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.

1. Introduction

The theory of cubic number fields and the related theory of the 3-part of class groups of quadratic fields is, in some respects, now quite well understood, thanks to the work of Delone–Faddeev [9], Davenport–Heilbronn [8], and more recently Bhargava [1, 2], although some tantalizing questions remain (e.g., prove that the number of cubic fields with given discriminant D is $O(|D|^\varepsilon)$ for all $\varepsilon > 0$). In [6] and [7] we have contributed to this theory by giving completely explicit formulas for the Dirichlet generating series of discriminants of cubic fields having *given* resolvent.

Generalizing this theory to number fields of larger degree ℓ seems difficult, although Bhargava has remarkable results for $\ell = 4$ and 5 when the Galois group is S_ℓ. In the present paper, we show that the theory developed in [6] and [7] can be completely generalized to degree ℓ extensions having Galois group D_ℓ when ℓ is an odd prime.

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. There exists a unique quadratic subextension K/k of N/k, and K is called the *quadratic resolvent* of L. The extension N/K is cyclic with $\mathrm{Gal}(N/K) \simeq C_\ell$, and a quite nontrivial theorem due to J. Martinet involving the computation of higher ramification groups (see e.g., Corollary 10.1.25 of [3]) 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, so that the relative discriminant $\mathfrak{d}(L/k)$ of L/k is given by the formula $\mathfrak{d}(L/k) = \mathfrak{d}(K/k)^{(\ell-1)/2} f(L)^{\ell-1}$. Note that L has ℓ distinct conjugates in $\widetilde{L}$.

We study the set $\mathcal{F}_\ell(K)$ of D_ℓ-extensions of degree ℓ 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 (which of course implicitly depends on the base field k)

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

Date: April 24, 2013.

1991 *Mathematics Subject Classification.* 11R16.

[1]A remark on our choice of notation: Readers familiar with [7] or [6] should note that by and large we adopt the notation of [7] and the progression of [6]; the reader knowledgeable with the latter paper can immediately see the similarities and differences. (See also Morra's thesis [14] for a version of [6] with more detailed proofs.) What was called (K_2, K, L, K_2') in [6] 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.

where $\mathcal{N}(f(L)) = \mathcal{N}_{k/\mathbb{Q}}(f(L))$ is the absolute norm of the ideal $f(L)$. Our most general result is Theorem 6.1, and we also obtain a more explicit version of Theorem 6.1 in the case $k = \mathbb{Q}$.

The paper is organized as follows. In Section 2 we give a characterization of the fields $L \in \mathcal{F}_\ell(K)$ using Galois and Kummer theory. This will be done by first establishing a bijection between such fields and elements 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. Second, we enumerate these elements of K_z in terms of sets $(\mathfrak{a}_0, \dots, \mathfrak{a}_{\ell-2}, \overline{u})$, where the $\mathfrak{a}_i$ are ideals satisfying certain conditions, and $\overline{u}$ is an element of a Selmer group associated to K_z.

In Section 3, we recall the ramification properties of primes in the cyclotomic extension K_z/K and we compute the conductors $f(N/K)$ and $f(L)$ corresponding to the sets described in Section 2. In Sections 4, 5, and 6 we use these results to obtain a preliminary version of the formula for $\Phi_\ell(K, s)$, involving a number of explicit but not very convenient quantities, and in Sections 7 and 8 we give this formula a more explicit form in the case where the base field k is equal to $\mathbb{Q}$, which is our main case of interest.

Finally, in Sections 9 and 10, still in the case $k = \mathbb{Q}$, we transform this formula into a much nicer form, completely analogous to the one obtained for the cubic case in [7], and we give a number of examples.

2. Galois and Kummer Theory

2.1. **Galois and Kummer theory, and the Group Ring.** We will use the results of [5], 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 [6] (cases (1) and (2) correspond to cyclic extensions of k of degree ℓ, which have been treated in [5]). Cases (3) and (4) are considerably simpler since we do not have to adjoin ζ_ℓ to K to apply Kummer theory.

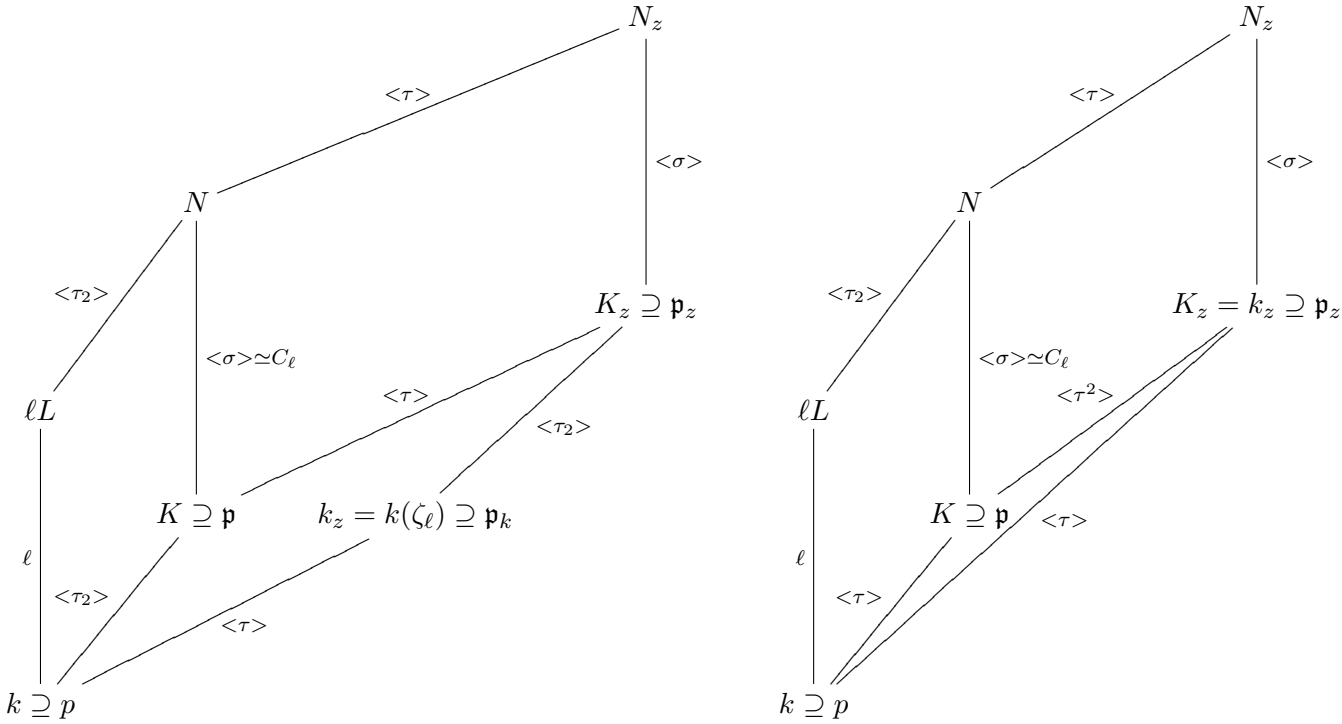
We are particularly interested in the case $k = \mathbb{Q}$, in which case either $[K_z : K] = \ell - 1$, or $[K_z : K] = (\ell - 1)/2$, i.e., $K \subset k_z$, which is equivalent to $K = \mathbb{Q}(\sqrt{\ell^*})$ with $\ell^* = (-1)^{(\ell-1)/2}\ell$. To balance generality and simplicity, *we assume 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 [5].

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 [10]. □

We set the following definitions:

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

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

(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 $\sum_{b \neq a} e_a M$. □

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 $1 \leq j \leq \ell - 1$.*
(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. 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. If $\theta^\ell = \alpha$ with $\theta \in N_z$, 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 $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[T]$. The group conditions on τ and τ_2 are automatically satisfied, and those on σ are exactly those corresponding to the set T. It follows that N_z/k is Galois, and the uniqueness statement modulo the equivalence relation follows from the corresponding one in Kummer theory.

To do by FT: expand the final paragraph a little □

Recall from [3] 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, which shows in particular that the Selmer group is finite, is readily checked, using in particular (by Maschke's theorem) the fact that $|G|$ is coprime to ℓ:

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 $u\mathbb{Z}_{K_z} = \mathfrak{q}^\ell$.

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 $\overline{u} \ne \overline{1}$ 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 $\alpha\mathbb{Z}_{K_z} = \prod_{0\le i\le \ell-2} \mathfrak{a}_i^{g^i}\mathfrak{q}^\ell$, 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. [2]

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 $\overline{\mathfrak{a}} \in (\mathrm{Cl}_\mathfrak{m}(K_z)/\mathrm{Cl}_\mathfrak{m}(K_z)^\ell)[T]$.*

[2] This detailed reasoning was omitted from [6], so the proof given there is incomplete.

Lemma 2.10. *Keep the above notation, and in particular recall that* $\mathfrak{a} = \prod_{0\le i\le \ell-2} \mathfrak{a}_i^{g^i}$. *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. □

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 [11] and [12]), and in particular Scholz's theorem can be generalized to this context, see for instance [13] for the case $\ell = 5$.

To do: Look up where exactly this can be found in Gras?

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 [15]. □

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 [4] 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 [4] 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 is left to the reader. □

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 [4] and [5] some results concerning the cyclotomic extensions k_z/k and K_z/K.

Proposition 3.1. *Keep the above notation, assume that p lies over ℓ, and write $e(\mathfrak{p}) = e(\mathfrak{p}/p)$ and $e(p)$ for the respective absolute ramification indices over ℓ. Then we have*

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

In addition, in the general case, we have $e(\mathfrak{p}_z/\mathfrak{p}_k) = 1$ if $e(\mathfrak{p}/p) = 1$, and if $e(\mathfrak{p}/p) = 2$ we have

$$e(\mathfrak{p}_z/\mathfrak{p}_k) = \begin{cases} 1 & \text{if } v_2(e(p)) < v_2(\ell-1) \ , \\ 2 & \text{if } v_2(e(p)) \geq v_2(\ell-1) \ . \end{cases}$$

Proof. The first formulas follow from loc. cit. . Furthermore we have $e(\mathfrak{p}_z/p) = e(\mathfrak{p}_z/\mathfrak{p})e(\mathfrak{p}/p) = e(\mathfrak{p}_z/\mathfrak{p}_k)e(\mathfrak{p}_k/p)$, and by the same results we have $e(\mathfrak{p}_k/p) = (\ell-1)/(\ell-1, e(p))$. Thus

$$e(\mathfrak{p}_z/\mathfrak{p}_k) = \frac{\ell-1}{(\ell-1, e(\mathfrak{p}/p)e(p))} \frac{(\ell-1, e(p))}{\ell-1} e(\mathfrak{p}/p) = \frac{(\ell-1, e(p))}{(\ell-1, e(\mathfrak{p}/p)e(p))} e(\mathfrak{p}/p) \ ,$$

and from this we easily obtain the given formulas. □

Definition 3.2. *(1) To simplify notation, 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 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 $\mathfrak{p}$ is any ideal 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 $1 \leq r(e) \leq \ell-1$.

Definitions (1) and (2) will only be used for p above ℓ, where we always have $e(\mathfrak{p}_z/p) \mid (\ell-1)$.

Definition 3.3. *Let $\overline{\alpha} \in (K_z^*/K_z^{*\ell})[T]$ be as in Proposition 2.4, let $\mathfrak{p}$ be an ideal of K above ℓ, let $\mathfrak{p}_z$ be an ideal of K_z above $\mathfrak{p}$, and set*

$$M(\mathfrak{p}) = \ell e(\mathfrak{p}_z/\ell)/(\ell-1) \quad \text{and} \quad m(\mathfrak{p}) = M(\mathfrak{p})/e(\mathfrak{p}_z/\mathfrak{p}) = \ell e(\mathfrak{p})/(\ell-1) \ ;$$

note that $M(\mathfrak{p}) \in \mathbb{Z}$ by Proposition 3.1.

Finally, denote by C_n the congruence $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$ in K_z.

- *If C_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*

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

Remarks 3.4. *(1) Writing temporarily $q := r(e(\mathfrak{p}))/(\ell-1, e(\mathfrak{p})) = r(e(\mathfrak{p}))/(\ell-1, r(e(\mathfrak{p})))$, we see that q is an integer, and that $q = 1$ 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 C_n (the congruence $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}_z^n}$) is independent of the ideal $\mathfrak{p}_z$ above p. In other words, using the notation of Definition 3.2, it is equivalent to $x^\ell/\alpha \equiv 1 \pmod{{}^*p^{n/e(\mathfrak{p}_z/p)}}$ or to $x^\ell/\alpha \equiv 1 \pmod{{}^*\mathfrak{p}^{n/e(\mathfrak{p}_z/\mathfrak{p})}}$.*

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 $A_\alpha(\mathfrak{p}) < M(\mathfrak{p})$ then*

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

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

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

(3) Assume that $A_\alpha(\mathfrak{p}) < M(\mathfrak{p})$, or equivalently $a_\alpha(\mathfrak{p}) < m(\mathfrak{p})$. Then $a_\alpha(\mathfrak{p}) \in \mathbb{Z}$, and more precisely

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

Proof. (1) follows from Proposition 3.8 of [5] and the first part of (2) is clear by the inequality that we now prove. Assume that

$$A_\alpha(\mathfrak{p}) < M(\mathfrak{p}) = \ell e(\mathfrak{p}_z/\ell)/(\ell-1) = \ell e(\mathfrak{p})/(\ell-1, e(\mathfrak{p})) .$$

First note that thanks to (1) we have $A_\alpha(\mathfrak{p}) \ge e(\mathfrak{p})/(\ell-1, e(\mathfrak{p})) \ge r(e(\mathfrak{p}))/(\ell-1, e(\mathfrak{p}))$, so that $a_\alpha(\mathfrak{p}) \ge 0$. Furthermore since $M(\mathfrak{p}) \equiv e(\mathfrak{p})/(\ell-1, e(\mathfrak{p})) \pmod{(\ell-1)/(\ell-1, e(\mathfrak{p}))}$, by (1) the inequality $A_\alpha(\mathfrak{p}) < M(\mathfrak{p})$ is equivalent to $A_\alpha(\mathfrak{p}) \le M(\mathfrak{p}) - (\ell-1)/(\ell-1, e(\mathfrak{p}))$, hence

$$a_\alpha(\mathfrak{p}) \le \frac{\ell e(\mathfrak{p}_z/\ell)/(\ell-1)}{e(\mathfrak{p}_z/\mathfrak{p})} - \frac{(\ell - 1 + r(e(\mathfrak{p})))/((\ell-1), e(\mathfrak{p}))}{e(\mathfrak{p}_z/\mathfrak{p})} = \frac{\ell e(\mathfrak{p})}{\ell-1} - \frac{\ell - 1 + r(e(\mathfrak{p}))}{\ell-1} ,$$

proving (2). For the first statement of (3), note that

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

Since $e(\mathfrak{p}_z/\mathfrak{p}) = (\ell-1)/(\ell-1, e(\mathfrak{p}))$, the first summand is an integer by (1), and the second also since $e(\mathfrak{p}) \equiv r(e(\mathfrak{p})) \pmod{\ell-1}$. Finally note that by the same formula, since $r(e(\mathfrak{p})) > 0$ we have $a_\alpha(\mathfrak{p}) < A_\alpha(\mathfrak{p})/e(\mathfrak{p}_z/\mathfrak{p})$, but since $r(e(\mathfrak{p})) \le \ell - 1$ we have $a_\alpha(\mathfrak{p}) \ge A_\alpha(\mathfrak{p})/e(p_z/\mathfrak{p}) - 1$, proving the second statement of (3). □

Remark 3.7. *As mentioned in* [6]*, 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 for instance .... (to be done by FT)*

After introducing all this notation and giving the main properties, the crucial theorem that we will use gives the conductor of the extension N/K:

Theorem 3.8. *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* N/K *is given as follows:*

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

Proof. This is simply a reformulation of Theorem 3.15 of [5]. Note that in the above formula we could replace $\mathfrak{p}$ by $p^{1/e(\mathfrak{p}/p)}$, which would emphasize the fact (used in the next corollary) that $f(N/K)$ comes from an ideal of the base field k. □

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*

$$a_\alpha(\mathfrak{p}) \equiv \lceil e(\mathfrak{p})/(\ell-1)\rceil \pmod 2. \tag{3.1}$$

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* D_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* D_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 C_n is equivalent to that of $D_{n/e(\mathfrak{p}_z/\mathfrak{p})}$. If $a = a_\alpha(\mathfrak{p}) = m(\mathfrak{p})$, then C_n is soluble for $n = \ell e(\mathfrak{p}_z/\ell)/(\ell-1)$, which is equivalent to $D_{m(\mathfrak{p})} = D_a$ 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 C_n for $n = A_\alpha(\mathfrak{p})$ is equivalent to that of $C_{n'}$ 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 $C_{A_\alpha(\mathfrak{p})}$ and $C_{n'}$ is equivalent to that of $D_{n''}$, 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 $e(\mathfrak{p}_z/p) = 1$ when $(\ell-1) \mid e(\mathfrak{p})$.)

Furthermore the nonsolubility of C_n for $n = A_\alpha(\mathfrak{p})+1$ is equivalent to that of $C_{n'}$ 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 $C_{A_\alpha(\mathfrak{p})+1}$ and $C_{n'}$ are equivalent to that of $D_{n''}$, where $n'' = n'/e(\mathfrak{p}_z/\mathfrak{p}) = a + h(1, a, \mathfrak{p})$, proving the lemma. □

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 $\mathcal{N}_{K/\mathbb{Q}}(f(N/K)) = \mathcal{N}_{k/\mathbb{Q}}(f(L))^{[K:k]} = \mathcal{N}_{k/\mathbb{Q}}(f(L))^2$. To avoid having both the norm from $K/\mathbb{Q}$ and from $k/\mathbb{Q}$, and to emphasize the fact that we are mainly interested in the latter, we set explicitly the following definition:

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

$$\mathcal{N}(\mathfrak{a}) = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})^{1/2} .$$

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

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 $L = K_z(\sqrt[\ell]{\alpha})^G$, 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 $\prod_{\mathfrak{p}|\ell} \mathcal{N}(\mathfrak{p})^{e(\mathfrak{p})} = p^{[K:\mathbb{Q}]}$, and writing

$$e(\mathfrak{p}) = (\lceil e(\mathfrak{p})/(\ell-1) \rceil - 1)(\ell-1) + r(e(\mathfrak{p})) ,$$

we obtain

$$(\ell-1)\Phi_\ell(K,s)=\ell^{-\frac{\ell}{\ell-1}[k:\mathbb{Q}]s}\prod_{\mathfrak{p}|\ell}\mathcal{N}(\mathfrak{p})^{-\frac{\ell-1-r(e(\mathfrak{p}))}{\ell-1}s}\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,$$

where

$$S_\alpha(s)=\sum_{\overline{u}\in S_\ell(K_z)[T]}\prod_{\substack{\mathfrak{p}|\ell\\ \mathfrak{p}\nmid\mathfrak{a}_\alpha}}\mathcal{N}(\mathfrak{p})^{\lceil a_{\alpha u}(\mathfrak{p})\rceil s}\ ,$$

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*

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

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 $\prod_{\mathfrak{p}_i|p_i}\mathcal{N}(\mathfrak{p}_i)=\mathcal{N}(p_i)^{1/e(\mathfrak{p}_i/p_i)}$, we thus have

$$S_\alpha(s)=\sum_{(a_1,\dots,a_g)\in A}\prod_{1\le i\le g}\mathcal{N}(p_i)^{\lceil a_i\rceil s/e(\mathfrak{p}_i/p_i)}\sum_{\substack{\overline{u}\in S_\ell(K_z)[T]\\ \forall i,\ a_{\alpha u}(\mathfrak{p}_i)=a_i}}1\ .$$

Remarks 4.3. *(1) Although we primarily work with prime ideals $\mathfrak{p}$ of K, in the above definitions and formulas the sums are really over the prime ideals p_i of k below them. In particular, note that Lemma 3.5 implies that $a_{\alpha u}(\overline{\mathfrak{p}_i})=a_{\alpha u}(\mathfrak{p}_i)$ when p_i is split in K/k, and it is really $\mathcal{N}(p_i)$ and* not *$\mathcal{N}(\mathfrak{p}_i)$ which occurs in the formula.*

(2) We have omitted some additional necessary conditions on the a_i, e.g., (3.1)*, but as stated the inner sum simply 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 $\mathfrak{p}_i^{b_i}=p_i^{b_i/e(\mathfrak{p}_i)/p_i}$. Inclusion-exclusion then shows that the inner sum is equal to

$$\sum_{\substack{\overline{u}\in S_\ell(K_z)[T]\\ \forall i,\ a_{\alpha u}(\mathfrak{p}_i)=a_i}}1=\sum_{(\varepsilon_1,\dots,\varepsilon_g)\in\{0,1\}^g}(-1)^{\sum_i\varepsilon_i}f_\alpha\left(\prod_{1\le i\le g}p_i^{b_i/e(\mathfrak{p}_i/p_i)}\right),$$

and for a_i satisfying the conditions described for A we have $0\le b_i\le m(\mathfrak{p}_i)$ and $b_i\in\mathbb{Z}\cup\{m(\mathfrak{p}_i)\}$.

If we let B be the set of g-uples $(b_1,\dots,b_g)$ with $0\le b_i\le m(\mathfrak{p}_i)$, $b_i\in\mathbb{Z}\cup\{m(\mathfrak{p}_i)\}$, we therefore have

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

$$v(b_i,\varepsilon_i)=b_i-h(\varepsilon_i,b_i,p_i);\ ,$$

where 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 4.4. *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 [7]) that the corresponding value for $b=0$ was mistakenly written as 0 in [6]; it must be 1, so that the corresponding factor Q is omitted from the product. □

Definition 4.5. *(1) We let $\mathcal{B}$ be the set of formal products of the form $\mathfrak{b}=\prod_{p_i|\ell} p_i^{b_i/e(\mathfrak{p}_i/p_i)}$, 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.

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

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

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 [3]

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

[3]There is an unimportant misprint in [6], 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.

We obtain

$$\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J}\frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s}=\sum_{E\subset\{p|\ell\}}\sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p|\ell,p\nmid\mathfrak{a}_\alpha\}=E}}\frac{1}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\cdot$$

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

$$=\sum_{E\subset\{p|\ell\}}\sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ p|\mathfrak{b}\Rightarrow p\in E}}\lceil\mathcal{N}\rceil\mathfrak{b}^s\prod_{p_i\in E}Q(p_i^{b_i/e(\mathfrak{p}_i/p_i)},s)\sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p|\ell,p\nmid\mathfrak{a}_\alpha\}=E}}\frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ .$$

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

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

$$=\sum_{\mathfrak{b}\in\mathcal{B}}\lceil\mathcal{N}\rceil(\mathfrak{b})^sP(\mathfrak{b},s)\sum_{\substack{E\subset\{p|\ell\}\\ p|\mathfrak{b}\Rightarrow p\in E\\ p\nmid\mathfrak{b}\text{ and }(\ell-1)|e(\mathfrak{p})\Rightarrow p\notin E}}\ \sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ \{p|\ell,\ p\nmid\mathfrak{a}_\alpha\}=E}}\frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}\ ,$$

so that

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

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

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

(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 below. 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. *With this notation we have*

$$(\mathfrak{a}_\alpha,\ell\mathbb{Z}_K)=\mathfrak{r}^e(\mathfrak{b})\ .$$

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 3.1 would imply that $e(\mathfrak{p}_z/\mathfrak{p})>1$, contradicting Corollary 2.11. □

By Corollary 2.11, we therefore have $\mathfrak{r}^e(\mathfrak{b}) \mid \mathfrak{d}_\ell$. Thus we obtain

$$\sum_{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J} \frac{S_\alpha(s)}{\mathcal{N}(\mathfrak{a}_\alpha)^s} = \sum_{\substack{\mathfrak{b}\in\mathcal{B}\\ \mathfrak{r}^e(\mathfrak{b})\mid\mathfrak{d}_\ell}} \lceil\mathcal{N}\rceil(\mathfrak{b})^s P(\mathfrak{b},s) \sum_{\substack{(\mathfrak{a}_0,\dots,\mathfrak{a}_{\ell-2})\in J\\ (\mathfrak{a}_\alpha,\ell\mathbb{Z}_K)=\mathfrak{r}^e(\mathfrak{b})}} \frac{f_\alpha(\mathfrak{b})}{\mathcal{N}(\mathfrak{a}_\alpha)^s}. \tag{4.1}$$

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. If $f_\alpha(\mathfrak{b})\neq 0$, we check that $f_\alpha(\mathfrak{b})$ counts precisely those elements $\overline{u_0}S_{\mathfrak{b}}(K_z)[T]$ for any counted $\overline{u_0}$, and hence $f_\alpha(\mathfrak{b}) = |S_{\mathfrak{b}}(K_z)[T]|$.

Now we prove that $f_\alpha(\mathfrak{b})\neq 0$ if and only if $\overline{\mathfrak{a}}\in\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$, i.e., if and only if there exist $\mathfrak{q}_1$ and $\beta_1\equiv 1 \pmod{{}^*\mathfrak{b}}$ with $\mathfrak{a}\mathfrak{q}_1^\ell = \beta_1\mathbb{Z}_{K_z}$. If there exists $\overline{u}\in S_\ell(K_z)[T]$ such that $x_0^\ell = \alpha u\beta$ for some $\beta\equiv 1 \pmod{{}^*\mathfrak{b}}$, write $u\mathbb{Z}_{K_z} = \mathfrak{q}^\ell$, and we may take $\mathfrak{q}_1 = \mathfrak{q}_0\mathfrak{q}/x_0$ and $\beta_1 = 1/\beta \equiv 1 \pmod{{}^*\mathfrak{b}}$. Conversely, if $\mathfrak{a}\mathfrak{q}_1^\ell = \beta_1\mathbb{Z}_{K_z}$ with $\beta_1\equiv 1 \pmod{{}^*\mathfrak{b}}$, then $\alpha\mathbb{Z}_{K_z} = \mathfrak{a}\mathfrak{q}_0^\ell = \beta_1(\mathfrak{q}_0/\mathfrak{q}_1)^\ell$. Thus, $u=\alpha/\beta_1$ is a virtual unit. Since $\mathfrak{a}\in(I/I^\ell)[T]$, for all $t\in T$ we have $t(\beta_1)=\gamma_t^\ell$ for some $\gamma_t\in K_z^*$, and since $\overline{\alpha}\in(K_z/K_z^{*\ell})[T]$ it follows that $t(u)$ is an ℓth power in K_z. Thus $\overline{u}\in S_\ell(K_z)[T]$, and $1^\ell\equiv\beta_1\equiv\alpha/u \pmod{{}^*\mathfrak{b}}$, so $f_\alpha(k)\neq 0$, proving the lemma. □

Note that when we assume $\overline{\mathfrak{a}}\in\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$ we have automatically $\overline{\mathfrak{a}}\in\mathrm{Cl}(K_z)^\ell$, so we only need to assume in addition that $\overline{\mathfrak{a}}\in(I(K_z)/I(K_z)^\ell)[T]$.

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 **??**, 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 [5], 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 an nontrivial theorem of Herbrand (see Theorem 2.3 of [5]), 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 [6] 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 [5], or Lemma 1.5.6 of [14]. □

For the next result, we recall the following quite nontrivial theorem, see [5] Corollary 2.8:

To do (by FT): Rewrite this theorem, and if needed also the next lemma, to specialize to the cases of K and k. The notation is for K, so I will describe what changes for k. I will do this when I go through Section 6, since the theorem is used there.

Theorem 5.4. *Let K be any number field, and let g, K_z, τ as usual. We have*

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

where

$$x(\mathfrak{p}) = \lceil v_{\mathfrak{p}}(\mathfrak{b})\rceil - \lceil (v_{\mathfrak{p}}(\mathfrak{b}) - r_0(je(\mathfrak{p})))/\ell\rceil \ ,$$

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

We will use this result for the field K and for the field k. 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 have:

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 Theorem 5.4.

Proof. Note first that we have the exact sequence of $\mathbb{F}_\ell[G]$-modules

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

Furthermore, I claim that $(\mathfrak{c}_z/\mathfrak{b}_z)[\tau_2 - 1] = (\mathfrak{c}_z \cap k_z)/(\mathfrak{b}_z \cap k_z)$. Indeed, let $x \in \mathfrak{c}_z$ and assume that $\tau_2(x) \equiv x \pmod{\mathfrak{b}_z}$, so that $\tau_2(x) = x + y$ for some $y \in \mathfrak{b}_z$. Applying τ_2 we see that $\tau_2(y) = -y$, so $\tau_2(x + y/2) = x + y + \tau_2(y)/2 = x + y/2$, and $x + y/2 \equiv x \pmod{\mathfrak{b}_z}$ (note that 2 is invertible modulo ℓ hence modulo $\mathfrak{b}$), proving my claim, and the result follows. □

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 $(\mathfrak{a}_i)$ satisfying 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, 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

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

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 [6]:

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*

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

where

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

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. Let $(\mathfrak{a}_0,\cdots,\mathfrak{a}_{\ell-2})$ satisfy condition (a) of Proposition 2.8, and set as usual $\mathfrak{a}=\prod_{0\le i\le\ell-2}\mathfrak{a}_i^{g^i}$. By the remark preceding Lemma 2.10 we have $\overline{\mathfrak{a}}\in(\mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell)[T]$. 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 we have

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

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 J' is the set of $(\ell-1)$uples of coprime squarefree ideals of K_z, satisfying condition (a) of Proposition 2.8, but now with no class group condition, so satisfying the condition of Lemma 2.10.

Assume first that we are in the general case. By this lemma we can thus 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:

- The ideal $\mathfrak{a}_0$ is a squarefree ideal of K_z such that $\tau^{(\ell-1)/2}(\mathfrak{a}_0)=\tau_2(\mathfrak{a}_0)$.
- The ideals $\mathfrak{a}_0$ and $\tau^i(\mathfrak{a}_0)$ are coprime for $(\ell-1)\nmid i$.
- 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 it is clear that the ideals $\mathfrak{a}_i=\tau^{-i}(\mathfrak{a}_0)$ are 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.
- We have $\mathcal{N}_{K_z/K}(\mathfrak{a}_0)=\mathfrak{a}_\alpha$.
- 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

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

We are of course now going to use multiplicativity. We do this in two steps: first, write again temporarily $\mathfrak{a}_0 = \mathfrak{c}\mathfrak{d}$, 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 $H(\mathfrak{b}, \chi, s) = S_c S_d$ 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

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

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 $\mathfrak{d} \neq \mathbb{Z}_{K_z}$ 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 and since $\mathfrak{b}$ is stable by τ_2 we have

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

with

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

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 $\mathcal{N}_{K_z/K}(\mathfrak{c}) = \prod_{\mathfrak{p}|p}\mathfrak{p} = \mathfrak{p}$ 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.

Assume now that we are in the special case with $\ell \equiv 1 \pmod 4$. Most of the proof in the general case applies. The definition of $H(\mathfrak{b}, \chi, s)$ is the same, and we also replace the sum over J' by a sum over ideals $\mathfrak{a}_0$ of K_z satisfying suitable conditions. The rest of the proof goes through (and is simpler since we know that p is split in K/k), and we find that the formula in the general case is also valid in the special case with $\ell \equiv 1 \pmod 4$.

Finally assume that we are in the special case with $\ell \equiv 3 \pmod 4$. Here 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. Here, as in [6], we replace this sum by a sum over pairs $(\mathfrak{a}, \mathfrak{a}_1)$ with $\mathfrak{a} = \mathfrak{a}_0\mathfrak{a}_1$, and we again find that the formula is the same. □

Note: in [6] the quantity $\chi(\mathfrak{r}^e(\mathfrak{b}))$ appears in the proof, and disappears in the result. If I am not mistaken we have in fact $\chi(\mathfrak{r}^e(\mathfrak{b})) = 1$.

As we have mentioned above, if $\ell > 2[k : \mathbb{Q}] + 1$, and in particular if $k = \mathbb{Q}$ and $\ell \geq 5$, 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 $\ell \geq 2[k : \mathbb{Q}] + 3$, for instance that $k = \mathbb{Q}$ and $\ell \geq 5$. We have*

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

where

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

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

For applications we need to specialize all the results of this paper to the case where the base field is $k = \mathbb{Q}$. From now on, we assume that $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field with discriminant D.

7.1. **Computation of $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]|$.**

Proposition 7.1. *(1) Assume that $\ell \nmid D$. Then $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]| = 1$, ℓ, and ℓ for $\mathfrak{b} = (1)$, (ℓ), or $(\ell^{\ell/(\ell-1)})$ respectively.*

(2) Assume that $\ell \mid D$ but $D \neq (-1)^{(\ell-1)/2}\ell$. Then $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]| = 1$, 1, ℓ, and ℓ for $\mathfrak{b} = (1)$, $(\sqrt{(-1)^{(\ell-1)/2}\ell})$, (ℓ), or $(\ell^{\ell/(\ell-1)})$ respectively.

(3) Assume that $D = (-1)^{(\ell-1)/2}\ell$, i.e., that we are in the special case. Then $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^{\ell})[T]| = 1$, 1, ℓ, and ℓ for the same $\mathfrak{b}$'s as in (2), except when $\ell = 3$ in which case the values are 1, 1, 1, and ℓ.

Proof. Consider Definition 4.5. The only ideal of $\mathbb{Q}$ above ℓ is of course $\ell\mathbb{Z}$, so the set $\mathcal{B}$ is the set of ℓ^b, where $0 \le b \le \ell/(\ell-1)$ and $e(\mathfrak{p}/\ell)b \in \mathbb{Z}$ if $b < \ell/(\ell-1)$. We consider three cases.

(1) Assume that $\ell \nmid D$. Here we have $\mathfrak{b} = \mathbb{Z}_K$, $\ell\mathbb{Z}_K$, or $\ell^{\ell/(\ell-1)}\mathbb{Z}_K$, and $e(\mathfrak{p}_z/\ell) = \ell - 1$. Thus, $\mathfrak{b}_z = \mathbb{Z}_{K_z}$, $\ell\mathbb{Z}_{K_z}$, or $(1-\zeta_\ell)^\ell\mathbb{Z}_{K_z}$, so $\mathfrak{c}_z = \mathbb{Z}_{K_z}$, $\mathfrak{p}_z$, or $\mathfrak{p}_z$, $\mathfrak{b}_k = \mathbb{Z}_{\mathbb{Q}_z}$, $\ell\mathbb{Z}_{\mathbb{Q}_z}$, or $(1-\zeta_\ell)^\ell\mathbb{Z}_{\mathbb{Q}_z}$, and $\mathfrak{c}_k = \mathbb{Z}_{\mathbb{Q}_z}$, $(1-\zeta_\ell)\mathbb{Z}_{\mathbb{Q}_z}$, or $(1-\zeta_\ell)\mathbb{Z}_{\mathbb{Q}_z}$, so by Theorem 5.4 $|(\mathfrak{c}_z/\mathfrak{b}_z)[\tau - g]| = 1$, ℓ^2, or ℓ^2, and $|(\mathfrak{c}_k/\mathfrak{b}_k)[\tau - g]| = 1$, ℓ, or ℓ, proving (1).

(2) Assume that $\ell \mid D$ and $K \not\subset \mathbb{Q}_z$. Here we have $\mathfrak{b} = \mathbb{Z}_K$, $\sqrt{(-1)^{(\ell-1)/2}\ell}\mathbb{Z}_K$, $\ell\mathbb{Z}_K$, or $\ell^{\ell/(\ell-1)}\mathbb{Z}_K$, and $e(\mathfrak{p}_z/\mathfrak{p}) = (\ell-1)/2$ so $e(\mathfrak{p}_z/\ell) = \ell - 1$. Note also that by Proposition 3.1, since $e(\ell)$ is odd we have $e(\mathfrak{p}_z/\mathfrak{p}_k) = e(\mathfrak{p}/p) = 2$ in this case. Thus $\mathfrak{p}_z$ is the unique ideal of K_z above ℓ and $e(\mathfrak{p}_z/\ell) = 2(\ell-1)$. We thus have $\mathfrak{b}_z = \mathbb{Z}_{K_z}$, $\mathfrak{p}_z^{\ell-1}$, $\mathfrak{p}_z^{2(\ell-1)}$, or $\mathfrak{p}_z^{2\ell}$, so $\mathfrak{c}_z = \mathbb{Z}_{K_z}$, $\mathfrak{p}_z$, $\mathfrak{p}_z^2$, or $\mathfrak{p}_z^2$, $\mathfrak{b}_k = \mathbb{Z}_{\mathbb{Q}_z}$, $(1-\zeta_\ell)^{(\ell-1)/2}\mathbb{Z}_{\mathbb{Q}_z}$, $\ell\mathbb{Z}_{\mathbb{Q}_z}$, or $(1-\zeta_\ell)^\ell\mathbb{Z}_{\mathbb{Q}_z}$, and $\mathfrak{c}_k = \mathbb{Z}_{\mathbb{Q}_z}$, $(1-\zeta_\ell)\mathbb{Z}_{\mathbb{Q}_z}$, $(1-\zeta_\ell)\mathbb{Z}_{\mathbb{Q}_z}$, or $(1-\zeta_\ell)\mathbb{Z}_{\mathbb{Q}_z}$, so by Theorem 5.4 $|(\mathfrak{c}_z/\mathfrak{b}_z)[\tau - g]| = 1$, ℓ, ℓ^2, ℓ^2, and $|(\mathfrak{c}_k/\mathfrak{b}_k)[\tau - g]| = 1$, ℓ, ℓ, or ℓ, proving (2).

(3) Assume that $D = (-1)^{(\ell-1)/2}\ell$. Here we have $T = \{\tau + g\}$, so we only need to compute $|(\mathfrak{c}_z/\mathfrak{b}_z)[\tau + g]|$, and by Theorem 2.7 of [5], since $-g = g^{(\ell+1)/2}$, this is equal to 1, ℓ, ℓ^2, or ℓ^2 respectively.

□

7.2. **Analogue of Theorem 3.2 of** [7]**.** Recall that if $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field of discriminant D, the mirror field with respect to ℓ is the degree $\ell - 1$ field $K' = \mathbb{Q}(\sqrt{D}(\zeta_\ell - \zeta_\ell^{-1}))$. The following lemma is immediate from the general results proved in the preceding sections and is left to the reader:

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

- *We have $p \in \mathcal{D}$ if and only if $p \equiv \left(\frac{D}{p}\right) \equiv \pm 1 \pmod{\ell}$, in other words $p \neq \ell$ and $p \equiv \left(\frac{D}{p}\right) \pmod{\ell}$.*
- *In the general case, this is equivalent to $e(p) = f(p) = 1$, where $e(p)$ and $f(p)$ denote the ramification and residual indexes in $K'/\mathbb{Q}$.*
- *In the special case with $\ell \equiv 1 \pmod 4$, this is equivalent to $p \equiv 1 \pmod{\ell}$.*
- *In the special case with $\ell \equiv 3 \pmod 4$, this is equivalent to $p \equiv \pm 1 \pmod{\ell}$.*

The analogue of [7] is as follows, where we assume that $\ell \neq 3$, since the case $\ell = 3$, which is slightly different, is treated in loc. cit.:

Theorem 7.3. *Assume that $\ell \ge 5$ and let $K = \mathbb{Q}(\sqrt{D})$. We have*

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

where $c_D = 1$ if $D < 0$, $c_D = \ell$ if $D > 0$, 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. We briefly explain how this follows from our previous results.

- We have $k = \mathbb{Q}$ so $\ell^{\ell/(\ell-1)[k:\mathbb{Q}]s} = \ell^{\ell s/(\ell-1)}$.
- The factor $\prod_{p|\ell} \mathcal{N}(p)^{\cdots}$ 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 factor coming from (1) this gives ℓ^{-2s} if $\ell \nmid D$ and $\ell^{-3s/2}$ if $\ell \mid D$.
- We have $\ell^{RU(K)} = \ell^{r_2(K)-r_2(k)}$ in the general case we can check from the definition of $RU(K)$ that this is also valid in the special case. Thus in all cases $\ell^{RU(K)} = \ell/c_D$ with our definition of c_D.
- By Definition 4.5, if $\ell \nmid D$ we have $\lceil \mathcal{N} \rceil(\mathfrak{b}) = (1, *, \ell, \ell^2)$, while if $\ell \mid D$ we have $\lceil \mathcal{N} \rceil(\mathfrak{b}) = (1, \ell^{1/2}, \ell, \ell^{3/2})$ for $\mathfrak{b} = ((1), (\sqrt{(-1)^{(\ell-1)/2}\ell}), (\ell), (\ell^{\ell/(\ell-1)}))$, using the convention of Definition 4.1.
- 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 Definition 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 4.4 and the definition of $P(\mathfrak{b}, s)$, when $\ell \nmid D$ we have $P(\mathfrak{b}, s) = (1, *, -\ell^{-s}, 1)$, and when $\ell \mid D$ we have $P(\mathfrak{b}, s) = (1, 1 - \ell^{-s/2}, -\ell^{-s/2}, 1)$ respectively for the usual sequence of $\mathfrak{b}$.
- By Proposition 7.1, when $\ell \nmid D$ we have $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]| = (1, *, \ell, \ell)$, and when $\ell \mid D$ we have $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]| = (1, 1, \ell, \ell)$ respectively. Note that if $\ell = 3$ (which we exclude) and $\ell \mid D$ we have instead $|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^\ell)[T]| = (1, 1, 1, \ell)$ respectively.

□

Corollary 7.4. *Assume that $\ell \geq 5$ and let $r_2(D) = 1$ for $D < 0$ and $r_2(D) = 0$ for $D > 0$ be the number of complex places of $K = \mathbb{Q}(\sqrt{D})$. There exists a function $\phi_D(s) = \phi_{D,\ell}(s)$, holomorphic for $\Re(s) > 1/2$, such that*

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

where

$$L_\ell(s) = \begin{cases} 1 + \dfrac{\ell - 1}{\ell^{2s}} & \text{if } \ell \nmid D, \\ 1 + \dfrac{\ell - 1}{\ell^s} & \text{if } \ell \mid D. \end{cases}$$

Proof. Same as in [6]: $\phi_D(s)$ is the contribution of the nontrivial characters, and the other term is the contribution of the trivial characters. □

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, we have

$$M_\ell(D;X) = C_\ell(D)X + O(X^{1-1/\ell+\varepsilon})$$

for any $\varepsilon > 0$, with $C_\ell(D) = c_1(\ell)c_2(\ell)c_3(\ell)$, where $c_3(\ell)$ is given by one of the following two equivalent formulas:

$$\begin{aligned}
c_3(\ell) &= \mathrm{Res}_{s=1} \prod_{e(p)=f(p)=1} (1+(\ell-1)/p^s) = c_4(\ell)c_5(\ell)c_6(\ell)c_7(\ell)\ , \quad \textit{with}\\
c_4(\ell) &= \mathrm{Res}_{s=1}\zeta_{K'}(s)\ , \quad c_5(\ell) = \prod_{p\mid \ell D}(1-1/p^{f(p)})^{g(p)}\ ,\\
c_6(\ell) &= \prod_{e(p)=f(p)=1} \left((1+(\ell-1)/p)(1-1/p)^{(\ell-1)}\right)\ , \quad \textit{and}\\
c_7(\ell) &= \prod_{e(p)=1,\ f(p)>1} (1-1/p^{f(p)})^{(\ell-1)/f(p)}\ ,
\end{aligned}$$

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

(2) In the special case with $\ell \equiv 1 \pmod 4$ we have

$$M_\ell(D;X) = C_\ell(D)X + O(X^{1-1/\ell+\varepsilon})$$

for any $\varepsilon > 0$, with $C_\ell(D) = c_1(\ell)c_2(\ell)c_3(\ell)$, where $c_3(\ell)$ is given by one of the following two equivalent formulas:

$$\begin{aligned}
c_3(\ell) &= \mathrm{Res}_{s=1} \prod_{p\equiv 1 \pmod \ell} (1+(\ell-1)/p^s) = c_4(\ell)c_5(\ell)c_6(\ell)c_7(\ell)\ , \quad \textit{with}\\
c_4(\ell) &= \mathrm{Res}_{s=1}\zeta_{\mathbb{Q}_z}(s)\ , \quad c_5(\ell) = 1-1/\ell\ ,\\
c_6(\ell) &= \prod_{p\equiv 1 \pmod \ell} \left((1+(\ell-1)/p)(1-1/p)^{(\ell-1)}\right)\ , \quad \textit{and}\\
c_7(\ell) &= \prod_{p\not\equiv 0,1 \pmod \ell} (1-1/p^{f(p)})^{(\ell-1)/f(p)}\ ,
\end{aligned}$$

where $f(p)$ is the residual index of $\mathfrak{p}_z/p$ in $\mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$.

(3) In the special case with $\ell \equiv 3 \pmod 4$ we have

$$M_\ell(D;X) = C_\ell(D)(X\log(X) + C'_\ell(D)) + O(X^{1-1/\ell+\varepsilon})$$

for any $\varepsilon > 0$, with $C_\ell(D) = c_1(\ell)c_2(\ell)c_3(\ell)$, where $c_3(\ell)$ is given by one of the following two equivalent formulas:

$$c_3(\ell) = \lim_{s\to 1^+}(s-1)^2 \prod_{p\equiv\pm1 \pmod{\ell}} (1+(\ell-1)/p^s) = c_4(\ell)c_5(\ell)c_6(\ell)c_7(\ell)\ , \quad \textit{with}$$

$$c_4(\ell) = (\mathrm{Res}_{s=1}\zeta_{\mathbb{Q}_z^+}(s))^2\ , \quad c_5(\ell) = (1-1/\ell)^2\ ,$$

$$c_6(\ell) = \prod_{p\equiv\pm1 \pmod{\ell}} \left((1+(\ell-1)/p)(1-1/p)^{(\ell-1)}\right)\ , \quad \textit{and}$$

$$c_7(\ell) = \prod_{p\not\equiv0,\pm1 \pmod{\ell}} (1-1/p^{f(p)})^{(\ell-1)/f(p)}\ ,$$

where $\mathbb{Q}_z^+$ is the totally real subfield of $\mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$, $f(p)$ is the residual index of $\mathfrak{p}_z^+/p$ in $\mathbb{Q}_z^+$, and $C'_\ell(D)$ can also be given explicitly if desired.

Proof. In the general case, using the same proof as in [6], we see that the result follows, with $C_\ell(D)$ equal to the residue at $s=1$ of $\Phi_\ell(K,s)$, which we need to compute. This residue is equal to $L_\ell(1)/((\ell-1)\ell^{1-r_2(D)})R(1)$, where $L_\ell(1) = (\ell^2+\ell-1)/\ell^2$ if $\ell\nmid D$ and $L_\ell(1) = 1-1/\ell$ if $\ell \mid D$, and $R(1)$ is the residue at $s=1$ of $Z(s) = \prod_{e(p)=f(p)=1}(1+(\ell-1)/p^s)$, proving the first formula for $c_3(\ell)$. Note that since we assume that $\ell\ge5$, the condition $e(p)=f(p)=1$ implies that $p\ne\ell$, otherwise it must simply be added. Now

$$\frac{Z(s)}{\zeta_{K'}(s)} = \prod_{e(p)>1}(1-1/p^{f(p)s})^{g(p)} \prod_{e(p)=f(p)=1}(1+(\ell-1)/p^s)(1-1/p^s)^{\ell-1} \prod_{e(p)=1,\ f(p)>1}(1-1/p^{f(p)s})^{(\ell-1)/f(p)}\ ,$$

so we deduce that

$$R(1) = \mathrm{Res}_{s=1}\zeta_{K'}(s)c_5(\ell)c_6(\ell)c_7(\ell)$$

with $c_5(\ell)$, $c_6(\ell)$, and $c_7(\ell)$ as above.

Furthermore, it is immediate to check (in our context where we assume that $[K_z:K] = \ell-1$), that $\mathrm{Disc}(K')$ is given as follows:

$$\mathrm{Disc}(K') = \begin{cases} \ell^{\ell-2}(-D)^{(\ell-1)/2} & \text{when } \ell\nmid D\ , \\ \ell^{\ell-2}(-D/\ell)^{(\ell-1)/2} & \text{when } \ell\mid D \text{ and } \ell\equiv1 \pmod 4\ , \\ \ell^{\ell-3}(-D/\ell)^{(\ell-1)/2} & \text{when } \ell\mid D \text{ and } \ell\equiv3 \pmod 4\ . \end{cases}$$

In particular, $e(p)>1$ if and only if $p\mid D\ell$, with the exception of $\ell=3$ and $3\mid D$, which we exclude since we assume $\ell\ge5$.

The proof in the special case is similar and left to the reader. Note the marked difference in the asymptotics when $\ell\equiv1 \pmod 4$ and $\ell\equiv3 \pmod 4$. □

In a separate paper, we will explain how to compute the constants $c_i(\ell)$ to high accuracy for reasonably small values of $|D|$. For now, note the following: $c_1(\ell)$ and $c_2(\ell)$ are trivial, $c_4(\ell)$ is given by Dirichlet's class number formula, and $c_5(\ell)$ is a finite product. On the other hand $c_6(\ell)$ and $c_7(\ell)$ are infinite products of quantities of the type $1+O(1/p^2)$, so are convergent, but quite slowly, although they can be used to compute 7 or 8 decimal digits. In the separate paper mentioned above, we will see that to compute $c_3(\ell)$ to high accuracy, 100 decimal digits, say, we will use the first formula, and we will give large tables.

Examples. Here we only give a few values of $C_\ell(D)$, including the special cases:

$$C_3(-3) = 0.06690773330137837129184 16\cdots, \quad C_3(-4) = 0.13621906762412128414498 67\cdots,$$
$$C_3(-7) = 0.15334595465287062305345 32\cdots, \quad C_3(5) = 0.08188400744596363582320 37\cdots,$$
$$C_3(8) = 0.06977943259820586455859 30\cdots, \quad C_3(12) = 0.08038289770565540456224 05\cdots,$$
$$C_5(-3) = 0.05078532444978009937820 16\cdots, \quad C_5(-4) = 0.05337790516311959812206 55\cdots,$$
$$C_5(-7) = 0.06465347505231857105984 35\cdots, \quad C_5(5) = 0.02037818705590371465589 36\cdots,$$
$$C_5(8) = 0.01347477474759191404378 63\cdots, \quad C_5(12) = 0.01547775565944279761141 20\cdots,$$
$$C_7(-3) = 0.02963321632473007452472 19\cdots, \quad C_7(-4) = 0.02925825266997578403651 46\cdots,$$
$$C_7(-7) = 0.01210526342145122980185 79\cdots, \quad C_7(5) = 0.00646767332647141002590 68\cdots,$$
$$C_7(8) = 0.00574549743302454817258 06\cdots, \quad C_7(12) = 0.00350788649474193309189 74\cdots.$$

The formula of Corollary 7.5 suggests that the following conjecture should be true:

Conjecture 1. *Let $M_\ell^-(X)$ (resp., $M_\ell^+(X)$) be the number of degree ℓ fields L with Galois group D_ℓ and imaginary quadratic (resp., real quadratic) resolvent, with $|\mathrm{Disc}(L)| \le X$. There exists a strictly positive constant C_ℓ such that as $X \to \infty$*

$$M_\ell^-(X) \sim C_\ell X^{2/(\ell-1)} \quad \text{and} \quad M_\ell^+(X) \sim \frac{C_\ell}{\ell} X^{2/(\ell-1)}\ .$$

By the Davenport–Heilbronn theorem, this conjecture is true for $\ell = 3$ with $C_3 = 1/(4\zeta(3))$. One can of course wonder whether all the constants C_ℓ are given by an Euler product, or even as rational multiples of $1/\zeta(\ell)$, but the convergence of sequences giving C_ℓ (even for $\ell = 3$) is so slow that it is impossible to make any reasonable guess.

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

Even though the quantities $|G_{\mathfrak{b}}|$ have disappeared from our final formula (except of course that we sum on characters of $G_{\mathfrak{b}}$), it is useful to study them. Note that this was not done in [6]. I am indebted to Hendrik Lenstra for help in this section.

First note the following:

Proposition 8.1. *Recall the notation used above. In particular, let $N_z = K_z(\sqrt[\ell]{\alpha})$, and let $\mathfrak{b} = \mathbb{Z}_{K_z}$, $(1-\zeta_\ell)^{(\ell-1)/2}\mathbb{Z}_{K_z}$ (only when $\ell \mid D$), $(1-\zeta_\ell)^{\ell-1}\mathbb{Z}_{K_z} = \ell\mathbb{Z}_{K_z}$, or $(1-\zeta_\ell)^{\ell}\mathbb{Z}_{K_z}$ as above. Then $\mathfrak{f}(N_z/K_z) \mid \mathfrak{b}$ if and only if $\overline{\alpha} \in S_{\mathfrak{b}^*}(K_z)$, where $\mathfrak{b}^* = (1-\zeta_\ell)^\ell/\mathfrak{b}$ (see Definition 4.9).*

Proof. This is very classical, and essentially due to Kummer and Hecke: for instance, by Theorem 3.7 of [5] we have

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

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 $\overline{\alpha} \in S_{\mathfrak{b}^*}(K_z)$. □

Corollary 8.2. *Recall that $G = \mathrm{Gal}(K_z/\mathbb{Q})$, and for simplicity of notation set $C_{\mathfrak{b}} = \mathrm{Cl}_{\mathfrak{b}}(K_z)/\mathrm{Cl}_{\mathfrak{b}}(K_z)^\ell$. There exists a perfect pairing of $\mathbb{F}_\ell[G]$-modules*

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

where of course as usual $\boldsymbol{\mu}_\ell$ is the group of ℓth roots of unity.

Proof. This is simply the Kummer pairing: let M/K_z be the Abelian ℓ-extension corresponding by class field theory to $C_{\mathfrak{b}}$, so with conductor $\mathfrak{b}$. If $\overline{\mathfrak{a}} \in C_{\mathfrak{b}}$, we denote as usual by $\sigma_{\mathfrak{a}} \in \mathrm{Gal}(M/K_z)$ the image of $\mathfrak{a}$ under the Artin map. Thus, by the above proposition, if $\overline{\alpha} \in S_{\mathfrak{b}^*}(K_z)$ and α is any lift, we have $K_z(\sqrt[\ell]{\alpha}) \subset M$, and we define the pairing by

$$(\overline{\mathfrak{a}}, \overline{\alpha}) \mapsto \sigma_{\mathfrak{a}}(\sqrt[\ell]{\alpha})/\sqrt[\ell]{\alpha} \in \boldsymbol{\mu}_\ell \ ,$$

which does not depend on any choice of representatives. It is classical and immediate that this is a perfect pairing. □

Corollary 8.3. *Recall that $G_{\mathfrak{b}} = C_{\mathfrak{b}}[T]$. 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 $T^* = \{\tau + 1\}$.*

(1) We have a perfect pairing

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

(2) In particular, we have a canonical isomorphism

$$G_{\mathfrak{b}} \simeq \mathrm{Hom}(S_{\mathfrak{b}^*}(K_z)[T^*], \boldsymbol{\mu}_\ell) \ .$$

Proof. It is clear that the pairing of the preceding corollary is G-equivariant, i.e., that for any $\tau_1 \in G$ we have $< \tau_1(\overline{\mathfrak{a}}), \tau_1(\overline{\alpha}) >= \tau_1(< \overline{\mathfrak{a}}, \overline{\alpha} >)$. Since τ sends ζ_ℓ to ζ_ℓ^g, it follows that for any j we have a perfect pairing

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

Assume first that we are in the general case. Applying this to $j = 1$ gives a perfect pairing between $C_{\mathfrak{b}}[\tau - g]$ and $S_{\mathfrak{b}^*}(K_z)[\tau - 1]$, and similarly, since τ_2 leaves ζ_ℓ fixed, we obtain a perfect pairing between $G_{\mathfrak{b}} = C_{\mathfrak{b}}[\tau - g, \tau_2 + 1]$ and $S_{\mathfrak{b}^*}(K_z)[\tau - 1, \tau_2 + 1]$.

Assume now that we are in the special case. Applying the above formula to $j = (\ell + 1)/2$ (since $g^{(\ell+1)/2} \equiv -g \pmod{\ell}$) gives a perfect pairing between $G_{\mathfrak{b}} = C_{\mathfrak{b}}[\tau + g]$ and $S_{\mathfrak{b}^*}(K_z)[\tau + 1]$, proving (1), and (2) is of course an immediate consequence of the definition of a perfect pairing. □

As mentioned in the proof, if $\varepsilon = \pm 1$ then in the general case we have that more generally $C_{\mathfrak{b}}[\tau - g^j, \tau_2 + \varepsilon]$ pairs with $S_{\mathfrak{b}^*}(K_z)[\tau - g^{1-j}, \tau_2 + \varepsilon]$.

Proposition 8.4. *(1) In the general case we have $S_{\mathfrak{b}^*}(K_z)[T^*] \simeq S_{\mathfrak{b}^* \cap K}(K)$.*

(2) Assume that we are in the special case and that $\ell \geq 5$ is such that $\ell \equiv 3 \pmod 4$ and ℓ does not divide the numerator of the Bernoulli number $B_{(\ell+1)/2}$. Then $S_{\mathfrak{b}^*}(K_z)[T^*] = \{1\}$ for all $\mathfrak{b}$.

(3) Assume that we are in the special case, that $\ell \equiv 1 \pmod 4$ and ℓ is a regular prime. Then $S_{\mathfrak{b}^*}(K_z)[T^*] = \{1\}$ if $\mathfrak{b} = \mathbb{Z}_{K_z}$ or $\mathfrak{b} = (1 - \zeta_\ell)^{(\ell-1)/2}\mathbb{Z}_{K_z}$, and $|S_{\mathfrak{b}^*}(K_z)[T^*]| = \ell$ if $\mathfrak{b} = (1 - \zeta_\ell)^{(\ell-1)}\mathbb{Z}_{K_z}$ or $\mathfrak{b} = (1 - \zeta_\ell)^{\ell}\mathbb{Z}_{K_z}$.

Proof. (1). Assume first that we are in the general case. I first claim that $S_{\mathfrak{b}^*}(K_z)[\tau - 1] \simeq S_{\mathfrak{b}^* \cap K}(K)$. Indeed, we have an evident map from $S_{\mathfrak{b}^* \cap K}(K)$ to $S_{\mathfrak{b}^*}(K_z)[\tau - 1]$ coming from the inclusion of K into K_z, and this map is injective since if $\alpha \in K$ is an ℓth power in K_z, it is necessarily an ℓth power in K since $[K_z : K] = \ell - 1$ is coprime to ℓ. It is also surjective: if $\alpha \in K_z$ is a virtual unit such that $\tau(\alpha)/\alpha = \gamma^\ell$ for some $\gamma \in K_z$ and $x^\ell/\alpha \equiv 1 \pmod{\mathfrak{b}^*}$ is soluble, then $\mathcal{N}_{K_z/K}(\gamma)^\ell = 1$, hence $\mathcal{N}_{K_z/K}(\gamma) = 1$ (since $\zeta_\ell \notin K$), so by Hilbert 90 applied to the cyclic extension K_z/K there exists $\beta \in K_z$ with $\gamma = \beta/\tau(\beta)$, hence $\tau(\alpha\beta^\ell)/(\alpha\beta^\ell) = 1$, so $a = \alpha\beta^\ell$ is a virtual unit of K_z equivalent to α in $S_{\mathfrak{b}^*}(K_z)$ which in fact belongs to K, and again since $[K_z : K]$

is coprime to ℓ we deduce that it is a virtual unit of K, and the solubility of $x^\ell/a \equiv 1 \pmod{\mathfrak{b}^* \cap K}$ is true for the same reason, proving my claim.

It follows that $S_{\mathfrak{b}^*}(K_z)[\tau-1,\tau_2+1]$ is canonically isomorphic to $S_{\mathfrak{b}^*\cap K}(K)[\tau_2+1]$. Now I claim that we have

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

Indeed, if $\alpha \in S_{\mathfrak{b}^*\cap K}(K)$ then we have the identity

$$\alpha = (\alpha/\tau_2(\alpha))^{(\ell+1)/2}(\alpha\tau_2(\alpha))^{(\ell+1)/2}\alpha^{-\ell} \ ,$$

and the first factor belongs to $S_{\mathfrak{b}^*\cap K}(K)[\tau_2+1]$ and the second to $S_{\mathfrak{b}^*\cap K}(K)[\tau_2-1]$, since $\mathfrak{b}^* \cap K$ is stable by τ_2. Furthermore, if $\alpha\tau_2(\alpha) = \beta_1^\ell$ and $\alpha/\tau_2(\alpha) = \beta_2^\ell$ then $\alpha^2 = (\beta_1\beta_2)^\ell$, so α is itself an ℓth power, proving my claim.

Finally, I claim that $S_\ell(K)[\tau_2-1]$ is the trivial group, hence a fortiori all the groups $S_{\mathfrak{b}^*\cap K}[\tau-1]$: let $\alpha \in K$ such that $\tau_2(\alpha) = \alpha\gamma^\ell$ for some $\gamma \in K$. Applying τ_2 again we deduce that $(\gamma\tau_2(\gamma))^\ell = 1$, hence that $\gamma\tau_2(\gamma) = 1$, so by a trivial version of Hilbert 90 we deduce that $\gamma = \tau_2(\beta)/\beta$ for some $\beta \in K$, hence that $\tau_2(\alpha/\beta^\ell) = \alpha/\beta^\ell$. Thus α/β^ℓ is a virtual unit of $\mathbb{Q}$ equivalent to α, and the result follows since $S_\ell(\mathbb{Q})$ is trivial for ℓ odd, finishing the proof of (1).

(2) and (3). Assume now that we are in the special case, so that $K_z = \mathbb{Q}_z = \mathbb{Q}(\zeta_\ell)$. If $\ell \equiv 3 \pmod 4$ and $v_\ell(B_{(\ell+1)/2}) = 0$ then by another result of Herbrand, this implies that $(\mathrm{Cl}(K_z)/\mathrm{Cl}(K_z)^\ell)[\tau+1] = \{0\}$, and of course the same is true by definition if $\ell \equiv 1 \pmod 4$ and ℓ is a regular prime. Thus $S_\ell(K_z) \simeq U(K_z)/U(K_z)^\ell$ and $S_\ell(K_z)[T^*] \simeq (U(K_z)/U(K_z)^\ell)[\tau - g^{(\ell-1)/2}]$. By the theorem of Herbrand on units mentioned above (Theorem 2.3 of [5]), we deduce that $S_\ell(K_z)[T^*]$ is trivial if $(\ell-1)/2$ is odd and >1, i.e., if $\ell \equiv 3 \pmod 4$, $\ell \neq 3$, and otherwise that it is an $\mathbb{F}_\ell$-vector space of dimension 1. It is then easy to check (**to be done**) that if ε is an $\mathbb{F}_\ell$-generator, $x^\ell \equiv \varepsilon \pmod{\ell\mathbb{Z}_{K_z}}$ is not solvable while $x^\ell \equiv \varepsilon \pmod{\sqrt{\ell^*}\mathbb{Z}_{K_z}}$ is solvable, proving (2) and (3). □

Remarks 8.5. *(1) Since we are studying degree ℓ extensions, the restrictions on ℓ are not very serious. In fact, for $\ell \equiv 3 \pmod 4$ I do not know of any example where ℓ divides the numerator of $B_{(\ell+1)/2}$, but on probabilistic grounds infinitely may such examples should exist.*

(2) Evidently we could extend the above proposition to all primes ℓ if really necessary.

(3) Note that for $\ell \equiv 3 \pmod 4$ we simply use Herbrand's theorem. Ribet proved the much deeper fact that the converse is true, i.e., that if $(\mathrm{Cl}(K_z)/\mathrm{Cl}(K_z)^\ell)[\tau+1] = \{0\}$ then ℓ divides the numerator of $B_{(\ell+1)/2}$, and much more general results, but we do not need this. Note that this is a special case of the main conjecture of Iwasawa theory, proved by Mazur–Wiles.

Lemma 8.6. *(1) Assume that $\ell \nmid D$. For $\mathfrak{b} = \mathbb{Z}_{K_z}$, $(1-\zeta_\ell)^{\ell-1}\mathbb{Z}_{K_z} = \ell\mathbb{Z}_{K_z}$, or $(1-\zeta_\ell)^\ell\mathbb{Z}_{K_z}$, we have $\mathfrak{b}^* \cap K = \ell^2\mathbb{Z}_K$, $\ell\mathbb{Z}_K$, or $\mathbb{Z}_K$ respectively.*

(2) Assume that $\ell \mid D$, that we are in the general case, and write $\ell\mathbb{Z}_K = \mathfrak{p}_\ell^2$. For $\mathfrak{b} = \mathbb{Z}_{K_z}$, $(1-\zeta_\ell)^{(\ell-1)/2}\mathbb{Z}_{K_z}$, $(1-\zeta_\ell)^{\ell-1}\mathbb{Z}_{K_z} = \ell\mathbb{Z}_{K_z}$, or $(1-\zeta_\ell)^\ell\mathbb{Z}_{K_z}$, we have $\mathfrak{b}^* \cap K = \mathfrak{p}_\ell^3$, $\mathfrak{p}_\ell^2$, $\mathfrak{p}_\ell$, or $\mathbb{Z}_K$ respectively.

Proof. Immediate. □

Corollary 8.7. *Assume that we are in the general case.*

(1) We have a canonical isomorphim $G_\mathfrak{b} \simeq \mathrm{Hom}(S_{\mathfrak{b}^*\cap K}(K), \boldsymbol{\mu}_\ell)$.

(2) In particular

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

where

$$z(\mathfrak{b}) = \begin{cases} 2 & \text{if } \mathfrak{b} = \mathbb{Z}_{K_z}\ , \\ 1 & \text{if } \ell \mid D,\ \mathfrak{b} \neq \mathbb{Z}_{K_z}, \text{ and } \mathfrak{b} \neq (1-\zeta_\ell)^\ell \mathbb{Z}_{K_z}\ , \\ 0 & \text{if } \ell \nmid D \text{ and } \mathfrak{b} \neq \mathbb{Z}_{K_z} \text{ or if } \mathfrak{b} = (1-\zeta_\ell)^\ell \mathbb{Z}_{K_z}\ . \end{cases}$$

(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) follows from the above computations. In particular $|G_\mathfrak{b}| = |S_{\mathfrak{b}^* \cap K}(K)|$. Now, from the two exact sequences given above involving $S_\mathfrak{b}(K)$ and $S_\ell(K)$, and since $\dim_{\mathbb{F}_\ell}(U(K)/U(K)^\ell) = 1 - r_2(D)$, it is easily shown that for any ideal $\mathfrak{b}_1$ of K we have

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

where $Z_{\mathfrak{b}_1} = (\mathbb{Z}_K/\mathfrak{b}_1)^*$. Applying this to $\mathfrak{b}_1 = \mathfrak{b}^* \cap K$ gives the formula of (2) with $z(\mathfrak{b}) = \dim_{\mathbb{F}_\ell}(Z_{\mathfrak{b}_1}/Z_{\mathfrak{b}_1}^\ell)$. Using the formula for $\mathfrak{b}_1$ given in Lemma 8.6 implies the given formula for $z(\mathfrak{b})$. □

Note that (3) is a generalization of Proposition 7.7 of [6].

Corollary 8.8. *Assume that we are in the special case and that $\ell \geq 5$.*

(1) If $\ell \equiv 3 \pmod 4$ and ℓ does not divide the numerator of $B_{(\ell+1)/2}$ then $G_\mathfrak{b}$ is trivial for all $\mathfrak{b}$.

(2) If $\ell \equiv 1 \pmod 4$ and ℓ is a regular prime then $G_\mathfrak{b}$ is trivial if $\mathfrak{b} = \mathbb{Z}_{K_z}$ or $\mathfrak{b} = \sqrt{\ell^*}\mathbb{Z}_{K_z}$, while $|G_\mathfrak{b}| = \ell$ if $\mathfrak{b} = \ell\mathbb{Z}_{K_z}$ or $\mathfrak{b} = (1-\zeta_\ell)^\ell \mathbb{Z}_{K_z}$.

Note that the condition that $G_\mathfrak{b}$ is trivial for all $\mathfrak{b}$ implies that the "remainder term" $\phi_D(s)$ vanishes identically.

Corollary 8.9. *Assume that $\ell \geq 5$ and $D < 0$, and that either we are in the general case and $\ell \nmid h(D)$, or we are in the special case (hence $\ell \equiv 3 \pmod 4$), $\ell > 3$, and ℓ does not divide the numerator of $B_{(\ell+1)/2}$. 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 because of the possible nontriviality of $\mathfrak{r}^e(\mathfrak{b})$ when $\ell = 3$ it is necessary in that case to distinguish between $D \equiv 3$ and $D \equiv 6 \pmod 9$, but for $\ell > 3$ this is not necessary.

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

As we have done in [7], we must now transform the sum over characters of $G_{\mathfrak{b}} = (\mathrm{Cl}_{\mathfrak{b}}/\mathrm{Cl}_{\mathfrak{b}}^{\ell})[T]$ into more explicit objects. We first give two examples, the first one proved in [6], and the second to be proved, in the special case:

Examples in the special case:

For $\ell = 3$ (corresponding to pure cubic fields):

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

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 $p\equiv\pm1 \pmod 9$.

For $\ell = 5$:

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

where E is the quintic field defined by $x^5+5x^3+5x-1=0$ (discriminant 5^7, Galois group $C_5\rtimes C_4$), and

$$\omega_E(p)=\begin{cases}-1 & \text{if } p \text{ is inert or totally ramified in } E\ ,\\ 4 & \text{if } p \text{ is totally split in } E\ ,\\ 0 & \text{otherwise.}\end{cases}$$

Recall also that for $\ell\equiv 3 \pmod 4$, $\ell>3$, we have only the main term and no extra term.

For $\ell\equiv 1 \pmod 4$, generalizing the above example we have the following:

Proposition 9.1. *Assume that $\ell\equiv 1 \pmod 4$, let ε be a fundamental unit of $\mathbb{Q}(\sqrt{\ell})$, and let*

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

be the characteristic polynomial of $\zeta_\ell-\zeta_\ell^{-1}$. Then if ℓ is a regular prime 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 degree ℓ defined by $xP(x)-\mathrm{Tr}(\varepsilon)=0$ (discriminant $\ell^{(3\ell-1)/2}$, Galois group $C_\ell\rtimes(\mathbb{Z}/\ell\mathbb{Z})^*$), and

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

Proof. **To be done.**

□

References

[1] 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.

[2] M. Bhargava, *Higher Composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886.

[3] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Math. **193**, Springer-Verlag, New York, 1999.

[4] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Cyclotomic extensions of number fields*, Indag. Math. **14** (2003), 183–196.

[5] 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.

[6] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[7] H. Cohen and F. Thorne, *Dirichlet Series Associated to Cubic Fields with Given Quadratic Resolvent*, preprint.

[8] 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.

[9] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree (English translation)*, AMS, Providence, 1964.

[10] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York, 2004.

[11] G. Gras, *Class Field Theory*, Springer Monographs in Math. (2005).

[12] G. Gras, *Théorèmes de Réflexion*, J. Th. Nombres Bordeaux **10** (1998), 399–499.

[13] Y. Kishi, *The Spiegelungssatz for $p = 5$ from a constructive approach*, Math. J. Okayama Univ. **47** (2005), 1–27.

[14] A. Morra, *Comptage asymptotique et algorithmique dextensions cubiques relatives* (in English), thesis, Université Bordeaux I, 2009. Available online at `http://perso.univ-rennes1.fr/anna.morra/these.pdf`.

[15] L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1996.

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`