofar as it shows that τ acts transitively on the $\mathfrak{a}_i$.
- In place of (d), we have $\mathcal{N}_{K_z/k}(\mathfrak{a}_0)=\mathcal{N}(\mathfrak{a}_\alpha)$.

We evaluate S_d by imitating case (1) above with K_z/k in place of K_z/K (note that p is totally split in K_z/k), and we obtain the same results. In evaluating S_c, the condition $\mathcal{N}_{K_z/k}(\mathfrak{c})=p$ appears in place of $\mathcal{N}_{K_z/K}(\mathfrak{c})=\prod_{\mathfrak{p}\mid p}\mathfrak{p}$ in the definition of $S_{c,p}$, and again we check that we obtain the same results.

In the special case with $\ell\equiv 3 \pmod 4$, we replace the sum over J' by a sum over pairs $(\mathfrak{a}_0,\mathfrak{a}_1)$ of ideals of K_z satisfying suitable conditions:

- In place of (a), $\mathfrak{a}_0$ and $\mathfrak{a}_1$ are fixed by $\tau^{(\ell-1)/2}$.
- In place of (b), the ideals $\mathfrak{a}_0$, $\mathfrak{a}_1$, $\tau^{2i}(\mathfrak{a}_0)$, and $\tau^{2i}(\mathfrak{a}_1)$ must all be coprime.
- In place of (d), we have $\mathcal{N}_{K_z/K}(\mathfrak{a}_0\mathfrak{a}_1)=\mathcal{N}(\mathfrak{a}_\alpha)$.
- In place of (e), we have $\chi(\overline{\mathfrak{a}})=\chi(\overline{\mathfrak{a}_0\mathfrak{a}_1^g})^{(\ell-1)/2}$.

We must again consider all splitting types in K/k, and the arguments are similar. If p is inert, we compute that

$$S_{d,p}=1+\sum_{0\le i\le\frac{\ell-3}{2}}\frac{\chi(\mathfrak{p}_z)^{-g^{2i}\cdot(\ell-1)/2}}{\mathcal{N}(p)^s}+\sum_{0\le i\le\frac{\ell-3}{2}}\frac{\chi(\mathfrak{p}_z)^{-g^{2i+1}\cdot(\ell-1)/2}}{\mathcal{N}(p)^s},$$

equal to the same expression as before. If p is split, the relevant computation is

$$\chi(\mathfrak{p}_z\tau^{(\ell-1)/2}(\mathfrak{p}_z))^{(\ell-1)/2}=\chi(\mathfrak{p}_z^{1-g^{(\ell-1)/2}})^{(\ell-1)/2}=\chi(\mathfrak{p}_z)^{-1},$$

and again we obtain the same results. For $p\in\mathcal{D}_\ell$ the argument is similar, once again considering all three cases and obtaining the same result. $\square$

As mentioned in Remarks 3.11, if $\ell>2[k:\mathbb{Q}]+1$, and in particular if $k=\mathbb{Q}$ and $\ell\ge 5$, we always have $\mathfrak{r}^e(\mathfrak{b})=(1)$. The theorem simplifies and gives the following:

Corollary 6.2. *Keep the same notation, and assume that $\ell\ge 2[k:\mathbb{Q}]+3$, for instance that $k=\mathbb{Q}$ and $\ell\ge 5$. We have*

$$\Phi_\ell(K,s)=\frac{\ell^{RU(K)}}{(\ell-1)\ell^{\frac{\ell}{\ell-1}[k:\mathbb{Q}]s}}\prod_{\mathfrak{p}\mid\ell}\mathcal{N}(\mathfrak{p})^{-\frac{\ell-1-r(e(\mathfrak{p}))}{\ell-1}s}\sum_{\mathfrak{b}\in\mathcal{B}}\frac{\lceil\mathcal{N}\rceil(\mathfrak{b})^sP(\mathfrak{b},s)}{|(Z_\mathfrak{b}/Z_\mathfrak{b}^\ell)[T]|}\sum_{\chi\in\widehat{G_\mathfrak{b}}}F(\mathfrak{b},\chi,s)\ ,$$

where

$$F(\mathfrak{b},\chi,s)=\prod_{p\in\mathcal{D}'(\chi)}\left(1+\frac{\ell-1}{\mathcal{N}(p)^s}\right)\prod_{p\in\mathcal{D}\setminus\mathcal{D}'(\chi)}\left(1-\frac{1}{\mathcal{N}(p)^s}\right)\ .$$

In the general case, we now prove that the group $G_\mathfrak{b}$ can be described in somewhat simpler terms, in terms of the mirror field K' of K.

Proposition 6.3. *There is a natural isomorphism*

$$\frac{\mathrm{Cl}_\mathfrak{b}(K_z)}{\mathrm{Cl}_\mathfrak{b}(K_z)^\ell}[T]\to\frac{\mathrm{Cl}_{\mathfrak{b}'}(K')}{\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell}[\tau-g],$$

where $\mathfrak{b}'=\mathfrak{b}\cap K'$.

Moreover, using this isomorphism to regard a character χ of $\frac{\mathrm{Cl}_\mathfrak{b}(K_z)}{\mathrm{Cl}_\mathfrak{b}(K_z)^\ell}[T]$ as a character $\widetilde{\chi}$ of $\frac{\mathrm{Cl}_{\mathfrak{b}'}(K')}{\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell}[\tau-g]$, the condition $\chi(\mathfrak{p}_z)=1$ defining $\mathcal{D}(\chi)\cap\mathcal{D}'_\ell(\chi)$ is equivalent to the condition $\widetilde{\chi}(\mathfrak{p}_{K'})=1$ for the unique prime $\mathfrak{p}_{K'}$ of K' below $\mathfrak{p}_z$.

Proof. The first statement is also proved in [13], so we will be brief. As $\tau^{(\ell-1)/2}\tau_2$ acts trivially on $G_\mathfrak{b}$, it can be checked that elements of $G_\mathfrak{b}$ can be represented by an ideal of the form $\mathfrak{a}\tau_2\tau^{(\ell-1)/2}\mathfrak{a}$, which is of the form $\mathfrak{a}'\mathbb{Z}_{K_z}$ for some ideal $\mathfrak{a}'$ of K'. We therefore obtain a well-defined injective map $\frac{\mathrm{Cl}_\mathfrak{b}(K_z)}{\mathrm{Cl}_\mathfrak{b}(K_z)^\ell}[T]\to\frac{\mathrm{Cl}_{\mathfrak{b}'}(K')}{\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell}[\tau-g]$, which may easily be shown to be surjective as well.

The latter statement follows because the condition $\widetilde{\chi}(\mathfrak{p}_{K'})=1$ is equivalent to $\chi(\mathfrak{p}_{K'}\mathbb{Z}_{K_z})=1$, which is easily seen to be equivalent to $\chi(\mathfrak{p}_z)=1$ for any splitting type of $\mathfrak{p}_z|\mathfrak{p}_{K'}$. $\square$

7. Specialization to $k=\mathbb{Q}$

We now specialize all of the results of this paper to the case where the base field is $k=\mathbb{Q}$, where we will obtain more explicit results. Henceforth we assume that $K=\mathbb{Q}(\sqrt{D})$ is a quadratic field with discriminant D.

By definition, $\mathcal{B}=\{1,(\ell),(\ell)^{\ell/(\ell-1)}\}$ in the general case with $\ell\nmid D$, and $\mathcal{B}=\{1,(\ell)^{1/2},(\ell),(\ell)^{\ell/(\ell-1)}\}$ in the special case or in the general case with $\ell\mid D$. Note that we can also write the latter as

$$\mathfrak{b}_z\in\left\{\mathbb{Z}_{K_z},\ (1-\zeta_\ell)^{(\ell-1)/2}\mathbb{Z}_{K_z},\ (1-\zeta_\ell)^{\ell-1}\mathbb{Z}_{K_z}=\ell\mathbb{Z}_{K_z},(1-\zeta_\ell)^{\ell}\mathbb{Z}_{K_z}\right\}. \tag{7.1}$$

Throughout, we use the notation $(-,-,-,-)$ to describe quantities depending on $\mathcal{B}$, with asterisks denoting 'not applicable'.

Proposition 7.1. *We have that $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|$ is equal to $(1,*,\ell,\ell)$ or $(1,1,\ell,\ell)$ for $\ell\nmid D$ or $\ell|D$ respectively, unless $\ell=3$ in the special case, in which case $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{3})[T]|=(1,1,1,3)$.*

Proof. This follows from Lemma 5.5, (5.2), and (5.3). In the general case we obtain

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|=\Big((0,*,2,4)-(0,*,0,2)\Big)-\Big((0,*,1,1)-(0,*,0,0)\Big)=(0,*,1,1)\ ,$$

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|=\Big((0,1,2,3)-(0,0,0,1)\Big)-\Big((0,1,1,1)-(0,0,0,0)\Big)=(0,0,1,1)\ ,$$

depending on whether $\ell\nmid D$ or $\ell|D$ respectively; in the special case we obtain

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|=(0,0,1,1)-(0,0,0,0)=(0,0,1,1)\ ,$$

$$|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|=(-1,0,0,1)-(-1,0,0,0)=(0,0,0,1)\ ,$$

depending on whether $\ell\geq 5$ or $\ell=3$ respectively. $\square$

Recall that the mirror field of $K=\mathbb{Q}(\sqrt{D})$ with respect to ℓ is the degree $\ell-1$ field $K'=\mathbb{Q}(\sqrt{D}(\zeta_\ell-\zeta_\ell^{-1}))$. The following is immediate from the results of Section 2:

Lemma 7.2. *Let p be a prime different from ℓ.*

- *We have $p\in\mathcal{D}$ if and only if $p\equiv\left(\frac{D}{p}\right)\equiv\pm1\pmod{\ell}$, in other words $p\neq\ell$ and $p\equiv\left(\frac{D}{p}\right)\pmod{\ell}$.*
- *In the general case, this is equivalent to p splitting completely in $K'/\mathbb{Q}$.*
- *In the special case with $\ell\equiv1\pmod 4$, this is equivalent to $p\equiv1\pmod{\ell}$.*
- *In the special case with $\ell\equiv3\pmod 4$, this is equivalent to $p\equiv\pm1\pmod{\ell}$.*

We come now to the analogue of Theorem 3.2 of [14]. The case $\ell=3$, which is slightly different, is treated in loc. cit.:

Theorem 7.3. *Assume that $\ell\geq5$ and let $K=\mathbb{Q}(\sqrt{D})$. We have*

$$\Phi_\ell(K,s)=\frac{\ell^{r_2(D)}}{\ell-1}\sum_{\mathfrak{b}\in\mathcal{B}}A_{\mathfrak{b}}(s)\sum_{\chi\in\widehat{G_{\mathfrak{b}}}}F(\mathfrak{b},\chi,s)\ ,$$

where the $A_{\mathfrak{b}}(s)$ are given by the following table:

Condition on D	$A_{(1)}(s)$	$A_{(\sqrt{(-1)^{(\ell-1)/2}\ell})}(s)$	$A_{(\ell)}(s)$	$A_{(\ell^{\ell/(\ell-1)})}(s)$
$\ell \nmid D$	ℓ^{-2s}	0	$-\ell^{-2s-1}$	$1/\ell$
$\ell \mid D$	$\ell^{-3s/2}$	$\ell^{-s}-\ell^{-3s/2}$	$-\ell^{-s-1}$	$1/\ell$

$$F(\mathfrak{b},\chi,s)=\prod_{p\equiv\left(\frac{D}{p}\right)\pmod{\ell},\ p\neq\ell}\left(1+\frac{\omega_\chi(p)}{p^s}\right)\,,$$

where we set:

$$\omega_\chi(p)=\begin{cases}\ell-1 & \text{if } \chi(\mathfrak{p}_z)=1\\ -1 & \text{if } \chi(\mathfrak{p}_z)\neq 1\,,\end{cases}$$

where as usual $\mathfrak{p}_z$ is any ideal of K_z above p.

Proof. The computation is routine, given the following consequences of our previous results:

- We have $k=\mathbb{Q}$ so $\ell^{\frac{\ell}{\ell-1}[k:\mathbb{Q}]s}=\ell^{\ell s/(\ell-1)}$.
- The factor $\prod_{\mathfrak{p}\mid\ell}\mathcal{N}(\mathfrak{p})^{\cdots}$ is equal to $\ell^{-(\ell-2)s/(\ell-1))}$ if $\ell\nmid D$ and to $\ell^{-(\ell-3)s/(2(\ell-1))}$ if $\ell\mid D$. Multiplied by the first factor this gives ℓ^{-2s} if $\ell\nmid D$ and $\ell^{-3s/2}$ if $\ell\mid D$.
- We have $\ell^{RU(K)}=\ell^{r_2(D)}$ by Lemma 5.2, with $r_2(D):=r_2(\mathbb{Q}(\sqrt{D}))$.
- By Definitions 4.4 and 4.1, we have $\lceil\mathcal{N}\rceil(\mathfrak{b})=(1,*,\ell,\ell^2)$ and $\lceil\mathcal{N}\rceil(\mathfrak{b})=(1,\ell^{1/2},\ell,\ell^{3/2})$ for $\ell\nmid D$ and $\ell\mid D$ respectively.
- As already mentioned, if $k=\mathbb{Q}$ and $\ell>3$ we have $\mathfrak{r}^e(\mathfrak{b})=(1)$, so the terms and conditions involving $\mathfrak{r}^e(\mathfrak{b})$ disappear (in other words we use Corollary 6.2).
- By Definitions 2.12, Proposition 2.15, and Lemma 7.2, we have $p\in\mathcal{D}$ if and only if $p\equiv\left(\frac{D}{p}\right)\pmod{\ell}$ and $p\neq\ell$, and $\mathcal{D}_\ell=\emptyset$ when $\ell\neq 3$ by what we have just said.
- By Lemma 4.3 and Definition 4.4 of $P(\mathfrak{b},s)$, when $\ell\nmid D$ and $\ell\mid D$ respectively. we have $P(\mathfrak{b},s)=(1,*,-\ell^{-s},1)$, and $P(\mathfrak{b},s)=(1,1-\ell^{-s/2},-\ell^{-s/2},1)$ for $\ell\nmid D$ respectively for the usual sequence of $\mathfrak{b}$.
- The values of $|(Z_\mathfrak{b}/Z_\mathfrak{b}^\ell)[T]|$ are given in Proposition 7.1.

□

Corollary 7.4. *Assume that $\ell\geq 5$, and set $L_\ell(s)=1+(\ell-1)/\ell^{2s}$ if $\ell\nmid D$ and $L_\ell(s)=1+(\ell-1)/\ell^{s}$ if $\ell\mid D$. There exists a function $\phi_D(s)=\phi_{D,\ell}(s)$, holomorphic for $\Re(s)>1/2$, such that*

$$\sum_{L\in\mathcal{F}_\ell(K)}\frac{1}{f(L)^s}=\phi_D(s)+\frac{1}{(\ell-1)\ell^{1-r_2(D)}}L_\ell(s)\prod_{p\equiv\left(\frac{D}{p}\right)\pmod{\ell},\ p\neq\ell}\left(1+\frac{\ell-1}{p^s}\right)\,.$$

Proof. Same as in Proposition 7.5 of [12]: The main term is the contribution of the trivial characters, and $\phi_D(s)$ is the contribution of the nontrivial characters: we first regard each $\chi\in\widehat{G_\mathfrak{b}}$ as a character of $\frac{\mathrm{Cl}_{\mathfrak{b}'}(K')}{\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell}$ by Proposition 6.3 and then by setting χ equal to 1 on the orthogonal complement of $\frac{\mathrm{Cl}_{\mathfrak{b}'}(K')}{\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell}[\tau-g]$. By the previous lemma, the primes occurring in the product are precisely those for which p is totally split in K'. Therefore, for each set of nontrivial characters $\chi,\chi^2,\dots,\chi^{\ell-1}\in\widehat{G_b}$, the sum of products $F(\mathfrak{b},\chi,s)$ may be written as $g(s)+\sum_\chi L(s,\chi)$, where $L(s,\chi)$ is the (holomorphic) Hecke L-function associated to χ, and $g(s)$ is a Dirichlet series supported on squarefull numbers, absolutely convergent and therefore holomorphic in $\Re(s)>1/2$. Therefore $\phi_D(s)$ is holomorphic in $\Re(s)>1/2$ as well. We also note that the product of the main term may similarly be written as $h(s)+L(s,\omega_0)$, where ω_0 is the trivial Hecke character, and $h(s)$ satisfies the same properties as $g(s)$.

The $\ell=3$ case is slightly different due to the nontriviality of $\mathfrak{r}^e(\mathfrak{b})$; see [12]. □

This brings us to our asymptotic formulas:

Corollary 7.5. *Assume that $\ell \geq 5$ and denote by $M_\ell(D;X)$ the number of $L \in \mathcal{F}_\ell(\mathbb{Q}(\sqrt{D}))$ such that $f(L) \leq X$. Set $c_1(\ell) = 1/((\ell-1)\ell^{1-r_2(D)})$, $c_2(\ell) = (\ell^2+\ell-1)/\ell^2$ when $\ell \nmid D$ or $c_2(\ell) = 2 - 1/\ell$ when $\ell \mid D$.*

(1) *In the general case, for any $\varepsilon > 0$ we have*

$$M_\ell(D;X) = C_\ell(D)X + O(X^{1-\frac{2}{\ell+3}+\varepsilon})\ , \text{ with}$$

$$C_\ell(D) = c_1(\ell)c_2(\ell)\mathrm{Res}_{s=1} \prod_{e(p)=f(p)=1} \left(1 + \frac{\ell-1}{p^s}\right)\ ,$$

where $e(p)$ and $f(p)$ are the usual quantities associated to the splitting of p in K'.

(2) *In the special case with $\ell \equiv 1 \pmod 4$, for any $\varepsilon > 0$ we have*

$$M_\ell(D;X) = C_\ell(D)X + O(X^{1-\frac{2}{\ell+3}+\varepsilon})\ , \text{ with}$$

$$C_\ell(D) = c_1(\ell)c_2(\ell)\mathrm{Res}_{s=1} \prod_{p\equiv 1 \pmod{\ell}} \left(1 + \frac{\ell-1}{p^s}\right)\ .$$

(3) *In the special case with $\ell \equiv 3 \pmod 4$, for any $\varepsilon > 0$ we have*

$$M_\ell(D;X) = C_\ell(D)(X\log(X) + C'_\ell(D)) + O(X^{1-\frac{2}{\ell+3}+\varepsilon})\ , \text{ with}$$

$$C_\ell(D) = c_1(\ell)c_2(\ell)\lim_{s\to 1^+}(s-1)^2 \prod_{p\equiv \pm 1 \pmod{\ell}} \left(1 + \frac{\ell-1}{p^s}\right)\ ,$$

and $C'_\ell(D)$ can also be given explicitly if desired.

Proof. In the general case, using the same proof as in [12], we see that the result follows, with $C_\ell(D)$ equal to the residue at $s=1$ of $\Phi_\ell(K,s)$. Note that since we assume that $\ell \geq 5$, the condition $e(p) = f(p) = 1$ implies that $p \neq \ell$, otherwise it must simply be added. Note the marked difference in the asymptotics when $\ell \equiv 1 \pmod 4$ and $\ell \equiv 3 \pmod 4$.

We briefly recall how to obtain the error term. By the proof of Corollary 7.4, it equals (up to an implied constant depending on D and ℓ) the error made in estimating partial sums of Hecke L-functions of degree $\ell - 1$.

We do this in the standard way, subject to the limitation that we may not shift any contour to $\Re(s) \leq 1/2$. We have by Perron's formula, for each Hecke L-function $\xi(s) = \sum_n a(n)n^{-s}$ and any $c > 1$,

$$\sum_{n<X} a(n) = \int_{c-i\infty}^{c+i\infty} \xi(s)\frac{X^s}{s}ds\ ,$$

and we shift the portion of the contour from $c - iT$ to $c + iT$ to $\Re(s) = \sigma$ for $\sigma \in (1/2, 1)$ and $T > 0$ to be determined. By convexity we have $|\xi(s)| \ll T^{\frac{\ell-1}{2}(1-\sigma+\varepsilon)}$, and choosing $c = 1+\varepsilon$, $\sigma = 1/2+\varepsilon$ our integral is $\ll T^{\frac{\ell-1}{2}(\frac{1}{2}+2\varepsilon)}X^{\frac{1}{2}+\varepsilon} + \frac{X^{1+2\varepsilon}}{T}$; then choosing $T = X^{\frac{2}{\ell+3}}$ we obtain an error term of $X^{1-\frac{2}{\ell+3}+\varepsilon}$. ∎

In a separate paper by the first author [9], one explains how to compute the constants $C_\ell(D)$ to high accuracy (100 decimal digits, say) for reasonably small values of $|D|$. For example, we have

$$C_3(-3) = 0.066907733301378371291841 6\cdots\ , \quad C_3(-4) = 0.136219067624121284144986 7\cdots\ .$$

Writing $N^{\pm}_{D_\ell}(X)$ for the number of degree ℓ fields L with Galois group D_ℓ, $|\mathrm{Disc}(L)| \le X$, and whose quadratic resolvent is respectively real or imaginary, it is natural to ask whether we can obtain estimates for $N^{\pm}_{D_\ell}(X)$. A plausible guess is that for some $C_\ell > 0$ we have

$$N^{-}_{D_\ell}(X) \sim C_\ell X^{2/(\ell-1)} \quad \text{and} \quad N^{+}_{D_\ell}(X) \sim \frac{C_\ell}{\ell} X^{2/(\ell-1)}\ . \tag{7.2}$$

By Davenport–Heilbronn this is known for $\ell = 3$ with $C_3 = 1/(4\zeta(3))$, but it is unclear how to recover this value of C_3, even heuristically, from our work. As such we still seem to be far from a proof of (7.2).

8. Study of the Groups $G_{\mathfrak{b}}$

In this section, where we continue to assume that $k = \mathbb{Q}$ and also assume that $\ell \ge 5$, we study the groups $G_{\mathfrak{b}}$ appearing in Theorem 7.3. In particular, each Euler product appearing in Theorem 7.3 corresponds to a character of $G_{\mathfrak{b}}$, and so we want to study the size of this group.

We are indebted to Hendrik Lenstra for help in this section. This was not done in [12], but much of this was done in our paper [13] with Rubinstein-Salzedo on the Ohno–Nakagawa relation. Accordingly we give only a brief account of those results which are proved there.

We recall a few of the important notations used previously:

- K_z is an abelian extension of $\mathbb{Q}$ containing the ℓth roots of unity, with $G = \mathrm{Gal}(K_z/\mathbb{Q}) = \langle \tau, \tau_2 \rangle$ or $\langle \tau \rangle$ in the general and special cases respectively.
- As in Proposition 2.4, $N_z = K_z(\sqrt[\ell]{\alpha})$ is a cyclic extension, for which we wrote $\alpha\mathbb{Z}_{K_z} = \mathfrak{q}^\ell \prod_{0 \le i \le \ell-2} \mathfrak{a}_i^{g^i}$ and (in Proposition 2.19) $\prod_{0 \le i \le \ell-2} \mathfrak{a}_i = \mathfrak{a}_\alpha \mathbb{Z}_{K_z}$ for an ideal $\mathfrak{a}_\alpha$ of K.
- We recall the possibilities for $\mathfrak{b}$ (equivalently, $\mathfrak{b}_z$) from (7.1), and we continue to use the notation $(-,-,-,-)$ for quantities depending on $\mathfrak{b}$.

For any $\mathfrak{b}$ as in (7.1) we define $\mathfrak{b}^* := (1-\zeta_\ell)^\ell/\mathfrak{b}$.

Proposition 8.1. *With the notation above, we have $\mathfrak{f}(N_z/K_z) \mid \mathfrak{b}$ if and only if $\overline{\alpha} \in S_{\mathfrak{b}^*}(K_z)$.*

Proof. This is very classical, and essentially due to Kummer and Hecke: for instance, by Theorem 3.7 of [11] we have

$$\mathfrak{f}(N_z/K_z) = (1-\zeta_\ell)^\ell \mathfrak{a}_\alpha \Big/ \prod_{\mathfrak{p}_z \mid \ell,\ \mathfrak{p}_z \nmid \mathfrak{a}_\alpha} \mathfrak{p}_z^{A_\alpha(\mathfrak{p}_z)-1}\ .$$

Thus, since $\mathfrak{a}_\alpha$ is coprime to the product then $\mathfrak{f}(N_z/K_z) \mid (1-\zeta_\ell)^\ell$ if and only if $\mathfrak{a}_\alpha = \mathbb{Z}_K$, i.e., if and only if α is a virtual unit. If this is the case, then $\mathfrak{f}(N_z/K_z) \mid \mathfrak{b}$ if and only if the product divides $(1-\zeta_\ell)^\ell/\mathfrak{b} = \mathfrak{b}^*$, and by definition of A_α and its immediate properties recalled in Proposition 3.6, this is equivalent to the solubility of the congruence $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{b}^*}$, hence to $\overline{\alpha} \in S_{\mathfrak{b}^*}(K_z)$. ☐

Theorem 8.2. [13, Corollary 3.3] *Writing $C_{\mathfrak{b}} := \mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$, so that $G_{\mathfrak{b}} = C_{\mathfrak{b}}[T]$, and $\boldsymbol{\mu}_\ell$ for the group of ℓth roots of unity, there exists a perfect, G-equivariant pairing of $\mathbb{F}_\ell[G]$-modules*

$$C_{\mathfrak{b}} \times S_{\mathfrak{b}^*}(K_z) \mapsto \boldsymbol{\mu}_\ell\ .$$

Proof. This is the Kummer pairing: given $\overline{\mathfrak{a}} \in C_{\mathfrak{b}}$, let $\sigma_{\mathfrak{a}}$ denote its image under the Artin map; given $\overline{\alpha} \in S_{\mathfrak{b}^*}(K_z)$, let α be any lift; then define the pairing by $(\overline{\mathfrak{a}}, \overline{\alpha}) \mapsto \sigma_{\mathfrak{a}}(\sqrt[\ell]{\alpha})/\sqrt[\ell]{\alpha} \in \boldsymbol{\mu}_\ell$. ☐

Corollary 8.3. [13, Corollary 3.4 (in part)] *In the general case, where $T = \{\tau - g, \tau_2 + 1\}$, define $T^* = \{\tau - 1, \tau_2 + 1\}$, and in the special case, where $T = \{\tau + g\}$, define $T^* = \{\tau + 1\}$. Then we have a perfect pairing*

$$G_{\mathfrak{b}} \times S_{\mathfrak{b}^*}(K_z)[T^*] \mapsto \boldsymbol{\mu}_\ell\ .$$

In particular, we have

$$|G_{\mathfrak{b}}| = |S_{\mathfrak{b}^*}(K_z)[T^*]|\ .$$

Proof. Recalling that $\tau(\zeta_\ell)=\zeta_\ell^g$, for any j the preceding corollary yields a perfect pairing

$$C_{\mathfrak{b}}[\tau-g^j]\times S_{\mathfrak{b}^*}(K_z)[\tau-g^{1-j}]\mapsto \boldsymbol{\mu}_\ell\ .$$

We conclude by taking $j=1$ and $j=(\ell+1)/2$ in the general and special cases respectively. □

In the special case we have the following useful fact:

Proposition 8.4. *In the special case, we have* $\mathrm{Cl}(\mathbb{Q}_z)/\mathrm{Cl}(\mathbb{Q}_z)^\ell[\tau+1]=\{1\}$.

Proof. We first show that there exists an isomorphism

$$\mathrm{Cl}(\mathbb{Q}_z)/\mathrm{Cl}(\mathbb{Q}_z)^\ell[\tau+1]\simeq \mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell[\tau+1]\ .$$

By Lemma 2.3 (which also applies to $t=\tau+1$), the left side consists of those classes which may be represented by ideals of the form $\mathcal{N}_{\mathbb{Q}_z/K}(\mathfrak{a})/\tau(\mathcal{N}_{\mathbb{Q}_z/K}(\mathfrak{a}))$. We therefore obtain a well-defined, injective map to $\mathrm{Cl}(K)/\mathrm{Cl}(K)^\ell[\tau+1]$. Any ideal in the target space may be represented by an ideal of the form $\mathfrak{c}/\tau(\mathfrak{c})$, which is equivalent to $(\mathfrak{c}/\tau(\mathfrak{c}))^{(\ell-1)^2}$, and $\mathfrak{c}^{(\ell-1)^2}=\mathcal{N}_{\mathbb{Q}_z/K}(\mathfrak{c}^{2(\ell-1)}\mathbb{Z}_{\mathbb{Q}_z})$, so that the map is surjective as well.

Now it suffices to show that $\ell\nmid h(\pm\ell)$, where $h(D)$ denotes the class number of $\mathbb{Q}(\sqrt{D})$, and this follows from the classical and easy fact that $h(\pm\ell)<\ell$ for all prime ℓ. □

Remark 8.5. *For $\ell\equiv 3\pmod 4$ it is also possible to prove the proposition via the Herbrand-Ribet theorem and a congruence for Bernoulli numbers.*

Now suppose that $\ell\equiv 1\pmod 4$. Then the *Ankeny-Artin-Chowla conjecture* (AAC) [1, 29] states that if $\epsilon=(a+b\sqrt{\ell})/2$ is the fundamental unit of $\mathbb{Q}(\sqrt{\ell})$, then $\ell\nmid b$. We will use the statement of the conjecture directly, but we note that Ankeny and Chowla [2] and Kiselev [23] proved that it is equivalent to the condition $\ell\nmid B_{(\ell-1)/2}$, which is trivially true if ℓ is a regular prime, a result first proved by Mordell [29]. It has been verified for $\ell\le 2\cdot 10^{11}$ by van der Poorten, te Riele, and Williams [33], but as mentioned in the introduction, on heuristic grounds it it probably false.

Lemma 8.6. *Suppose that the AAC conjecture is true for ℓ. Then the congruence $x^\ell\equiv\varepsilon\pmod{(1-\zeta)^k\mathbb{Z}_{\mathbb{Q}_z}}$ is solvable for $k=(\ell-1)/2$, and not for any larger value of k.*

Proof. Write $\varepsilon=(a+b\sqrt{\ell})/2$ with a, b in $\mathbb{Z}$. Note first that $(1-\zeta)^{(\ell-1)/2}\mathbb{Z}_{\mathbb{Q}_z}=\sqrt{\ell}\mathbb{Z}_{\mathbb{Q}_z}$, and $\varepsilon\equiv a/2\equiv c\equiv c^\ell\pmod{\sqrt{\ell}\mathbb{Z}_K}$ with $c\equiv a/2\pmod{\ell}$, so the congruence is indeed solvable with $k=(\ell-1)/2$. Assume that it is soluble for a strictly larger k, hence modulo $\sqrt{\ell}(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}$. If $x=\sum_{0\le i\le\ell-2}a_i\zeta^i$ with $a_i\in\mathbb{Z}$ (or even in $\mathbb{Z}_\ell$), we have $x^\ell\equiv\sum_{0\le i\le\ell-2}a_i\pmod{\ell}$, so $x^\ell\equiv m\pmod{\ell}$ for some integer m. Thus, if $x^\ell\equiv\varepsilon\pmod{\sqrt{\ell}(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}}$ we have $a+b\sqrt{\ell}\equiv 2m\pmod{\sqrt{\ell}(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}}$. In particular $a\equiv 2m\pmod{\sqrt{\ell}}$, and since they are both integers we deduce that $a\equiv 2m\pmod{\ell}$, so our congruence gives $b\sqrt{\ell}\equiv 0\pmod{\sqrt{\ell}(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}}$, i.e., $b\equiv 0\pmod{(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}}$. Again since b is an integer this implies that $\ell\mid b$, contradicting AAC and proving (1). □

Remark 8.7. *If AAC is false for ℓ, then the congruence is soluble for all k: use $a^2-\ell b^2=-4$ to conclude that $(a/2)^\ell\equiv(a/2)\pmod{\ell^3}$, obtaining the congruence for $k=3(\ell-1)/2$, and use* [8, Theorem 10.2.9] *to conclude.*

We now return to the groups $S_{\mathfrak{b}^*}(K_z)[T^*]$.

Proposition 8.8. *(1) In the general case we have $S_{\mathfrak{b}^*}(K_z)[T^*]\simeq S_{\mathfrak{b}^*\cap K}(K)$.*
(2) In the special case with $\ell\equiv 3\pmod 4$, we have $S_{\mathfrak{b}^*}(K_z)[T^*]=\{1\}$ for all $\mathfrak{b}$.
(3) In the special case with $\ell\equiv 1\pmod 4$, if the Ankeny-Artin-Chowla conjecture is true for ℓ, then we have $|S_{\mathfrak{b}^*}(K_z)[T^*]|=(1,1,\ell,\ell)$ for $\mathfrak{b}$ as in (7.1). *If Ankeny-Artin-Chowla is false for ℓ, then we have instead $|S_{\mathfrak{b}^*}(K_z)[T^*]|=(\ell,\ell,\ell,\ell)$.*

Proof. (1) [13, Proposition 3.5]. We have an injection $S_{\mathfrak{b}^*\cap K}(K) \hookrightarrow S_{\mathfrak{b}^*}(K_z)[\tau-1]$ which we prove is surjective by Hilbert 90 and some elementary computations, yielding an isomorphism $S_{\mathfrak{b}^*}(K_z)[\tau-1,\tau_2+1] \simeq S_{\mathfrak{b}^*\cap K}(K)[\tau_2+1]$. Furthermore, we have

$$S_{\mathfrak{b}^*\cap K}(K) = S_{\mathfrak{b}^*\cap K}(K)[\tau_2+1] \oplus S_{\mathfrak{b}^*\cap K}(K)[\tau_2-1]\ ,$$

and we argue that $S_\ell(K)[\tau_2-1]$ is trivial (and a fortiori all the $S_{\mathfrak{b}^*\cap K}[\tau-1]$), again using Hilbert 90, finishing the proof of (1).

(2) and (3). Assume now that we are in the special case, so that $K_z = \mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$. By Proposition 8.4 we have $(\mathrm{Cl}(K_z)/\mathrm{Cl}(K_z)^\ell)[\tau+1] = \{1\}$, so that $S_\ell(K_z) \simeq U(K_z)/U(K_z)^\ell$ and $S_\ell(K_z)[T^*] \simeq (U(K_z)/U(K_z)^\ell)[\tau - g^{(\ell-1)/2}]$. By Theorem 2.3 of [11] we deduce that $S_\ell(K_z)[T^*]$ is trivial if $\ell \equiv 3 \pmod 4$, $\ell \neq 3$, and when $\ell \equiv 1 \pmod 4$ that it is an $\mathbb{F}_\ell$-vector space of dimension 1. If ε is a fundamental unit of $K = \mathbb{Q}(\sqrt{\ell})$, then since τ acts on ε as Galois conjugation of $K/\mathbb{Q}$, we have $\varepsilon\tau(\varepsilon) = \mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = -1$, which is an ℓth power. It follows that $S_\ell(K_z)[T^*] = \{\varepsilon^j,\ j \in \mathbb{F}_\ell\}$.

The sizes of the ray Selmer groups are then established by Lemma 8.6 and Remark 8.7. ∎

Remarks 8.9. *(1) The assumption that $\ell \neq 3$ is required when applying Theorem 2.3 of* [11], *and indeed (2) of the proposition is false for $\ell = 3$ (see Proposition 7.3 of* [12]*).*
(2) In Corollary 9.4 we will apply our computations to conclude that AAC is equivalent to the nonexistence of D_ℓ-fields ramified only at ℓ.

This proposition, in combination with Corollary 8.3, gives the size of $|G_\mathfrak{b}|$ in the special case, with possible exceptions $\ell \equiv 1 \pmod 4$ larger than $2\cdot 10^{11}$. In the general case we have the following:

Corollary 8.10. [13, Corollary 3.6] *Assume that we are in the general case.*
(1) We have a canonical isomorphism $G_\mathfrak{b} \simeq \mathrm{Hom}(S_{\mathfrak{b}^*\cap K}(K), \boldsymbol{\mu}_\ell)$.
(2) In particular

$$|G_\mathfrak{b}| = \ell^{r(\mathfrak{b})} \quad \textit{with} \quad r(\mathfrak{b}) = 1 - r_2(D) - z(\mathfrak{b}) + \mathrm{rk}_\ell(\mathrm{Cl}_{\mathfrak{b}^*\cap K}(K))\ ,$$

with $z(\mathfrak{b}) = (2,1,0,0)$ respectively, the second case occurring only if $\ell | D$.
(3) In particular still, if $D < 0$ and $\ell \nmid h(D)$ then $G_\mathfrak{b}$ is trivial for all $\mathfrak{b} \in \mathcal{B}$.

Proof. (1) is immediate. Lemma 2.6, and Proposition 2.12 of [11], the proofs of which adapt to K without change, yield

$$|S_{\mathfrak{b}_1}(K)||Z_{\mathfrak{b}_1}/Z_{\mathfrak{b}_1}^\ell| = \ell^{1-r_2(D)}|\mathrm{Cl}_{\mathfrak{b}_1}(K)/\mathrm{Cl}_{\mathfrak{b}_1}(K)^\ell|\ ,$$

where $Z_{\mathfrak{b}_1} = (\mathbb{Z}_K/\mathfrak{b}_1)^*$ and $\mathfrak{b}_1 = \mathfrak{b}^* \cap K$. This gives (2) with $z(\mathfrak{b}) = \dim_{\mathbb{F}_\ell}(Z_{\mathfrak{b}_1}/Z_{\mathfrak{b}_1}^\ell)$, and to finish we compute for $\mathfrak{b}$ as in (7.1):

- If $\ell \nmid D$, we have $\mathfrak{b}^*\cap K = (\ell^2\mathbb{Z}_K, *, \ell\mathbb{Z}_K, \mathbb{Z}_K)$.
- If $\ell \mid D$ with $\ell\mathbb{Z}_K = \mathfrak{p}_\ell^2$, we have $\mathfrak{b}^*\cap K = (\mathfrak{p}_\ell^3, \mathfrak{p}_\ell^2, \mathfrak{p}_\ell, \mathbb{Z}_K)$.

∎

Note that (3) is a generalization of Proposition 7.7 of [12].

Since the triviality of $G_\mathfrak{b}$ for all $\mathfrak{b}$ is equivalent to the vanishing of the "remainder term" $\phi_D(s)$ of Corollary 7.4, we may conclude that $\Phi_\ell(K,s)$ is given by a single Euler product in a wide class of examples:

Corollary 8.11. *Assume that $\ell \geq 5$, $D < 0$, and that either we are in the special case (so that $\ell \equiv 3 \pmod 4$), or that we are in the general case with $\ell \nmid h(D)$. Then we have*

$$\sum_{L\in\mathcal{F}_\ell(K)} \frac{1}{f(L)^s} = -\frac{1}{\ell-1} + \frac{1}{\ell-1}L_\ell(s) \prod_{p\equiv\left(\frac{D}{p}\right) \pmod{\ell},\ p\neq\ell} \left(1 + \frac{\ell-1}{p^s}\right)\ ,$$

where $L_\ell(s)$ is as above.

Proof. Clear from the theorem and corollaries; note that the condition $D < 0$ in the special case forces $\ell \equiv 3 \pmod 4$. ☐

Note that for $\ell = 3$, which we have excluded here, the possible nontriviality of $\mathfrak{r}^e(\mathfrak{b})$ forces us to also distinguish between $D \equiv 3$ and $D \equiv 6 \pmod 9$.

Examples with $\ell = 5$:

$$\sum_{L \in \mathcal{F}_5(\mathbb{Q}(\sqrt{-1}))} \frac{1}{f(L)^s} = -\frac{1}{4} + \frac{1}{4}\left(1 + \frac{4}{5^{2s}}\right) \prod_{p \equiv \pm 1 \pmod{20}} \left(1 + \frac{4}{p^s}\right) .$$

$$\sum_{L \in \mathcal{F}_5(\mathbb{Q}(\sqrt{-15}))} \frac{1}{f(L)^s} = -\frac{1}{4} + \frac{1}{4}\left(1 + \frac{4}{5^{s}}\right) \prod_{p \equiv \pm 1 \pmod{30}} \left(1 + \frac{4}{p^s}\right) .$$

9. Transformation of the Main Theorem

We now prove, as we did in [14] for the case of $\ell = 3$, that the characters of $G_\mathfrak{b}$ appearing in Theorem 6.1 can be given a simpler description, in terms of the splitting of primes in degree ℓ extensions of k. Our main result along these lines extends Theorem 4.1 of [14] and Lemma 3.9 of [13], and does not assume that $k = \mathbb{Q}$, and thus is new even for $\ell = 3$.

For the case $k = \mathbb{Q}$ we will further specialize the result and obtain an explicit formula, relying (in the general case) on the results of [13].

We first recall a bit of group theory, and introduce some notation. The *Frobenius group* $F_\ell = C_\ell \rtimes C_{\ell-1}$ is the non-abelian group of order $\ell(\ell-1)$ given by the presentation

$$\langle \tau, \sigma \ : \ \tau^{\ell-1} = \sigma^\ell = 1, \tau\sigma\tau^{-1} = \sigma^h \rangle \ ,$$

for any primitive root $h \pmod \ell$. As may be easily checked, $C_{\ell-1}$ is not normal in F_ℓ, nor is any nontrivial subgroup of $C_{\ell-1}$; moreover, there are ℓ subgroups isomorphic to $C_{\ell-1}$, generated by $\tau\sigma^i$ for $0 \le i \le \ell - 1$, and all of these subgroups are conjugate.

We say that a degree ℓ field extension E/k is an *F_ℓ-extension* if its Galois closure has Galois group F_ℓ over k.

Now, let K, K_z, τ, τ_2 be defined as before. In the general case recall that K' was defined to be the mirror field of K, e.g., the subfield of K_z fixed by $\tau^{(\ell-1)/2}\tau_2$; in the special case write $K' = K_z = k_z$. We chose $\tau \in \mathrm{Gal}(k_z/k)$ and a primitive root $g \pmod \ell$ with $\tau(\zeta_\ell) = \zeta_\ell^g$. In the special case τ lifts uniquely to an element of $\mathrm{Gal}(K_z/K)$ and restricts to a unique element of $\mathrm{Gal}(K'/k)$, so in either case the choice of $g \pmod \ell$ uniquely determines $\tau \in \mathrm{Gal}(K'/k)$.

Theorem 9.1. *For each $\mathfrak{b} \in \mathcal{B}$ (as in Theorem 6.1), there exists a bijection between the following sets:*

- *Characters $\chi \in \widehat{G_\mathfrak{b}}$, up to the equivalence relation $\chi \sim \chi^a$ for each a coprime to ℓ.*
- *Subgroups of index ℓ of $G_\mathfrak{b}$.*
- *F_ℓ-extensions E/k (up to isomorphism), whose Galois closure E' contains K', with the conductor $\mathfrak{f}(E'/K')$ dividing $\mathfrak{b}' = \mathfrak{b} \cap K$, such that $\tau\sigma\tau^{-1} = \sigma^g$ for $\tau \in \mathrm{Gal}(K'/k)$ as described above and any generator σ of $\mathrm{Gal}(E'/K')$.*

Moreover, for each corresponding pair (χ, E) and each prime $p \in \mathcal{D} \cup \mathcal{D}_\ell$, the following is true: we have $p \in \mathcal{D}'(\chi) \cup \mathcal{D}'_\ell(\chi)$ if and only if p is totally split in E; equivalently, $p \notin \mathcal{D}'(\chi) \cup \mathcal{D}'_\ell(\chi)$ if and only if p is totally inert or totally ramified in E.

Recall (Definition 2.12) that $\mathcal{D} \cup \mathcal{D}_\ell$ was defined in terms of splitting conditions in K_z/k, so that this theorem describes each Euler factor in $\Phi_\ell(K,s)$ in terms of splitting conditions in a fixed set of number fields.

Proof. The proof borrows heavily from those of Proposition 4.1 of [14] and Lemma 3.9 of [13].

The correspondence between the first two sets is immediate: $G_{\mathfrak{b}}$ is elementary ℓ-abelian, and characters correspond to their kernels.

By Proposition 6.3, regard $G_{\mathfrak{b}} = \frac{\mathrm{Cl}_{\mathfrak{b}'}(K')}{\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell}[\tau \mp g]$, where the sign is $-$ in the general case and $+$ in the special case. $G'_{\mathfrak{b}} = \mathrm{Cl}_{\mathfrak{b}'}(K')/\mathrm{Cl}_{\mathfrak{b}'}(K')^\ell$, and by Lemmas 2.1 and 2.3 we have the orthogonal decomposition $G'_{\mathfrak{b}} = G_{\mathfrak{b}} \times G''_{\mathfrak{b}}$, where $G''_{\mathfrak{b}}$ is the direct sum of all of the other eigenspaces for the actions of τ. Thus, subgroups of $G_{\mathfrak{b}}$ of index ℓ correspond to subgroups B of $\mathrm{Cl}_{\mathfrak{b}'}(K')$ of index ℓ containing $G''_{\mathfrak{b}}$.

By class field theory, there exists a unique abelian extension E'/K', with Galois group C_ℓ and conductor dividing $\mathfrak{b}'$, for which the Artin map induces an isomorphism $\mathrm{Cl}_{\mathfrak{b}'}(K')/B \simeq \mathrm{Gal}(E'/L)$. The uniqueness forces E' to be Galois over k; here we use that $\mathfrak{b}$, B, and $\mathrm{Cl}_{\mathfrak{b}}(K')$ are preserved by $\mathrm{Gal}(K'/k)$. For each fixed $\mathfrak{b}$, we obtain a different E' for each B.

Because the action of $\mathrm{Gal}(K'/k)$ on $\mathrm{Cl}_{\mathfrak{b}'}(K')/B_\chi$ matches its conjugation action on $\mathrm{Gal}(E'/K')$, we have

$$\mathrm{Gal}(E'/k) = \langle \tau, \sigma \ : \tau^{\ell-1} = \sigma^\ell = 1, \tau\sigma\tau^{-1} = \sigma^{\mp g} \rangle \simeq F_\ell \ , \tag{9.1}$$

and we take E to be the fixed field of $\langle \tau \rangle$ (or, alternatively, of any conjugate subgroup).

It must finally be proved that whether $p \in \mathcal{D}'(\chi)$ or not is determined by its splitting in E. In the general case, or in the special case with $\ell \equiv 1 \pmod 4$, Proposition 2.15 or Corollary 2.11 implies that $\mathcal{D} \cup \mathcal{D}_\ell$ is precisely the set of primes p which split completely in K'/k, and by definition $\mathcal{D}'(\chi) \cup \mathcal{D}'_\ell(\chi)$ is the set of primes $p \in \mathcal{D} \cup \mathcal{D}_\ell$ for which one (equivalently, all) of the primes $\mathfrak{p}_{K'}$ of K' above p split completely in E'. If $\mathfrak{p}_{K'}$ splits completely in E', then so does p, so p also splits completely in E/k. Conversely, if any $\mathfrak{p}_{K'}$ is completely ramified or inert in K_z, then p must also do the same in each E; to see this, recall that ramification and inertial degrees are multiplicative, and that $[E' : E] = \ell - 1$.

When $\ell \equiv 3 \pmod 4$, p may be inert or ramified in K/k (but still splits completely in K'/K) so it is slightly more subtle to argue that if $\mathfrak{p}_{K'}$ splits completely in E'/K' then p does so in E/k. Given these hypotheses, let $\mathfrak{P}$ be a prime of E' over $\mathfrak{p}_{K'}$; then the decomposition group $D(\mathfrak{P}/p)$ has size 2. We check that for some conjugate $\mathfrak{P}'$ of $\mathfrak{P}$, $D(\mathfrak{P}'/p) = \langle \tau^{(\ell-1)/2} \rangle$, which implies that p splits completely in E. Indeed, all degree $\ell - 1$ subgroups of F_ℓ are conjugate, so that p must split completely in each of the degree ℓ subextensions of E'/k.

□

For $\ell = 3$ and $k = \mathbb{Q}$, in [14] we further applied a theorem of Nakagawa to give a precise description of *all* the extensions $E/\mathbb{Q}$ occurring in the statement of Theorem 9.1, in terms of their discriminants. Using this, we obtained the formula

$$\frac{2}{3^{r_2(D)}}\Phi_3(Q(\sqrt{D}), s) = M_1(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) + \sum_{E \in \mathcal{L}_3(D)} M_{2,E}(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{\omega_E(p)}{p^s}\right), \tag{9.2}$$

where: $\mathcal{L}_3(D)$ is the set of all cubic fields of discriminant $-D/3$, $-3D$, and $-27D$; $\omega_E(p)$ is 2 or -1 depending on whether p is split or inert in E, as in Theorem 9.1; and $M_1(s)$ and $M_{2,E}(s)$ are 3-adic factors (a sum of the appropriate $A_{\mathfrak{b}}(s)$.

9.1. **Explicit computations in the special case.** For $\ell = 3$, we have the following explicit formula (corresponding to pure cubic fields), which was previously proved in [12].

$$\sum_{L\in\mathcal{F}_3(\mathbb{Q}(\sqrt{-3}))}\frac{1}{f(L)^s}=-\frac{1}{2}+\frac{1}{6}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{2}{p^s}\right)+\frac{1}{3}\prod_p\left(1+\frac{\omega_E(p)}{p^s}\right)\ ,$$

where E is the cubic field defined by $x^3-3x-1=0$ (discriminant 3^4, Galois group C_3), and

$$\omega_E(p)=\begin{cases}-1 & \text{if } p \text{ is inert or totally ramified in } E\ ,\\ 2 & \text{if } p \text{ is totally split in } E\ ,\\ 0 & \text{otherwise.}\end{cases}$$

In fact, since E is cyclic cubic, we never have $\omega_E(p) = 0$, and $\omega_E(p) = 2$ if and only if $p \equiv \pm 1 \pmod 9$.

For $\ell \equiv 3 \pmod 4$ and $\ell > 3$, a generalization was proved in Corollary 8.11. For $\ell \equiv 1 \pmod 4$, the generalization is more complicated due to the nontriviality of $S_{\mathfrak{b}^*}(K_z)[T^*]$. Define a polynomial

$$P(X)=-2iT_\ell(iX/2)=\sum_{k=0}^{(\ell-1)/2}\ell\frac{(\ell-k-1)!}{k!(\ell-2k)!}X^{\ell-2k}\ .$$

Here $T_\ell(X)$ is the Chebyshev polynomial of the first kind, satisfying

$$P(x-x^{-1})=x^\ell-x^{-\ell}\ , \tag{9.3}$$

so that $x^{-1}P(x)$ is the minimal polynomial of $\zeta_\ell-\zeta_\ell^{-1}$.

Proposition 9.2. *Assume that $\ell \equiv 1 \pmod 4$ satisfies the Ankeny-Artin-Chowla conjecture, and let ε be a fundamental unit of $\mathbb{Q}(\sqrt{\ell})$. Then we have*

$$\sum_{L\in\mathcal{F}_\ell(\mathbb{Q}(\sqrt{\ell}))}\frac{1}{f(L)^s}=-\frac{1}{\ell-1}+\frac{1}{\ell(\ell-1)}\left(1+\frac{\ell-1}{\ell^s}\right)\prod_{p\equiv 1\pmod{\ell}}\left(1+\frac{\ell-1}{p^s}\right)+\frac{1}{\ell}\prod_p\left(1+\frac{\omega_E(p)}{p^s}\right)\ ,$$

where E is the F_ℓ-field defined by $P(x)-\mathrm{Tr}(\varepsilon)=0$ of discriminant $\ell^{(3\ell-1)/2}$, and

$$\omega_E(p)=\begin{cases}-1 & \textit{if } p \textit{ is inert or totally ramified in } E\ ,\\ \ell-1 & \textit{if } p \textit{ is totally split in } E\ ,\\ 0 & \textit{otherwise.}\end{cases}$$

If $\ell \equiv 1 \pmod 4$ does not satisfy the Ankeny-Artin-Chowla conjecture, we have the same formula, but with $\mathrm{Disc}(E) = \ell^{\ell-2}$ *and $\omega_E(\ell) = \ell - 1$.*

Before presenting the proof, we make some additional observations.

Remarks 9.3.
(1) *In the equation for E we may replace* $\mathrm{Tr}(\varepsilon)$ *by* $\mathrm{Tr}(\pm\varepsilon^m)$ *for any odd $m \in \mathbb{Z}$ coprime to ℓ.*
(2) *Assuming AAC, the last product may be written as*

$$\left(1-\frac{1}{\ell}\right)\prod_{p\equiv 1\pmod{\ell}}\left(1+\frac{\omega_E(p)}{p^s}\right)\ .$$

(3) *When $p \equiv 1 \pmod{\ell}$ then p is totally split in E if and only if*

$$\varepsilon^{(p-1)/\ell}\equiv 1 \pmod p\ ,$$

and otherwise p is inert in E.

(4) If in addition $\mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$ has class number 1, then p is totally split in E if and only if $p = \mathcal{N}_{\mathbb{Q}_z/\mathbb{Q}}(\pi)$ for some $\pi \equiv 1 \pmod{\ell}$ in $\mathbb{Q}_z$.

Corollary 9.4. *Let $\ell \equiv 1 \mod 4$. Then there exist D_ℓ-fields ramified only at ℓ if and only if the Ankeny-Artin-Chowla conjecture is false for ℓ.*

Proof. Immediate by inspecting the Dirichlet series of the proposition; the proposition also shows that for any ℓ not satisfying the conjecture, the field is unique and has discriminant $\ell^{\frac{3(\ell-1)}{2}}$. $\square$

Remark 9.5. *This corollary recovers and strengthens a result of Jensen and Yui* [22, Theorem I.2.2], *who proved that if $\ell \equiv 1 \pmod 4$ is regular, then there are no D_ℓ-fields with discriminant a power of ℓ. (This can also be seen for $\ell \equiv 3 \pmod 4$ from Corollary 8.11.)*

The connection to the Ankeny-Artin-Chowla conjecture was previously observed by Lemmermeyer [26], *who suggested that a proof of Corollary 9.4 may exist somewhere in the literature.*

Before beginning the proof of Proposition 9.2 we establish the following:

Lemma 9.6. *We have*

$$\mathrm{Disc}(N_z) = \begin{cases} \ell^{(3\ell^2-2\ell-3)/2} & \text{if } AAC \text{ is true,} \\ \ell^{\ell(\ell-2)} & \text{if } AAC \text{ is false.} \end{cases}$$

In addition, in the extension $N_z/\mathbb{Q}_z$ the prime ideal $(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}$ is totally ramified if AAC is true and totally split otherwise.

Proof. The field N_z is a Kummer extension of $K_z = \mathbb{Q}_z$ with defining equation $x^\ell - \varepsilon = 0$, so that

$$\mathrm{Disc}(N_z) = \pm\mathcal{N}_{\mathbb{Q}_z/\mathbb{Q}}(\mathfrak{d}(N_z/\mathbb{Q}_z))\mathrm{Disc}(\mathbb{Q}_z)^\ell = \pm\ell^{\ell(\ell-2)}\mathcal{N}_{\mathbb{Q}_z/\mathbb{Q}}(\mathfrak{f}(N_z/\mathbb{Q}_z))^{\ell-1} ,$$

where $\mathfrak{f}(N_z/\mathbb{Q}_z)$ is the conductor.

By Hecke's Theorem 10.2.9 of [8][6] applied to $K = \mathbb{Q}_z$ and $\alpha = \varepsilon$ which is a unit, we have $\mathfrak{f}(N_z/\mathbb{Q}_z) = (1-\zeta)^{\ell+1-A_\varepsilon}$, where $A_\varepsilon = \ell+1$ if $x^\ell \equiv \varepsilon \pmod{(1-\zeta)^\ell}$ has a solution in $\mathbb{Q}_z$, and otherwise A_ε is the maximal k such that $x^\ell \equiv \varepsilon \pmod{(1-\zeta)^k}$ has a solution. By Lemma 8.6 we have $A_\varepsilon = (\ell-1)/2$ (resp., $A_\varepsilon = \ell+1$) if AAC is true (resp., false), hence $\mathfrak{f}(N_z/\mathbb{Q}_z) = (1-\zeta)^{(\ell+3)/2}\mathbb{Z}_{\mathbb{Q}_z}$ (resp., $\mathfrak{f}(N_z/\mathbb{Q}_z) = \mathbb{Z}_{\mathbb{Q}_z}$), from which the formula follows (note that the sign of the discriminant is positive since $\mathbb{Q}_z$ hence N_z is totally complex). In addition, if AAC is false, so that C_k is soluble for all k, then the same theorem of Hecke implies that $(1-\zeta)\mathbb{Z}_{\mathbb{Q}_z}$ is totally split, while if AAC is true then it is totally ramified. $\square$

Proof of Proposition 9.2. The result follows for an undetermined E by Theorem 9.1 and Proposition 8.8. To determine E, observe that Propositions 8.1 and 8.8 imply that $N_z = K_z(\epsilon^{1/\ell})$, and that the considerations in the proof of Theorem 9.1 allow us to take E to be *any* of the (conjugate) degree ℓ subfields of N_z, so that it suffices to exhibit one.

We take $E = \mathbb{Q}(\varepsilon^{1/\ell} - \varepsilon^{-1/\ell})$ for any fixed choice of $\varepsilon^{1/\ell}$, recalling that the fundamental unit has norm -1. Then the minimal polynomial of E is $P(x) - \mathrm{Tr}(\varepsilon)$ by construction, or more precisely by (9.3).

It remains only to argue that

$$\mathrm{Disc}(E) = \begin{cases} \ell^{(3\ell-1)/2} & \text{if AAC is true,} \\ \ell^{\ell-2} & \text{if AAC is false.} \end{cases}$$

We assume that AAC is true (if false, a similar proof applies). On the one hand we have

$$\mathrm{Disc}(N_z) = \mathrm{Disc}(E)^{\ell-1}\mathcal{N}_{E/\mathbb{Q}}(\mathfrak{d}(N_z/E)) ,$$

[6] Proposition 3.6 of [11] is not applicable since the extensions $N_z/\mathbb{Q}$ and N_z/K are not abelian.

in other words taking valuations and using the proposition:

$$(\ell-1)v_\ell(\mathrm{Disc}(E)) = (3\ell^2-2\ell-3)/2 - v_\ell(\mathcal{N}_{E/\mathbb{Q}}(\mathfrak{d}(N_z/E))) = (\ell-1)(3\ell-1)/2+\ell-2-v_\ell(\mathcal{N}_{E/\mathbb{Q}}(\mathfrak{d}(N_z/E)))\ .$$

On the other hand, the extension N_z/E is of degree $\ell-1$ hence tame, so $v_\ell(\mathcal{N}_{E/\mathbb{Q}}(\mathfrak{d}(N_z/E))) \le \ell-2$. Divisibility by $\ell-1$ thus implies the result, together with the additional result that $\mathcal{N}_{E/\mathbb{Q}}(\mathfrak{d}(N_z/E)) = \ell^{\ell-2} = \mathrm{Disc}(\mathbb{Q}_z)$. □

We conclude by establishing the statements made in the remarks. For (1), it is easily seen that our construction still produces a degree ℓ subfield of E. (2) follows because ℓ is totally split or inert in E if and only if it is totally split in $\mathbb{Q}_z$, and because ℓ is totally ramified in E.

To prove (3), we again apply Hecke's theorem 10.2.9 of [8]: p is totally split in E iff it is in $N_z/\mathbb{Q}_z$, hence by Hecke iff $x^\ell \equiv \varepsilon \pmod{\mathfrak{p}}$ is soluble in $\mathbb{Q}_z$. (Here $\mathfrak{p}$ is any prime of $\mathbb{Q}_z$ above p, which must have degree 1 since $p \equiv 1 \pmod{\ell}$ is totally split in $\mathbb{Q}_z$.) This is equivalent to $\varepsilon^{(p-1)/\ell} \equiv 1 \pmod{\mathfrak{p}}$, which by Galois theory will then be true for all primes $\mathfrak{p}$ above p since for any $\sigma \in \mathrm{Gal}(\mathbb{Q}_z/\mathbb{Q})$ we have either $\sigma(\varepsilon) = \varepsilon$ or $\sigma(\varepsilon) = -\varepsilon^{-1}$, and $(p-1)/\ell$ is even so the sign disappears. Hence this is equivalent to the condition $\varepsilon^{(p-1)/\ell} \equiv 1 \pmod{p}$, as desired.

Finally, (4) follows from Eisenstein's reciprocity law.

9.2. **Explicit formulas for $k = \mathbb{Q}$ in the general case.** Let $k = \mathbb{Q}$. In Theorem 9.1 we saw that characters χ of $G_{\mathfrak{b}}$ (up to the equivalence $\chi \sim \chi^a$ for $(a,\ell) = 1$) correspond to degree ℓ fields E having certain properties. In our companion paper [13] with Rubinstein-Salzedo, we further proved the following:

Theorem 9.7. [13] *Suppose that $k = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{D})$ with $D \neq 1, \pm\ell$, so that we are in the general case, and as before let K' be the mirror field of K.*

Then the fields E enumerated in Theorem 9.1 are precisely those F_ℓ-fields E, whose Galois closure contains K', subject to the condition $\tau\sigma\tau^{-1} = \sigma^g$ described there, satisfying the following additional conditions:

- *E is totally real if $D < 0$, and has $\frac{\ell-1}{2}$ pairs of complex embeddings if $D > 0$.*
- *$|\mathrm{Disc}(E)|$ has the form $\ell^a D^{\frac{\ell-1}{2}}$, where a satisfies*

$$\begin{aligned} &a \in \{0, 2\} && \text{if } \ell \nmid D\ , \\ &a \in \{0, \tfrac{\ell+3}{2}\} && \text{if } \ell \mid D \text{ and } \ell \equiv 1 \pmod{4}\ , \\ &a \in \{0, \tfrac{\ell+5}{2}\} && \text{if } \ell \mid D \text{ and } \ell \equiv 3 \pmod{4}\ . \end{aligned} \tag{9.4}$$

Moreover, if E is any F_ℓ-field satisfying these last two properties, then its Galois closure automatically contains K'.

Recall that we have $\mathfrak{b} \in \mathcal{B} = \{1, (\ell)^{1/2}, (\ell), (\ell)^{\ell/(\ell-1)}\}$, with the possibility $(\ell)^{1/2}$ occurring only if $\ell | D$. The complete list of fields enumerated in Theorem 9.7 corresponds to $\mathfrak{b} = (\ell)^{\ell/(\ell-1)}$. A careful reading of the proof of Theorem 9.7 (in [13]) shows that the remaining $\mathfrak{b}$ correspond to the following possibilities for a in (9.4):

Condition on D	$\mathfrak{b} = 1$	$\mathfrak{b} = (\ell)^{1/2}$	$\mathfrak{b} = (\ell)$	$\mathfrak{b} = (\ell)^{\ell/(\ell-1)}$
$\ell \nmid D$	$a = 0$	-	$a = 0, 2$	$a = 0, 2$
$\ell \mid D$ and $\ell \equiv 1 \pmod{4}$	$a = 0$	$a = 0$	$a = 0, \frac{\ell+3}{2}$	$a = 0, \frac{\ell+3}{2}$
$\ell \mid D$ and $\ell \equiv 3 \pmod{4}$	$a = 0$	$a = 0$	$a = 0, \frac{\ell+5}{2}$	$a = 0, \frac{\ell+5}{2}$

One exception occurs for $\ell = 3$: Only $a = 0$ corresponds to $\mathfrak{b} = (\ell)$ when $\ell \mid D$; this is because the inequality $\frac{\ell+5}{2} \le \ell - 1$ is true for all $\ell \equiv 3 \pmod{4}$ except for $\ell = 3$. (Note also for $\ell = 3$ that this result is equivalent to part of Proposition 4 in [?].)

This is sufficient to obtain an explicit formula for $\Phi_\ell(K,s)$ for any K and ℓ, provided that the appropriate F_ℓ-fields can be tabulated. We present two examples, which we also double-checked numerically using a program written in PARI/GP [32].

Example 9.8. *Let $K=\mathbb{Q}(\sqrt{13})$ and $\ell=5$. Then, we have*

$$\begin{aligned}\sum_{L\in\mathcal{F}_5(\mathbb{Q}(\sqrt{13}))}\frac{1}{f(L)^s}&=-\frac{1}{4}+\frac{1}{20}\left(1+\frac{4}{25^s}\right)\prod_p\left(1+\frac{4}{p^s}\right)+\frac{1}{5}\left(1-\frac{1}{25^s}\right)\prod_p\left(1+\frac{\omega_E(p)}{p^s}\right)\\&=59^{-s}+409^{-s}+475^{-s}+619^{-s}+709^{-s}+1009^{-s}+\cdots+4\cdot 24131^{-s}+\cdots\ ,\end{aligned}$$

where the products are over primes $p\equiv 1,16,19,24,34,36,44,51,54,56,59,61 \pmod{65}$, E is the field defined by the polynomial x^5+5x^3+5x-3, and $24131=59\cdot 409$.

Example 9.9. *Let $K=\mathbb{Q}(\sqrt{-7\cdot 41})$ and $\ell=7$. Then, we have*

$$\begin{aligned}\sum_{L\in\mathcal{F}_7(\mathbb{Q}(\sqrt{-287}))}\frac{1}{f(L)^s}&=-\frac{1}{6}+\frac{1}{6}\left(1+\frac{6}{7^s}\right)\prod_p\left(1+\frac{6}{p^s}\right)+\left(1-\frac{1}{7^s}\right)\prod_p\left(1+\frac{\omega_E(p)}{p^s}\right)\\&=1+7\cdot 301^{-s}+7\cdot 337^{-s}+7\cdot 581^{-s}+7\cdot 791^{-s}+\cdots+42\cdot 296897^{-s}+\cdots\ ,\end{aligned}$$

where the products are over primes $p\equiv\left(\frac{D}{p}\right) \pmod{\ell}$ excluding $p=\ell$, E is the field defined by the polynomial $x^7-14x^5+56x^3-56x-15$, and $296897=337\cdot 881$.

References

[1] N. C. Ankeny, E. Artin, and S. Chowla, *The class-number of real quadratic number fields*, Ann. of Math. (2) **56** (1952), 479–493.
[2] N. C. Ankeny and S. Chowla, *A further note on the class number of real quadratic fields*, Acta. Arith. **7** (1962), 271–272.
[3] M. Bhargava, *Higher Composition laws. I. A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) **159** (2004), no. 1, 217–250.
[4] M. Bhargava, *Higher Composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886.
[5] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.
[6] M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), no. 3, 1559–1591.
[7] M. Bhargava and A. Shnidman, *On the number of cubic orders of bounded discriminant having automorphism group C_3, and related problems*, Algebra and Number Theory **8** (2014), no. 1, 53–88.
[8] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Math. **193**, Springer-Verlag, New York, 1999.
[9] H. Cohen, *Exact counting of D_ℓ number fields with given quadratic resolvent*, Math. Comp. , to appear.
[10] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Cyclotomic extensions of number fields*, Indag. Math. **14** (2003), 183–196.
[11] H. Cohen, F. Diaz y Diaz, and M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. reine angew. Math. **550** (2002), 169–209.
[12] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.
[13] H. Cohen, S. Rubinstein-Salzedo, and F. Thorne, *Identities for field extensions generalizing the Ohno-Nakagawa relations*, submitted.
[14] H. Cohen and F. Thorne, *Dirichlet series associated to cubic fields with given quadratic resolvent*, Michigan Math. J. **63** (2014), no. 2, 253–273.
[15] H. Davenport, *Multiplicative number theory*, Springer-Verlag, New York, 2000.
[16] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.
[17] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree (English translation)*, AMS, Providence, 1964.
[18] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York, 2004.
[19] G. Gras, *Class Field Theory*, Springer Monographs in Math. (2005).

[20] G. Gras, *Théorèmes de Réflexion*, J. Th. Nombres Bordeaux **10** (1998), 399–499.
[21] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.
[22] C. Jensen and N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory **15** (1982), no. 3, 347–375.
[23] A. A. Kiselev, *An expression for the number of classes of ideals of real quadratic fields by means of Bernoulli numbers (in Russian)*, Dokl. Akad. Nauk. SSSR **61** (1948), 777–779.
[24] Y. Kishi, *The Spiegelungssatz for $p = 5$ from a constructive approach*, Math. J. Okayama Univ. **47** (2005), 1–27.
[25] M. Le, *Upper bounds for class numbers of real quadratic fields*, Acta Arith. **68** (1994), no. 2, 141–144.
[26] F. Lemmermeyer, *Dihedral extensions and the Ankeny-Artin-Chowla conjecture*, MathOverflow post, `http://mathoverflow.net/questions/13152/dihedral-extensions-and-the-ankeny-artin-chowla-conjecture`
[27] S. Louboutin, Y.-H. Park, and Y. Lefeuvre, *Construction of the real dihedral number fields of degree $2p$. Applications.*, Acta Arith. **89** (1999), no. 3, 201–215.
[28] A. Morra, *Comptage asymptotique et algorithmique dextensions cubiques relatives* (in English), thesis, Université Bordeaux I, 2009.
[29] L. J. Mordell, *On a Pellian equation conjecture*, Acta Arith. **6** (1960), 137–144.
[30] J. Nakagawa, *On the relations among the class numbers of binary cubic forms*, Invent. Math. **134** (1998), no. 1, 101–138.
[31] Y. Ohno, *A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms*, Amer. J. Math. **119** (1997), no. 5, 1083–1094.
[32] PARI/GP, version `2.5.1`, Bordeaux, 2011, available from `http://pari.math.u-bordeaux.fr/`
[33] A. J. van der Poorten, H. J. J. te Riele, and H. C. Williams, *Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* $100,000,000,000$, Math. Comp. **70** (2000), no. 235, 1311-1328; corrigenda and addition, Math. Comp. **72** (2002), no. 241, 521–523.
[34] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.
[35] L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1996.
[36] C. Weir, R. Scheidler, and E. Howe, *Constructing and tabulating dihedral function fields*, to appear in Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS-X 2012), Mathematical Science Publishers, Berkeley, 2013.

Université Bordeaux I, Institut de Mathématiques, U.M.R. 5251 du C.N.R.S, 351 Cours de la Libération, 33405 TALENCE Cedex, FRANCE
E-mail address: `Henri.Cohen@math.u-bordeaux1.fr`

Department of Mathematics, University of South Carolina, 1523 Greene Street, Columbia, SC 29208, USA
E-mail address: `thorne@math.sc.edu`