Idélic Approach in Enumerating Heisenberg Extensions

July 6, 2022

Abstract

For odd primes ℓ and number fields k, we study the asymptotic distribution of number fields L/k given as a tower of relative cyclic C_ℓ-extensions $L/F/k$ using the idélic approach of class field theory. This involves a classification for the Galois group of L/k based on local conditions on L/F and F/k, and an extension of the method of Wright in enumerating abelian extensions. We call the possible Galois groups for these extensions generalized and twisted Heisenberg groups. We then prove the strong Malle–conjecture for all these groups in their representation on ℓ^2 points.

Key words. Malle's conjecture, Heisenberg group, class field theory, distribution of number fields, local-global principle

1 Introduction

Let $G \leq S_n$ be a finite transitive permutation group and k be a number field. We say that a finite extension L/k with $[L : k] = n$ has Galois group $G = \mathrm{Gal}(L/k)$ if the normal closure $\tilde{L}$ has Galois group G as an abstract group, and the permutation action of G on the n embeddings of L into the algebraic closure $\bar{k}$ is isomorphic to G as a permutation group.

We define $N_k(G, X)$ to be the number of isomorphism classes of extensions L/k inside some fixed algebraic closure of k with $\mathrm{Gal}(L/k) = G$ and norm of the discriminant $\mathrm{Disc}(L/k) = \mathcal{N}_{k/\mathbb{Q}}(d_{L/k})$ bounded above by X. Gunter Malle has proposed a precise conjecture about the asymptotic behavior of the function $N_k(G, X)$ for $X \to \infty$.

Conjecture 1 ([24, 25])**.** *For all number fields k and all transitive permutation groups $G \leq S_n$ there exists a constant $c(G, k) > 0$ such that*

$$N_k(G, X) \sim c(k, G)x^{1/a(G)} \log(x)^{b(G,k)-1},$$

where $a(G)$ and $b(G, k)$ are both positive integers depending on k and G.

In this conjecture, Malle also gives a precise prediction for $a(G)$ and $b(k, G)$ [24, 25]. Please see Section 2.2 for a detailed introduction of those constants.

Malle's conjecture has been proven for abelian extensions over $\mathbb{Q}$ [23, 35]. For non-abelian groups, the first case is S_3 cubic fields proved by Davenport and Heilbronn and by Datskovsky and Wright over general number fields [14, 13]. Bhargava proved this conjecture for S_4 quartic fields and S_5 quintic fields in his ground breaking work [7, 8]. Later this was generalized to general base fields by Bhargava, Shankar and Wang [9]. Bhargava and Wood [10] and Belabas and Fouvry [6] independently proved the conjecture for S_3 sextic fields. The case of D_4 quartic

fields is proved by Cohen, Diaz y Diaz and Olivier [12]. It was generalized by Klüners to wreath products of the form $C_2 \wr H$ [18] under mild conditions on H. Masri, Thorne, Tsai and Wang [32, 26] proved this conjecture for groups of the form of $S_n \times A$ for abelian groups A and $n = 3, 4, 5$. Recent work of Fouvry and Koymans proves this conjecture for nonic Heisenberg extensions [15]. Koymans and Pagano [22] prove the conjecture for a family of Galois nilpotent extensions where the minimal index elements (see Section 2.2 for the definition) are central.

We also mention that there have been series of papers on proving the $a(G)$-constant in Conjecture 1, see e.g. [20, 1, 21, 19, 22], and variations of field counting questions for more general invariants [5, 34]. Klüners [17] has observed that the predicted $b(G, k)$-constant is not correct in general.

In this paper, our main goal is to prove Conjecture 1 for Galois groups that we call *generalized Heisenberg group* $H(\ell, d)$ and *twisted Heisenberg group* $\tilde{H}(\ell, d)$, see Section 2.1 for more details.

Theorem 1.1. *Let ℓ be an odd prime number and k be an arbitrary number field. Conjecture 1 is true for $G = H(\ell, d) \leq S_{\ell^2}$ and $\tilde{G} = \tilde{H}(\ell, d) \leq S_{\ell^2}$ for every $1 < d < \ell$.*

The groups $H(\ell, d)$ and $\tilde{H}(\ell, d)$ for $1 \leq d \leq \ell$ are exactly the possible Galois groups $\mathrm{Gal}(L/k)$ when L/F is a relative C_ℓ-extension over a C_ℓ-extension F/k. Theorem 1.1 covers all cases when $\mathrm{Gal}(L/k)$ is not the direct product $C_\ell \times C_\ell$, the abelian group C_{ℓ^2} and the wreath product $C_\ell \wr C_\ell$ (which are $H(\ell, 1)$, $\tilde{H}(\ell, 1)$ and $H(\ell, \ell)$ in our classification). In particular, all cases addressed in Theorem 1.1 are not Galois. We remark that the degree 9 Heisenberg group, $H(3, 2) \leq S_9$, is also proved in [15] for $k = \mathbb{Q}$, but with a different approach from ours. They also compute the constant $c(G, \mathbb{Q})$ and also they prove their result with an explicit error term.

We now give a brief introduction of the ideas of the proof of Theorem 1.1. Given a fixed C_ℓ-extension F/k, Theorem 3.6 gives an if-and-only-if criterion determining $\mathrm{Gal}(L/k)$ for a C_ℓ-extension L/F, based on finitely many local conditions for L/F. In the proof, firstly, we study all continuous homomorphisms ρ from the idéle class group C_F to C_ℓ as an $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module and prove that for each such ρ, its $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module structure is completely determined by its completions $\rho_\mathfrak{p} : \prod_{\mathfrak{P}|\mathfrak{p}} F_\mathfrak{P}^\times \to C_\ell$ for finitely many $\mathfrak{p}$. This will determine the parameter d in $H(\ell, d)$ or $\tilde{H}(\ell, d)$ for $\mathrm{Gal}(L/k)$. Secondly, we consider the difference of group structures of $H(\ell, d)$ and $\tilde{H}(\ell, d)$ (split or not as a group extension) to further pin down $\mathrm{Gal}(L/k)$ via studying $\rho_\mathfrak{p}$ where $\mathfrak{p}$ is an inert prime in F/k. Combining the two inputs, we write down a generating series for all C_ℓ-extensions L/F with a given $\mathrm{Gal}(L/k)$ for a fixed F/k.

Analytically, for a given (twisted) Heisenberg group, we first count in Theorem 4.5 the number of extensions L/k containing a fixed intermediate field F/k via studying the analytic behavior of the generating series of ρ with a particular $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module structure, see Section 4. This method is inspired by and extends the techniques of Wright–Wood [35, 34] on counting abelian extensions, where the generating series of $\rho : C_F \to C_\ell$ was studied but without constraints on the $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module structure of ρ. This allows us to compare our generating series with some Hecke L-functions and therefore we can study its right-most poles. Finally, we sum over all C_ℓ-extensions F/k. This method of summation closely follows the ideas in [29]. At the same time, a forthcoming work [4] of the second author and Alberts, Lemke Oliver and Wood will apply this idea to give the asymptotic distribution for more general family of groups.

We mention that Theorem 4.5 can also be treated by other methods. A similar generating series is also essentially studied in the appendix of [2], using an approach suggested by Wood. For this special case, we adopt a different way to control the total Galois groups. Given Proposition 4.4, Theorem 4.5 also follows from [2, 3], which answers this question for more general family of groups up to an existence result. See also [30, 31] on similar questions for other small degree

groups with more explicit results.

The structure of this paper is as follows. In Section 2, we first define and describe the generalized and twisted Heisenberg groups in Section 2.1, and then determine the constants $a(G)$ and $b(G,k)$ in Section 2.2. In Section 3, we study class field theory and classify $\mathrm{Gal}(L/k)$ based on the local information of $\rho : C_F \to C_\ell$. In Section 4, we first study the generating series of all L/F with a given $\mathrm{Gal}(L/k)$ for a fixed C_ℓ-extension F/k in Section 4.3 and 4.4, and finally we complete the proof by a partial summation in Section 4.5.

2 Generalized Heisenberg Groups

2.1 Galois Groups of Relative ℓ-Towers

In this section, we are aiming for a characterization for the Galois group we will consider in this paper. Most results for small ℓ-groups are standard, we only include the discussion for the convenience of the reader and for the introduction of notation that we will also use in later parts of the paper.

Given a base number field k, a C_ℓ-extension F/k and another C_ℓ-extension L/F, our goal is to describe the Galois group $\mathrm{Gal}(L/k)$ as a permutation group. Firstly, from standard Galois theory, the group $\mathrm{Gal}(L/k)$ can be embedded as a subgroup of $\mathrm{Gal}(L/F) \wr \mathrm{Gal}(F/k)$, in our case, $C_\ell \wr C_\ell = C_\ell^\ell \rtimes C_\ell \leq S_{\ell^2}$. We can canonically identify the vector space $V := \mathbb{F}_\ell^\ell$ with $\mathbb{F}_\ell[C_\ell]$ as an $\mathbb{F}_\ell[C_\ell]$-module from the definition of the wreath product. Let σ be a generator of $\mathrm{Gal}(F/k) = C_\ell$ and $\Delta = \langle \sigma - 1 \rangle$ to be the augmentation ideal of $\mathbb{F}_\ell[C_\ell]$. It follows from the fact that $\mathbb{F}_\ell[C_\ell]/\Delta \simeq \mathbb{F}_\ell$ that the linear action of σ on $\mathbb{F}_\ell[C_\ell]$ has one Jordan block with dimension ℓ, where the characteristic polynomial is $(\sigma-1)^\ell = \sigma^\ell - 1 = 0$. By linear algebra, the σ-invariant subspaces of $\mathbb{F}_\ell[C_\ell]$ are exactly the ideal Δ^d for $0 \leq d \leq \ell$. We will denote the $\Delta^{\ell-d}$ to be W_d, which is the unique dimension d invariant subspace of V.

Let's denote the quotient map by $\kappa : V \rtimes C_\ell \to C_\ell$ and the projection to the i-th C_ℓ-component in V by $\pi_i : V = C_\ell^\ell \to C_\ell$. In order for $G \leq C_\ell \wr C_\ell$ to be a Galois group of L/k, it must satisfy two conditions due to the existence of the intermediate field F: 1) the image $\kappa(G) = C_\ell$; 2) the image $\pi_i(G \cap V) = C_\ell$. It follows from the first condition that $G \cap V$ must be a σ-invariant subspace of V, thus equal to W_d for some $1 \leq d \leq \ell$, i.e., G satisfies

$$1 \to W_d \to G \to C_\ell \to 1.$$

For each d, depending on whether the group extension of C_ℓ by W_d is split or not, we can see different group structures for G. We first give an easy lemma which will be of use in later parts.

Lemma 2.1. *Let G be a group extension of W_d with C_ℓ for $d < \ell$. Let $g \in G \setminus W_d$. Then the extension is split, if and only if* $\mathrm{ord}(g) = \ell$, *if and only if* $\exp(G) = \ell$.

Proof. Say $g = ((a_1, \ldots, a_\ell), \sigma^k) \in C_\ell \wr C_\ell$ for $1 \leq k < \ell$. Then by computation

$$g^\ell = ((\sum_{i=1}^{\ell} a_i, \ldots, \sum_{i=1}^{\ell} a_i), e).$$

Therefore $\mathrm{ord}(g) = \ell$ if and only if $\sum_{i=1}^{\ell} a_i = 0 \in \mathbb{F}_\ell$, which is equivalent to $(a_1, \ldots, a_\ell) \in \Delta$, which is $W_{\ell-1}$.

Since all other elements in $G \setminus W_d$ can be written as $u \cdot g^k$ where $u \in W_d \subseteq W_{\ell-1}$, we see that $\mathrm{ord}(g) = \ell$ implies $\mathrm{ord}(u \cdot g^k) = \ell$ for all possible u and $1 \leq k < \ell$. Therefore we show the

second equivalence in the lemma. On the other hand, the extension splits if and only if there exists a section, if and only if there exists an element in $G\backslash W_d$ of order ℓ, which is equivalent to $\mathrm{ord}(g) = \ell$ by the above argument. □

If the extension is split, then $G \simeq W_d \rtimes C_\ell$ where the action is just σ acting on $\Delta^{\ell-d}$. If the extension is non-split, it is not difficult to see that all groups of exponent ℓ^2 corresponding to W_d are isomorphic to each other, e.g. see [33, Theorem 2] for a reference.

Definition 2.2. *For $1 \leq d < \ell$ we define the* generalized Heisenberg group of dimension d *to be the split extension of W_d by C_ℓ and denote it by $H(\ell, d)$, and define the* twisted Heisenberg group of dimension d *to be the non-split extension of W_d by C_ℓ and denote by $\tilde{H}(\ell, d)$.*

As special cases we get $H(\ell, 1) = C_\ell \times C_\ell$, and $\tilde{H}(\ell, 1) = C_{\ell^2}$. The identification of $H(\ell, 2)$ with the usual Heisenberg group of order ℓ^3 explains the motivation for this definition. We also define $H(\ell, \ell) := C_\ell \wr C_\ell$.

2.2 Malle's prediction

In this section, we are going to compute the constants $a(G)$ and $b(G, k)$ in Malle's prediction for all groups $H(\ell, d) \leq S_{\ell^2}$ and $\tilde{H}(\ell, d) \leq S_{\ell^2}$ for $1 < d < \ell$. Let us first define $a(G)$ and $b(G, k)$ for general permutation groups and number fields k.

Definition 2.3. *Let $G \leq S_n$ for $n > 1$ be a transitive subgroup acting on $\Omega = \{1, \ldots, n\}$.*

1. *For $g \in G$ we define the index* $\mathrm{ind}(g) := n -$ *the number of orbits of g on Ω.*
2. $\mathrm{ind}(G) := \min\{\mathrm{ind}(g) : \mathrm{id} \neq g \in G\}$, $a(G) := \mathrm{ind}(G)$.

Note that $a(G)$ here is the inverse of the $a(G)$ defined in [24]. Since all elements in a conjugacy class C of G have the same index we can define $\mathrm{ind}(C)$ in a canonical way. The absolute Galois group G_k of k acts on the set of conjugacy classes of G via the action on the $\bar{\mathbb{Q}}$–characters of G. That is, denote the composition $f : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(\mu_\infty) = \prod_p \mathbb{Z}_p^\times \to (\mathbb{Z}/|G|\mathbb{Z})^\times$ where $|G|$ is the order of the group. Then if $f(\sigma)(\mu_n) = \mu_n^k$, then the action of σ on an element g is $\sigma(g) = g^k$ for $g \in G$. The orbits under this action are called k-conjugacy classes.

Definition 2.4. *For a number field k and a transitive subgroup $G \leq S_n$ we define:*

$$b(k, G) := \#\{C : C \text{ non trivial } k\text{-conjugacy class of } G \text{ of minimal index } \mathrm{ind}(G)\}.$$

The minimal index is attained by elements of prime order. Let G be an ℓ-group and denote by $\mathcal{C}$ be the set of non-trivial conjugacy classes of minimal index in G. Then $\mathcal{C}$ is closed under taking k-th power when $1 \leq k \leq \ell - 1$ since $\mathrm{ind}(g) = \mathrm{ind}(g^k)$ for $\mathrm{ord}(g) = \ell$. Moreover, it is clear that g and g^k are not conjugate to each other in G. The action of the absolute Galois group G_k on $\mathcal{C}$ factors through the cyclotomic character $G_k \to \hat{\mathbb{Z}}^\times$. Let ζ_ℓ be a primitive ℓ-th root of unity and $\tau \in G_k$, where $\tau(\zeta_\ell) = \zeta_\ell^k$. Then its action on $\mathcal{C}$ is $\tau(g) = g^k$. Therefore it suffices to consider the action of $\mathrm{Gal}(k(\zeta_\ell)/k)$ on $\mathcal{C}$. By applying stabilizer-orbit formula to the action of $\mathrm{Gal}(k(\zeta_\ell)/k)$ on $\{g, g^2, \ldots, g^{\ell-1}\}$, we immediately get the following lemma.

Lemma 2.5. *Let $G \leq S_n$ be an ℓ-group and k be a number field. Then we have the formula*

$$b(G, k) = b(G, \mathbb{Q}) \frac{\ell - 1}{[k(\zeta_\ell) : k]}.$$

In this case $b(G, \mathbb{Q}(\zeta_\ell)) = (\ell - 1) b(G, \mathbb{Q})$ is the number of conjugacy classes of minimal index.

Now we are able to compute the constants $a(G)$ and $b(G,k)$ for our groups considered as transitive subgroups of S_{ℓ^2}.

Lemma 2.6. *For $G = H(\ell,d)$ or $\tilde{H}(\ell,d)$ with $1 < d < \ell$, we have that*

$$a(G) = (\ell-1)(\ell-d+1), \qquad b(G,k) = \binom{\ell}{d-1}\frac{\ell-1}{\ell[k(\zeta_\ell):k]}.$$

Proof. Firstly, we look at $G = H(\ell,d)$. Recall that G is a semi-direct product

$$1 \to W_d \to H(\ell,d) \xrightarrow{\kappa} C_\ell \to 1.$$

Denote by $H \leq W_d$ an index ℓ-subgroup with $\mathrm{Core}_G(H) = \{e\}$. Then the left multiplication action of G acting on the cosets of H realizes the permutation representation of $H(\ell,d) \leq S_{\ell^2}$. Since $H(\ell,d)$ has exponent ℓ, every element has only ℓ-cycles and fixed points. Therefore it suffices to count the number of fixed points for each element. Let us denote by c_iH the left cosets of H in G for $1 \leq i \leq \ell^2$. Then g fixes cH if and only if $g \in cHc^{-1}$. Therefore to count the number of fixed points of g, it suffices to count the number of i such that $g \in c_iHc_i^{-1}$. Notice that $H^{c_i} := c_iHc_i^{-1} = H^{\kappa(c_i)}$ since G splits, so it suffices to consider the conjugation H^σ from the semi-direct product, i.e. $\sigma \in C_\ell$.

Let σ be a generator of the C_ℓ-quotient and $H_i := H^{\sigma^i}$. Note that the number of fixed points of an element $g \in G$ is equal to

$$\ell\,|\{1 \leq i \leq \ell \mid g \in H_i\}|\,. \tag{2.1}$$

We now show that for arbitrary $I \subseteq \{1,\dots,\ell\}$, the intersection space as a subspace in W_d satisfies

$$\mathrm{Codim}(\bigcap_{i\in I} H_i) = \min\{|I|, d\}. \tag{2.2}$$

We prove (2.2) by induction. For $|I| = 1$, this holds clearly since our H has index ℓ in W_d. For $|I| = 2$, by inclusion-exclusion, we get for arbitrary $i \neq j$ that

$$\mathrm{Codim}(H_i + H_j) = \mathrm{Codim}(H_i) + \mathrm{Codim}(H_j) - \mathrm{Codim}(H_i \cap H_j).$$

Using $\mathrm{Codim}(H_i) = 1$ and $\mathrm{Codim}(H_i + H_j) = 0$ we get

$$\mathrm{Codim}(H_i \cap H_j) = 2.$$

Now by induction for $2 \leq |I| \leq d$, the general inclusion-exclusion formula for the dimension still holds with the computation of codimension, so we get for a subset $J(m) \subseteq I$ of size m:

$$\begin{aligned}\mathrm{Codim}(\bigcap_{i\in I} H_i) &= \sum_{1\leq m<|I|}\binom{|I|}{m}\mathrm{Codim}(\bigcap_{i\in J(m)\subseteq I} H_i)\cdot(-1)^{\ell-m+1}\\ &= \sum_{1\leq m<|I|}\binom{|I|}{m}m(-1)^{|I|-m+1} = |I|.\end{aligned}$$

For the second last equality, we use by induction that $\mathrm{Codim}(\bigcap_{i\in J(m)\subseteq I} H_i) = m$. For the last equality we use

$$\sum_{1\leq m\leq n}\binom{n}{m}m(-1)^{n-m+1} = 0.$$

This shows (2.2). Note that the intersection of d different H_i is the trivial group and that for $|I| = d-1$ we get $\dim(\bigcap_{i\in I} H_i) = 1$. Using (2.1) we see that non-trivial elements in $g \in \bigcap_{i\in I} H_i$

all have exactly $\ell(d-1)$ fixed points, since the intersection with a further H_i has dimension 0. Now such a g has $\frac{\ell^2-\ell(d-1)}{\ell}$ cycles of length ℓ and therefore we get:

$$\mathrm{ind}(g) = \ell^2 - \frac{\ell^2-\ell(d-1)}{\ell} - \ell(d-1) = (\ell-1)(\ell-d+1).$$

This is the minimal index using (2.1). Note that elements $g \in G \setminus W_d$ have no fixed points and we get $\mathrm{ind}(g) \geq \ell^2 - \ell = \ell(\ell-1) > (\ell-1)(\ell-d+1)$ since $d > 1$.

Now we consider $b(G, \mathbb{Q})$. For arbitrary I with $|I| = d-1$, using (2.2) we find $(\ell-1)$ many group elements with minimal index. So the number of elements with minimal index is

$$\binom{\ell}{d-1} \cdot (\ell-1).$$

The conjugation action from G has orbit sizes ℓ. Therefore the number of conjugacy classes of minimal index is equal to

$$b(H(\ell,d), \mathbb{Q}(\zeta_\ell)) = \binom{\ell}{d-1}\frac{\ell-1}{\ell}.$$

This gives the stated formula for G using the remark before the lemma.

For $G = \tilde{H}(\ell,d)$ or $G = H(\ell,d)$, notice that if an element $g \in G \leq C_\ell \wr C_\ell$ has non-trivial image $\kappa(g) \neq 0 \in C_\ell$, then the permutation action of g has no fixed point. So it suffices to consider elements in W_d. Both the cycle structure of W_d and the action of C_ℓ on W_d stay the same inside $C_\ell \wr C_\ell$. So both $a(\tilde{H}(\ell,d)) = a(H(\ell,d))$ and $b(\tilde{H}(\ell,d),k) = b(H(\ell,d),k)$. □

3 Arithmetic Theory

In this section, our main goal is to prove Theorem 3.6 which gives complete criteria for determining the Galois group $\mathrm{Gal}(L/k)$ from various local conditions on L/F where $L/F/k$ is a tower of number fields and both L/F and F/k are relative C_ℓ-extensions. We denote by $\mathbb{P}(k)$ and $\mathbb{P}(F)$ the set of all places (including the infinite ones) of k and F, respectively.

By class field theory, C_ℓ-extensions L/F are in bijection with surjective continuous homomorphisms $\rho : C_F \to \mathbb{F}_\ell$ where $C_F = I_F/F^\times$ is the idéle class group of F. Our goal is to determine $\mathrm{Gal}(L/k)$ from ρ. We denote by $G^\vee := \mathrm{Hom}(G, \mathbb{F}_\ell)$ the set of continuous group homomorphisms from G to $\mathbb{F}_\ell$.

3.1 S-idéle Class Groups

For any finite set of places S, we define the S-idéle class group $C_{F,S} := I_{F,S}/\mathcal{O}_{F,S}^\times$, where $I_{F,S} := \prod_{\mathfrak{P}\in S} F_\mathfrak{P}^\times \times \prod_{\mathfrak{P}\notin S} \mathcal{O}_\mathfrak{P}^\times$ is the S-idéle group of F and $\mathcal{O}_{F,S}^\times$ is the S-unit group of F. Then there is a canonical embedding $C_{F,S} \hookrightarrow C_F$, it induces a map $f : C_{F,S}/C_{F,S}^\ell \to C_F/C_F^\ell = I_F/F^\times I_F^\ell$, and thus induces a map $f^\vee : C_F^\vee \to C_{F,S}^\vee$. By class field theory, see e.g. [34, Lemma 2.8], if $S \subseteq \mathbb{P}(F)$ contains all infinite places and is large enough to generate the class group Cl_F, then $C_F \simeq C_{F,S}$. We will give a refined characterization for $C_F^\vee$, the ℓ-part of C_F when ℓ is odd.

Lemma 3.1. *Let $S \subseteq \mathbb{P}(F)$ be a finite set and ℓ be an odd prime. Then $f : C_{F,S}/C_{F,S}^\ell \to C_F/C_F^\ell$ is an isomorphism if and only if S is large enough to generate the ℓ-primary part of* Cl_F.

Proof. Firstly, we show that f is injective if S generates the ℓ-primary part of the class group. If $y \in I_{F,S}$ satisfies $y = x^\ell \cdot u$ for some $x \in I_F$ and $u \in F^\times$, then for the ideals $\mathfrak{b} = \prod_\mathfrak{P} \mathfrak{P}^{\mathrm{val}_\mathfrak{P}(y_\mathfrak{P})}$

and $\mathfrak{a} = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathrm{val}_{\mathfrak{P}}(x_{\mathfrak{P}})}$, we have $\mathfrak{b} = \mathfrak{a}^{\ell} \in \mathrm{Cl}_F$. The class group has a canonical decomposition $\mathrm{Cl}_F = A_1 \times A_2$ where $A_1 = \mathrm{Cl}_F[\ell^{\infty}]$ is the Sylow-ℓ subgroup of Cl_F, then we denote $\mathfrak{a} = (\mathfrak{a}_1, \mathfrak{a}_2)$ and $\mathfrak{b} = (\mathfrak{b}_1, \mathfrak{b}_2) = (\mathfrak{a}_1^{\ell}, \mathfrak{a}_2^{\ell}) \in \mathrm{Cl}_F$. Since ideal classes $\mathfrak{b}_1$ and $\mathfrak{b}$ are both generated by S, we see that $\mathfrak{b}_2$ is also generated by S. Therefore in $\mathfrak{a} \in \mathrm{Cl}_F$ the component $\mathfrak{a}_2$ can also be generated by S since ℓ is invertible in A_2, thus $\mathfrak{a} \in \mathrm{Cl}_F$ can be generated by S. Let's say $\mathfrak{a}' = \mathfrak{a} \cdot (v)$ has valuations supported on S where $v \in F^{\times}$, then denote $x' := xv \in I_{F,S}^{\times}$. Clearly $y = x^{\ell}u = (x'v^{-1})^{\ell}u = (uv^{-\ell}) \cdot (x')^{\ell}$ is an element in $\mathcal{O}_{F,S}^{\times} I_{F,S}^{\ell}$, here $uv^{-\ell} \in \mathcal{O}_{F,S}^{\times}$ since y and x' are both in $I_{F,S}$.

Secondly, in order to show that f is surjective, for an arbitrary element $x = (x_{\mathfrak{P}})$ in C_F/C_F^{ℓ}, we need to find a representative such that $x_{\mathfrak{P}} \in \mathcal{O}_{\mathfrak{P}}^{\times}$ for $\mathfrak{P} \notin S$. Firstly, we are allowed to reduce to the case where $0 \leq \mathrm{val}_{\mathfrak{P}}(x_{\mathfrak{P}}) < \ell$ by the quotient by C_F^{ℓ}. Then for each $\mathfrak{P}$ where $\mathrm{val}_{\mathfrak{P}}(x_{\mathfrak{P}}) \neq 0$, if the order of $\mathfrak{P} \in \mathrm{Cl}_F$ is $n_{\mathfrak{P}} = \ell^k \cdot n'$ where $(\ell, n') = 1$, we can write $\mathfrak{P}^{n'} = \mathfrak{a} \cdot (u_{\mathfrak{P}})$ where $\mathfrak{a}$ is an ideal generated by primes in S. Then multiplying by suitable powers of $u_{\mathfrak{P}} \in F^{\times}$, we can obtain another representative x' of x in C_F where $\mathrm{val}_{\mathfrak{P}}(x'_{\mathfrak{P}}) = 0 \mod \ell$ but which has the same valuation at any other prime outside S. We can iterate this operation to kill every non-zero $\mathrm{val}_{\mathfrak{P}}(x_{\mathfrak{P}})$ and find a representative of x in $I_{F,S}$.

Conversely, if S does not generate the ℓ-primary part of the class group, say $\mathfrak{p}$ is not generated by S, then f is not surjective since $(1, 1, \ldots, \pi, \ldots, 1) \in C_F/C_F^{\ell}$, where $\pi \in \mathcal{O}_{\mathfrak{p}}$ is the uniformizer for $\mathfrak{p}$, is not in the image of f. □

3.2 Rank of ρ

In the remaining part of this paper σ will be a generator of $\mathrm{Gal}(F/k) = C_{\ell}$.

For $\mathfrak{p} \in \mathbb{P}(k)$ we denote the component of I_F at $\mathfrak{p}$ by $I_F(\mathfrak{p}) := \prod_{\mathfrak{P}|\mathfrak{p}} F_{\mathfrak{P}}^{\times}$. For each $\rho \in C_F^{\vee}$ and $\mathfrak{p} \in \mathbb{P}(k)$, we get a local map $\rho_{\mathfrak{p}} \in I_F(\mathfrak{p})^{\vee}$ induced by the natural inclusion $I_F(\mathfrak{p}) \hookrightarrow I_F \twoheadrightarrow C_F$. Note that $I_F(\mathfrak{p}) = (F \otimes_k k_{\mathfrak{p}})^{\times}$, therefore $I_F(\mathfrak{p})$ is naturally a $\mathrm{Gal}(F/k)$-module, where the action is induced by its action on F. Thus $I_F(\mathfrak{p})^{\vee}$ is also a finite dimensional $\mathbb{F}_{\ell}[\mathrm{Gal}(F/k)]$-module by defining the action to be $\sigma(\rho_{\mathfrak{p}}) = \rho_{\mathfrak{p}} \circ \sigma^{-1}$. Since $\mathrm{Gal}(F/k)$-action preserves the valuation, we see $\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times}$ and $(\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times})^{\vee}$ are also natural $\mathrm{Gal}(F/k)$-modules. To simplify our notation, we will define

$$U_{\mathfrak{p}} := \begin{cases} \prod_{\mathfrak{P}|\mathfrak{p}} F_{\mathfrak{P}}^{\times}/(F_{\mathfrak{P}}^{\times})^{\ell} & \mathfrak{p} \in S_k, \\ \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}^{\times}/(\mathcal{O}_{\mathfrak{P}}^{\times})^{\ell} & \mathfrak{p} \notin S_k, \end{cases}$$

whenever a set S_k is specified in the context. Notice that $\rho_{\mathfrak{p}} \in I_F(\mathfrak{p})^{\vee}$ has a natural restriction to $U_{\mathfrak{p}}^{\vee}$.

The global object $C_F = I_F/F^{\times}$ is also a $\mathrm{Gal}(F/k)$-module since $\mathrm{Gal}(F/k)$ acts on $I_F(\mathfrak{p})$ for each $\mathfrak{p}$. This also induces a $\mathrm{Gal}(F/k)$-action on $C_F^{\vee}$ where $\sigma(\rho) = \rho \circ \sigma^{-1}$.

Notice that $\sigma^{\ell} - 1 = 0 = (\sigma - 1)^{\ell} \in \mathbb{F}_{\ell}[\mathrm{Gal}(F/k)]$, therefore for any $\mathbb{F}_{\ell}[\mathrm{Gal}(F/k)]$-module M we have $(\sigma - 1)^{\ell} M = 0$. We define the following notion of a *rank* for convenience of our paper, which is not the same with the usual notion of the rank of a R-module.

Definition 3.2. *Given an $\mathbb{F}_{\ell}[\mathrm{Gal}(F/k)]$-module M we define* the rank *of M to be the smallest integer r such that $(\sigma - 1)^r M = 0$. We denote it by $\mathrm{rk}(M)$. We also define $\mathrm{rk}(m) = \mathrm{rk}(\langle m \rangle)$ to be the rank of the module generated by $m \in M$. We define $M_d := \{m \in M \mid (\sigma - 1)^d m = 0\}$ to be the maximal submodule of M of rank d.*

Considering $C_F^{\vee}$ and $I_F(\mathfrak{p})^{\vee}$ both as $\mathbb{F}_{\ell}[\mathrm{Gal}(F/k)]$-modules, we have the following lemma characterizing the global rank in terms of the local ranks. In case $\mathfrak{p} \notin S_k$ we remark that the rank of $\rho_{\mathfrak{p}} \in U_{\mathfrak{p}}^{\vee}$ is smaller or equal to the rank of $\rho_{\mathfrak{p}} \in I_F(\mathfrak{p})^{\vee}$.

Lemma 3.3. *Given $\rho \in C_F^\vee$, we have*

$$\mathrm{rk}(\rho) = \max_{\mathfrak{p}\in\mathbb{P}(k)} \mathrm{rk}(\rho_\mathfrak{p}), \text{ where } \rho_\mathfrak{p} \in I_F(\mathfrak{p})^\vee.$$

Let $S \subseteq \mathbb{P}(F)$ be large enough to generate the ℓ-primary part of Cl_F. We denote by $S_k \subseteq \mathbb{P}(k)$ the finite set containing all valuations lying below one contained in S and by $T_k \subseteq \mathbb{P}(k)$ the set of ramified primes of F/k. Then we have:

$$\mathrm{rk}(\rho) = \max_{\mathfrak{p}\in S_k\cup T_k} \mathrm{rk}(\rho_\mathfrak{p}), \text{ where } \rho_\mathfrak{p} \in U_\mathfrak{p}^\vee.$$

Proof. For the first claim it suffices to notice that the restriction map $C_F^\vee \to \prod_{\mathfrak{p}\in\mathbb{P}(k)} I_F(\mathfrak{p})^\vee$ is injective and compatible with the $\mathrm{Gal}(F/k)$-action.

For the second claim, we use Lemma 3.1 to see that $C_F^\vee = C_{F,S}^\vee$. Since $C_F^\vee = (I_{F,S}/\mathcal{O}_{F,S}^\times)^\vee \to \prod_\mathfrak{p} U_\mathfrak{p}^\vee$ is injective and compatible with the $\mathrm{Gal}(F/k)$-action we have

$$\mathrm{rk}(\rho) = \max_{\mathfrak{p}\in\mathbb{P}(k)} \mathrm{rk}(\rho_\mathfrak{p}), \text{ where } \rho_\mathfrak{p} \in U_\mathfrak{p}^\vee.$$

Note $\mathrm{rk}(\rho_\mathfrak{p}) = 0$ for $\mathfrak{p} \notin S_k$ when $\mathfrak{p}$ is unramified in F/k and we get the claim. □

Note that in the second formula the sets S_k and T_k are finite sets and we reduced the computation of $\mathrm{rk}(\rho)$ to a finite local computation.

Lemma 3.4. *Let $\rho \in C_F^\vee$ and denote the corresponding C_ℓ-extension by L/F. Then $\mathrm{rk}(\rho) = d$ if and only if $\mathrm{Gal}(L/k) = H(\ell, d)$ or $\tilde{H}(\ell, d)$.*

Proof. For each subgroup M of $C_F^\vee$, we define $H := \bigcap_{\rho\in M} \mathrm{Ker}(\rho) \subseteq C_F$. Then M is a $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-submodule of $C_F^\vee$ if and only if H is a normal subgroup of $\mathrm{Gal}(F^{\mathrm{ab},\ell}/k)$ if and only if the fixed field of H is Galois over k.

Let $\rho \in C_F^\vee$ and denote L/F to be the corresponding C_ℓ-extension over F. Then the $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module $M = \langle\rho\rangle$ generated by ρ will correspond to the Galois closure $\tilde{L}$ of L over k. Let σ be the chosen generator of $\mathrm{Gal}(F/k)$. A cyclic module M has a single Jordan block for σ since it is isomorphic to a quotient of $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$. Then the minimal polynomial for σ acting on M is $(X-1)^d$ if and only if $\dim_{\mathbb{F}_\ell}(M) = d$. Finally, notice that $\mathrm{Gal}(\tilde{L}/F)^\vee = M$ (via quotient out by H) as $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module, so we have $\dim_{\mathbb{F}_\ell}(\mathrm{Gal}(\tilde{L}/F)) = \dim_{\mathbb{F}_\ell}(\mathrm{Gal}(\tilde{L}/F)^\vee) = \dim_{\mathbb{F}_\ell}(M) = d$. □

Lemma 3.5. *Let $\rho \in C_F^\vee = \mathrm{Hom}(C_F, \mathbb{F}_\ell)$ with $\mathrm{rk}(\rho) = d$ and $\mathfrak{p}_0 \in \mathbb{P}(k)$ be inert in F/k and not above ℓ. Let π be a uniformizer of $k_{\mathfrak{p}_0}$. Then $\mathrm{Gal}(L/k) = H(\ell, d)$ if and only if $\rho(\pi) = 0$.*

Proof. Recall that both $H(\ell, d)$ and $\tilde{H}(\ell, d)$ are extensions of the form

$$1 \to W_d = \mathrm{Gal}(L/F) \to G \to \mathrm{Gal}(F/k) = C_\ell \to 1,$$

where the extension splits if and only if any lift of a non-zero element of C_ℓ in G has order ℓ. On the other hand the extension is non-split, if every lift of a non-zero element of C_ℓ in G has order ℓ^2. So it suffices to prove that $\rho(\pi) = 0$ if and only if any lift of σ has order ℓ.

Let's say $\mathfrak{p}_0\mathcal{O}_F = \mathfrak{P}_0$ is inert in F/k and $\mathrm{Frob}_{\mathfrak{P}_0} = \sigma$ generates C_ℓ. If $\mathfrak{P}_0$ is further inert in L/F, then by local class field theory, the local map $\rho_\mathfrak{p}$ corresponds to the unique unramified degree ℓ-extension U over $F_{\mathfrak{P}_0}$ where $U/k_{\mathfrak{p}_0}$ gives the unique unramified degree ℓ^2-extensions over $k_{\mathfrak{p}_0}$ and has $\mathrm{Gal}(U/k_{\mathfrak{p}_0}) = C_{\ell^2}$, then the decomposition group at $\mathfrak{p}_0$ is isomorphic to $\mathrm{Gal}(U/k_{\mathfrak{p}_0})$ and is generated by $\mathrm{Frob}_{\mathfrak{p}_0}$ which has order ℓ^2.

If $\mathfrak{P}_0$ is split in L/F, then $\rho_{\mathfrak{p}_0}$ is the trivial map and the decomposition group at $\mathfrak{p}_0$ intersects trivially with W_d, therefore $\mathrm{Frob}_{\mathfrak{p}_0}$ has order ℓ.

If $\mathfrak{P}_0$ is ramified in L/F, there are two cases. On one hand, there is a unique ramified C_ℓ-extension $R/F_{\mathfrak{P}_0}$ such that $\mathrm{Gal}(R/k_{\mathfrak{p}_0}) = C_\ell \times C_\ell$. The extension $R/k_{\mathfrak{p}_0}$ is also the compositum of $F_{\mathfrak{P}_0}$ and $k_{\mathfrak{p}_0}(\pi^{1/\ell})$. Then $R = F_{\mathfrak{P}_0}(\pi^{1/\ell})$ and $\pi = \mathrm{Nm}_{R/F_{\mathfrak{P}_0}}(\pi^{1/\ell})$, therefore R corresponds to $\rho_{\mathfrak{p}}$ that maps $\rho_{\mathfrak{p}}(\pi) = 0$. In this case, the decomposition group at $\mathfrak{p}_0$ is isomorphic to $\mathrm{Gal}(R/k_{\mathfrak{p}_0}) = C_\ell \times C_\ell$ and $\mathrm{Frob}_{\mathfrak{p}_0}$ has order ℓ. On the other hand, all other ramified C_ℓ-extensions of $F_{\mathfrak{P}_0}$ are subfields of $RU/F_{\mathfrak{P}_0}$ with $\mathrm{Gal}(RU/k_{\mathfrak{p}_0}) = C_{\ell^2} \times_{C_\ell} (C_\ell \times C_\ell) = C_{\ell^2} \times C_\ell$, which has decomposition group C_{ℓ^2} and $\mathrm{Frob}_{\mathfrak{p}_0}$ has order ℓ^2. □

Now combining Lemmata 3.3, 3.4, and 3.5 we get the following theorem.

Theorem 3.6. *Let $S \subseteq \mathbb{P}(F)$ be large enough to generate the ℓ-primary part of Cl_F and $S_k, T_k \subseteq \mathbb{P}(k)$ be the sets defined in Lemma 3.3. Let $\mathfrak{p}_0 \in \mathbb{P}(k)$ be inert in F/k and not above ℓ. Let π be a uniformizer of $k_{\mathfrak{p}_0}$. For $\rho \in C_F^\vee$, $\rho_{\mathfrak{p}} \in U_{\mathfrak{p}}^\vee$, and the corresponding C_ℓ-extension L/F we have*

1. *$\mathrm{Gal}(L/k) = H(\ell, r)$ if and only if*

$$\mathrm{rk}(\rho) = \max_{\mathfrak{p} \in S_k \cup T_k} \mathrm{rk}(\rho_{\mathfrak{p}}) = r, \text{ and } \rho_{\mathfrak{p}_0}(\pi) = 0,$$

2. *$\mathrm{Gal}(L/k) = \tilde{H}(\ell, r)$ if and only if*

$$\mathrm{rk}(\rho) = \max_{\mathfrak{p} \in S_k \cup T_k} \mathrm{rk}(\rho_{\mathfrak{p}}) = r, \text{ and } \rho_{\mathfrak{p}_0}(\pi) \neq 0.$$

3.3 Rank of u

Here we study $\mathrm{rk}(u)$ for $u \in \mathcal{A} := \mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^\ell$. We use the sets S and S_k defined in Lemma 3.3. It is clear that both $\mathcal{A}$ and $U_{\mathfrak{p}}$ are $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-modules. For $1 \leq d \leq \ell$, we recall

$$U_{\mathfrak{p},d} := \{u_{\mathfrak{p}} \in U_{\mathfrak{p}} \mid \mathrm{rk}(u_{\mathfrak{p}}) \leq d\}, \qquad U_{\mathfrak{p},d}^\vee := \{\rho_{\mathfrak{p}} \in U_{\mathfrak{p}}^\vee \mid \mathrm{rk}(\rho_{\mathfrak{p}}) \leq d\}.$$

The following theorem relates $\mathrm{rk}(u)$ of the global unit u with $\mathrm{rk}(u_{\mathfrak{p}})$ of the local units for $\mathfrak{p} \in \mathbb{P}(k)$.

Theorem 3.7. *With the above condition, let $u \in \mathcal{O}_{F,S}^\times$. Then for $u \in \mathcal{A}$, we have*

$$\mathrm{rk}(u) = \max_{\mathfrak{p} \in \mathbb{P}(k)} \mathrm{rk}(u_{\mathfrak{p}}),$$

where $u_{\mathfrak{p}} \in U_{\mathfrak{p}}$ is the natural image of u in $U_{\mathfrak{p}}$. Moreover, with $v := (\sigma - 1)^d u$ for $\mathfrak{p} \notin S_k$ and split in $F(\zeta_\ell)/k$, denote by $\wp|\mathfrak{p}$ any prime ideal in $F(\zeta_\ell)$. Then we have

$$\mathrm{rk}(u_{\mathfrak{p}}) > d \iff \wp \text{ inert in } F(\zeta_\ell, v^{1/\ell})/F(\zeta_\ell).$$

Proof. For the first statement, we have $\mathrm{rk}(u) \leq d$ is equivalent to

$$v = 0 \in \mathcal{A} \iff v \in (\mathcal{O}_{F,S}^\times)^\ell \iff \forall \mathfrak{P} \in \mathbb{P}(F) \quad v \in (F_{\mathfrak{P}}^\times)^\ell,$$

where the second equivalence comes from Hasse's local-global principle, see e.g. [28, Theorem 9.1.11]. The last condition is equivalent to $\mathrm{rk}(u_{\mathfrak{p}}) \leq d$ for every $\mathfrak{p}$, therefore we showed that $\mathrm{rk}(u) \leq d \iff \forall \mathfrak{p}, \mathrm{rk}(u_{\mathfrak{p}}) \leq d$, it then implies that $\mathrm{rk}(u) = \max_{\mathfrak{p} \in \mathbb{P}(k)} \mathrm{rk}(u_{\mathfrak{p}})$.

Let's call $K = F(v^{1/\ell}, \zeta_\ell)$ with $\mathrm{Gal}(K/F) \simeq C_\ell \rtimes C_r$ where $r = [F(\zeta_\ell) : F]$. Let $\mathfrak{p} \notin S_k$ be a prime in k that is split in $F(\zeta_\ell)/k$ and $\wp$ be a prime ideal in $F(\zeta_\ell)$ with $\wp \cap F = \mathfrak{P}$ and $\wp \cap k = \mathfrak{p}$. Notice that $F_{\mathfrak{P}} = k_{\mathfrak{p}}$, and $K_\wp = F_{\mathfrak{P}}(v^{1/\ell})$, therefore

$$\mathrm{rk}(u_{\mathfrak{p}}) \leq d \iff v \in (F_{\mathfrak{P}}^\times)^\ell \iff K_\wp = F_{\mathfrak{P}} \iff \wp \text{ split in } K/F(\zeta_\ell).$$ □

For any $\mathbb{F}_\ell[\mathrm{Gal}(F/k)]$-module M, recall that $M^\vee = \mathrm{Hom}(M, \mathbb{F}_\ell)$, there is a natural pairing $M^\vee \times M \to \mathbb{F}_\ell$. The following statements will be important to us in Section 4.3.

Lemma 3.8. *Let $M = \mathbb{F}_\ell[C_\ell]$ and $M^\vee$ be its dual. For any $0 \le d \le \ell$ the two subspaces $M_d^\vee$ and $M_{\ell-d}$ are mutually orthogonal complements under the natural pairing $\langle \cdot, \cdot \rangle : M^\vee \times M \to \mathbb{F}_\ell$.*

Proof. For $M = \mathbb{F}_\ell[C_\ell]$ we define the submodule $M_d = (\sigma - 1)^{\ell-d} M$.

Recall that the induced action on $M^\vee$ is $(\sigma\rho)(m) = \rho(\sigma^{-1}(m))$. Therefore $\langle \rho, \sigma^{-1} m \rangle = \langle \sigma\rho, m \rangle$. For $\rho \in M_d^\vee$ and $m \in M_{\ell-d}$, we see that the pairing $\langle \rho, m \rangle = \langle (\sigma-1)^{\ell-d}\rho', (\sigma-1)^d m' \rangle = 0$ is always trivial.

On the other hand, if $\langle \rho, m \rangle = 0$ for every ρ with $\mathrm{rk}(\rho) \le d$, then $\langle \rho, (\sigma-1)^{\ell-d} m \rangle = 0$ for every ρ, so $(\sigma-1)^{\ell-d} m = 0$, i.e, $\mathrm{rk}(m) \le \ell - d$. This shows that the orthogonal complement of $M_d^\vee$ is $M_{\ell-d}$. Similarly, we can show the other direction. □

Recall from Section 2 that we have $C_\ell \wr C_\ell = W_\ell \rtimes C_\ell$ and we have identified W_ℓ with $\mathbb{F}_\ell[C_\ell]$ as an $\mathbb{F}_\ell[C_\ell]$-module. We can identify $\mathbb{F}_\ell[C_\ell]$ and $\mathbb{F}_\ell[C_\ell]^\vee$ by choosing a basis $\mathcal{E} := \{ g_i = \sigma^i \mid 1 \le i \le \ell \}$ for $\mathbb{F}_\ell[C_\ell]$ as an $\mathbb{F}_\ell$-module. Therefore we can identify $\mathbb{F}_\ell[C_\ell]^\vee$ with W_ℓ. Then we define for each $1 \le d \le \ell$,

$$\Phi_d := \{ \rho \in \mathbb{F}_\ell[C_\ell]^\vee \mid \mathrm{ind}(\rho) = a(H(\ell, d)) \}, \qquad \chi_d(m) := \sum_{\rho \in \Phi_d} \zeta_\ell^{\langle \rho, m \rangle}, \text{ where } \zeta_\ell = \exp(2\pi i/\ell) \in \mathbb{C}.$$

Notice that $\chi_d(m)$ is always an integer since Φ_d is closed under multiplication by $\mathbb{F}_\ell^\times$. For each $\rho \in \Phi_d$, $\sum_{i \in \mathbb{F}_\ell^\times} \zeta_\ell^{\langle i\rho, m \rangle}$ is either $\ell - 1$ or -1 depending on whether $\zeta_\ell^{\langle \rho, m \rangle}$ is 1 or not.

Lemma 3.9. *For $1 \le d \le \ell$ we have $\chi_d(m) = |\Phi_d|$ if and only if $m \in M_{\ell-d}$.*

Proof. It follows from Lemma 3.8 that if $u \in M_{\ell-d}$ then $\langle \rho, m \rangle = 0$ and therefore $\chi_d(m) = |\Phi_d|$. Conversely, notice that Φ_d contains $(\sigma - 1)^d \sigma^m$ for any m, therefore Φ_d generates W_d as an $\mathbb{F}_\ell$-module, therefore if $\langle \rho, m \rangle = 0$ for every ρ, we know that $u \in M_{\ell-d}$ by Lemma 3.8. □

Now notice that when $\mathfrak{p} \notin S_k$ is split in F/k, then $U_\mathfrak{p} \simeq \mathbb{F}_\ell[C_\ell]$, therefore it follows that $U_{\mathfrak{p},d}$ and $U_{\mathfrak{p},\ell-d}^\vee$ are orthogonal complements under this natural pairing. Moreover, since $U_\mathfrak{p} \simeq \mathbb{F}_\ell[C_\ell]$, via this identification, we can identify the $\rho \in U_\mathfrak{p}^\vee$ with those in Φ_d, then for $u \in U_\mathfrak{p}$, $\chi_d(u) = |\Phi_d|$ if and only if $u \in U_{\mathfrak{p},\ell-d}$.

4 Analytic Theory

Theorem 3.6 has given a full description of those $\rho : I_{F,S}/\mathcal{O}_{F,S}^\times \to C_\ell$ with $\mathrm{Gal}(\rho) = H(\ell, d)$ or $\tilde{H}(\ell, d)$. In this section, we are going to write up a Dirichlet series for $\mathrm{Disc}(L/F)$ where L/F are C_ℓ-extensions with $\mathrm{Gal}(\tilde{L}/k) = H(\ell, d)$ or $\tilde{H}(\ell, d)$ for a fixed $1 \le d \le \ell - 1$.

We fix F/k with $\mathrm{Gal}(F/k) = \langle \sigma \rangle$. Let $S \subseteq \mathbb{P}(F)$ be a finite $\mathrm{Gal}(F/k)$-invariant set containing all primes above ℓ, and which is large enough to generate the ℓ-primary part of Cl_F. Furthermore S contains a prime $\mathfrak{P}_0$ not above (ℓ) which is inert in F/k. We denote the prime below $\mathfrak{P}_0$ by $\mathfrak{p}_0$ and we fix a uniformizer π for $k_{\mathfrak{p}_0}$ and $F_{\mathfrak{P}_0}$. Like in Lemma 3.3 we define the set $S_k \subseteq \mathbb{P}(k)$ to contain all primes below primes in S.

4.1 Dirichlet Series for Homomorphisms

We give the generating series for all continuous homomorphisms from $I_{F,S}$ to C_ℓ with $\mathrm{rk}(\rho) \leq d$ and $\rho(\pi) = 0$. By Theorem 3.6, to get $\mathrm{rk}(\rho) \leq d$ it suffices to require $\mathrm{rk}(\rho_\mathfrak{p}) \leq d$ for every $\mathfrak{p} \in S_k \cup T_k$, where T_k denotes the set of ramified places of F/k. We define our generating series as complex functions for $s \in \mathbb{C}$

$$f_d(s) := \sum_{\rho \in I_{F,S}^\vee, \mathrm{rk}(\rho) \leq d, \rho(\pi)=0} \frac{1}{\mathrm{Disc}(\rho)^s} = \left(\sum_{\rho_{\mathfrak{p}_0} \in U_{\mathfrak{p}_0,d}^\vee, \rho(\pi)=0} \frac{1}{\mathrm{Disc}(\rho_{\mathfrak{p}_0})^s} \right) \prod_{\mathfrak{p} \neq \mathfrak{p}_0} \left(\sum_{\rho_\mathfrak{p} \in U_{\mathfrak{p},d}^\vee} \frac{1}{\mathrm{Disc}(\rho_\mathfrak{p})^s} \right),$$

where $\mathrm{Disc}(\rho_\mathfrak{p}) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{Disc}(\rho_\mathfrak{P})$ and $\mathrm{Disc}(\rho_\mathfrak{P})$ is the relative discriminant of the local field extension over $F_\mathfrak{P}$ associated to $\rho_\mathfrak{P} : F_\mathfrak{P}^\times \to C_\ell$. Similarly, we will also define

$$\tilde{f}_d(s) := \sum_{\rho \in I_{F,S}^\vee, \mathrm{rk}(\rho) \leq d, \rho(\pi)\neq 0} \frac{1}{\mathrm{Disc}(\rho)^s} = \left(\sum_{\rho_{\mathfrak{p}_0} \in U_{\mathfrak{p}_0,d}^\vee, \rho(\pi)\neq 0} \frac{1}{\mathrm{Disc}(\rho_{\mathfrak{p}_0})^s} \right) \prod_{\mathfrak{p} \neq \mathfrak{p}_0} \left(\sum_{\rho_\mathfrak{p} \in U_{\mathfrak{p},d}^\vee} \frac{1}{\mathrm{Disc}(\rho_\mathfrak{p})^s} \right)$$

to be the Dirichlet series enumerating ρ with $\mathrm{rk}(\rho) \leq d$ and $\rho(\pi) \neq 0$. Both functions are well-defined and analytic when $\Re(s)$ is large enough.

The function $f_d(s)$ is obviously over-counting the number of extensions L/F with $\mathrm{Gal}(L/k) = H(\ell, d)$ for two reasons: not every homomorphism ρ from $I_{F,S}$ factors through $\mathcal{O}_{S,F}^\times$; the rank $\mathrm{rk}(\rho)$ can be strictly smaller than d. We solve the first issue using some character sum to test whether ρ factors through $\mathcal{O}_{S,F}^\times$. In particular, in the next section, we will introduce the series $g_d(s)$ and $\tilde{g}_d(s)$ which takes issue into consideration. This method is inspired by [35] and [34] in counting abelian extensions over general number fields, although the analysis is more complicated in this generalization. We will solve the second issue simply by taking the difference of generating series for $\mathrm{rk}(\rho) \leq d$ and that for $\mathrm{rk}(\rho) \leq d-1$.

4.2 Character Sum

Recall that ρ factors through $\mathcal{O}_{S,F}^\times$ if and only if $\rho(\mathcal{O}_{S,F}^\times) = 0 \in \mathbb{F}_\ell$, i.e., for each $u \in \mathcal{O}_{S,F}^\times$ we have $\rho(u) = 0$. Define $\mathcal{A} := \mathcal{O}_{F,S}^\times / (\mathcal{O}_{F,S}^\times)^\ell$, and for each $u \in \mathcal{A}$, we also abuse the notation u to mean a representative in $\mathcal{O}_{F,S}^\times$, then it suffices to test $\rho(u) = 0$ for every $u \in \mathcal{A}$.

We define the characters t_u and χ to be

$$t_u(\rho) = \begin{cases} 1, & \text{if } \rho(u) = 0 \\ 0, & \text{if } \rho(u) \neq 0, \end{cases} \text{ and } \chi(\rho) = \begin{cases} 1, & \text{if } \rho(\mathcal{O}_{S,F}^\times) = 0, \\ 0, & \text{if otherwise.} \end{cases}$$

Say $u_1, \ldots, u_n$ is a basis for $\mathcal{A}$ with $t_{u_i}(\rho) = 1$ for each i, then $\chi(\rho) = 1$. We can also rewrite

$$t_u(\rho) = \frac{1}{\ell} \sum_{0 \leq m \leq \ell-1} \zeta_\ell^{\rho(u^m)},$$

then

$$\chi(\rho) = \prod_{i=1}^n t_{u_i}(\rho) = \prod_{i=1}^n \frac{1}{\ell} \Big(\sum_{0 \leq m \leq \ell-1} \zeta_\ell^{\rho(u_i^m)} \Big) = \frac{1}{|\mathcal{A}|} \Big(\sum_{u \in \mathcal{A}} \zeta_\ell^{\rho(u)} \Big).$$

Now we are ready to give the generating series for all homomorphisms $I_{F,S}/\mathcal{O}_{F,S}^\times \to \mathbb{F}_\ell$ with $\mathrm{rk}(\rho) \leq d$ and $\rho(\pi) = 0$, that is

$$g_d(s) := \sum_{\rho, \mathrm{rk}(\rho) \leq d, \rho(\pi)=0} \frac{\chi(\rho)}{\mathrm{Disc}(\rho)^s} = \frac{1}{|\mathcal{A}|} \sum_{u \in \mathcal{A}} g_{d,u}(s), \text{ where}$$

$$g_{d,u}(s) := \sum_{\rho \in I_{F,S}^\vee, \mathrm{rk}(\rho) \le d, \rho(\pi)=0} \frac{\zeta_\ell^{\rho(u)}}{\mathrm{Disc}(\rho)^s} = \left(\sum_{\rho_{\mathfrak{p}_0} \in U_{\mathfrak{p}_0,d}^\vee, \rho(\pi)=0} \frac{\zeta_\ell^{\rho_{\mathfrak{p}_0}(u)}}{\mathrm{Disc}(\rho_{\mathfrak{p}_0})^s} \right) \prod_{\mathfrak{p} \neq \mathfrak{p}_0} \left(\sum_{\rho_\mathfrak{p} \in U_{\mathfrak{p},d}^\vee} \frac{\zeta_\ell^{\rho_\mathfrak{p}(u)}}{\mathrm{Disc}(\rho_\mathfrak{p})^s} \right)$$

since $\mathrm{Disc}(\rho)$ and $\zeta_\ell^{\rho(u)}$ are both multiplicative. We then define $\tilde{g}_d(s)$ and $\tilde{g}_{d,u}(s)$ to be exactly the same except replacing $\rho(\pi) = 0$ with $\rho(\pi) \neq 0$. For each $\mathfrak{p} \notin S_k$, we have

$$g_{d,u,\mathfrak{p}}(s) = \sum_{\rho_\mathfrak{p} \in U_{\mathfrak{p},d}^\vee} \frac{\zeta_\ell^{\rho_\mathfrak{p}(u)}}{\mathrm{Disc}(\rho_\mathfrak{p})^s}.$$

We will denote the Euler product supported outside S_k by

$$g_{d,u}(s)' := \prod_{\mathfrak{p} \notin S_k} g_{d,u,\mathfrak{p}}(s), \tag{4.1}$$

and similarly for $\tilde{g}_{d,u}(s)'$.

4.3 Poles of $g_{d,u}(s)$ and $\tilde{g}_{d,u}(s)$

In this section, we are going to consider the right-most pole of $g_{d,u}(s)$ including its order. Recall that $\mathcal{A}_d$ is defined in Definition 3.2. Our main theorem in this section is the following:

Theorem 4.1. *Let $a = a(H(\ell,d))$ and $b = b(H(\ell,d),k)$ be Malle's constants (see Lemma 2.6) and $1 < d < \ell$. For each $u \in \mathcal{A}$, the Dirichlet series $g_{d,u}(s)$ and $\tilde{g}_{d,u}(s)$ have an analytic continuation to the right half plane $\Re(s) \ge 1/a$ except for a possible pole at $s = 1/a$ of order at most b. Moreover, the Euler products $g_{d,u}(s)'$ and $\tilde{g}_{d,u}(s)'$ (the truncated Euler products supported outside S_k in (4.1)) have a pole at $s = 1/a$ of order b if and only if $u \in \mathcal{A}_{\ell-d}$.*

Proof. Firstly, notice that when $\Re(s) \ge 1/a$, the two total series $g_{d,u}(s)$ and $\tilde{g}_{d,u}(s)$ only differ by a holomorphic factor at $\mathfrak{p}_0$ and the truncated ones $g_{d,u}(s)' = \tilde{g}_{d,u}(s)'$ coincide completely. Therefore it suffices to study the poles for $g_{d,u}(s)$.

We denote by $\zeta_L(s)$ the Dedekind-ζ function. For each u and d, we will show that if $u \in \mathcal{A}_{\ell-d}$ then $g_{d,u}(s)' = g_{d,1}(s)' = \zeta_L(as)^b \cdot h(s)$ with $h(s)$ being holomorphic for $\Re(s) \ge 1/a$; if $u \notin \mathcal{A}_{\ell-d}$, then $g_{d,u}(s)'$ has at most a pole at $s = 1/a$ of order strictly smaller than b.

If $u \in \mathcal{A}_{\ell-d}$, then $u \in U_{\mathfrak{p},\ell-d}$ by Theorem 3.7 and by Lemma 3.8, $\rho_\mathfrak{p}(u) = \langle \rho_\mathfrak{p}, u \rangle = 0$. For $\mathfrak{p} \notin S_k$, recall $g_{d,u,\mathfrak{p}}(s)$ is the local factor for $g_{d,u}(s)$ at $\mathfrak{p}$, then

$$g_{d,u,\mathfrak{p}}(s) = g_{d,1,\mathfrak{p}}(s) = \sum_{\rho_\mathfrak{p} \in U_{\mathfrak{p},d}^\vee} \frac{1}{\mathrm{Disc}(\rho_\mathfrak{p})^s},$$

and

$$g_{d,u}(s)' = g_{d,1}(s)' = \prod_{\mathfrak{p} \notin S_k} \left(\sum_{\rho_\mathfrak{p} \in U_{\mathfrak{p},d}^\vee} \frac{1}{\mathrm{Disc}(\rho_\mathfrak{p})^s} \right) = \zeta_{F(\zeta_\ell)}^b(as) \cdot h_d(s),$$

where $h_d(s)$ is holomorphic for $\Re(s) \ge 1/a$. For the last equality, we notice that only primes $\mathfrak{p}$ with $|\mathfrak{p}| \equiv 1(\ell)$ can admit a non-trivial $\rho_\mathfrak{p}$. If $\mathfrak{p}$ is split in F/k, then by the identification between $U_\mathfrak{p}^\vee$ and W_ℓ in Section 3.3, we have $\mathrm{Disc}(\rho_\mathfrak{p}) = |\mathfrak{p}|^{\mathrm{ind}(\rho_\mathfrak{p})} \ge |\mathfrak{p}|^a$ by Lemma 2.6. If $\mathfrak{p}$ is inert in F/k, then we also have $\mathrm{Disc}(\rho_\mathfrak{p}) > |\mathfrak{p}|^a$ since $a < \ell(\ell-1)$ when $d > 1$. And again by Lemma 2.6 the number of ρ_p witnessing $|\mathfrak{p}|^a$ is exactly $|\Phi_d| = \binom{\ell}{d} \cdot (\ell-1)$, which is equal to $b(H(\ell,d),k) \cdot \ell \cdot [k(\zeta_\ell) : k]$ by Lemma 2.6. Then it follows that the order of the pole at $s = 1/a$ is exactly $b(H(\ell,d),k)$.

If $u \notin \mathcal{A}_{\ell-d}$, equivalently $\mathrm{rk}(u) > \ell - d$, then by Theorem 3.7, for every $w|\mathfrak{p}$ in $F(\zeta_\ell)$ that is inert in $F((\sigma-1)^{\ell-d}(u)^{1/\ell}, \zeta_\ell)$, we have $\mathrm{rk}(u_\mathfrak{p}) > \ell - d$. Recall $\chi_d(u)$ from Section 3.3, we can rewrite

$$g_{d,u,\mathfrak{p}}(s) = 1 + \frac{\chi_d(u_\mathfrak{p})}{|\mathfrak{p}|^{as}} + \text{higher order terms in } |\mathfrak{p}|^{-s},$$

for split $\mathfrak{p}$ in F/k with $|\mathfrak{p}| \equiv 1(\ell)$. Here $\chi_d(u_\mathfrak{p}) = |\Phi_d|$ if and only if $u_\mathfrak{p} \in U_{\mathfrak{p},\ell-d}$ if and only if $\mathfrak{p}$ is split in $F((\sigma-1)^{\ell-d}(u)^{1/\ell}, \zeta_\ell)/F(\zeta_\ell)$, and otherwise $\chi_d(u_\mathfrak{p})$ is an integer that is strictly smaller than $|\Phi_d|$. More precisely, for each $\mathfrak{p} \equiv 1(\ell)$, say $\mathfrak{P}|\mathfrak{p}$ is a prime above $\mathfrak{p}$ in F, and $w|\mathfrak{P}$ is a prime above $\mathfrak{P}$ in $F(\zeta_\ell)$, for each local field $F_\mathfrak{P}$, we will fix a generator $y_\mathfrak{P} \equiv \zeta_{|\mathfrak{P}|-1} \mod \mathfrak{P}$ (the global roots of unity in $\bar{\mathbb{Q}}$) for $\mathcal{O}_\mathfrak{P}^\times/(\mathcal{O}_\mathfrak{P}^\times)^\ell$, then by [34, Lemma 2.14], if $\rho_\mathfrak{P}(y_\mathfrak{P}) = m \in \mathbb{F}_\ell$, then

$$\zeta_\ell^{\rho_\mathfrak{P}(u)} = \frac{\mathrm{Frob}_w(u^{m/\ell})}{u^{m/\ell}},$$

where Frob_w can be considered as the local Frobenius automorphism over $F(\zeta_\ell)_w$. If $\mathfrak{p}$ is split in F/k, say $\mathfrak{p}\mathcal{O}_F = \prod_{1\le i\le \ell}\mathfrak{P}_i = \prod_{1\le i\le \ell}\sigma^i(\mathfrak{P})$, then since $F_\mathfrak{P} \simeq F_{\sigma(\mathfrak{P})}$ via σ, the local images of u are related by $u_\mathfrak{P} = \sigma(u)_{\sigma(\mathfrak{P})}$. Denote $u_i := u_{\mathfrak{P}_i}$, then we can also rewrite

$$\chi_d(u_\mathfrak{p}) = \sum_{\rho\in\Phi_d}\prod_{\mathfrak{P}_i|\mathfrak{p}} \zeta_\ell^{\rho_{\mathfrak{P}_i}(u_{\mathfrak{P}_i})} = \sum_{\rho\in\Phi_d}\prod_{\mathfrak{P}_i|\mathfrak{p}} \left(\frac{\mathrm{Frob}_w(u_i^{1/\ell})}{u_i^{1/\ell}}\right)^{m_i},$$

where $\rho(y_{\mathfrak{P}_i}) = m_i \in \mathbb{F}_\ell$. This value $\chi_d(u_\mathfrak{p})$ is therefore completely determined by Frob_w in $L/F(\zeta_\ell)$ where $K := F(\zeta_\ell, u_1^{1/\ell}, \dots, u_\ell^{1/\ell})$, therefore in general the truncated series can be compared to a Hecke L-function of $K/F(\zeta_\ell)$, i.e., there exists $h_{d,u}(s)$ that is holomorphic at $\Re(s) \ge 1/a$ such that

$$g_{d,u}(s)' = L(\chi_{K/F(\zeta)}, as)\cdot h_{d,u}(s).$$

We thus showed that $g_{d,u}(s)'$ is holomorphic at $\Re(s) \ge 1/a$ except at $s = 1/a$. By Chebotarev density theorem, the density of primes in $F(\zeta_\ell)$ that has $\chi_d(u_\mathfrak{p}) = |\Phi_d|$ is $1/\ell$ by Theorem 3.7. Therefore when $u \notin \mathcal{A}_{\ell-d}$, the order of the possible pole for $g_{d,u}(s)'$ at $s = 1/a$ is strictly smaller than b. □

Remark 4.2. *For $d = \ell$, the series $g_d(s) + \tilde{g}_d(s)$ is exactly the Dirichlet series for C_ℓ-extensions over F, which was studied before in [35, 34].*

Remark 4.3. *For $d = 1$, both $H(\ell, 1)$ and $\tilde{H}(\ell, 1)$ are abelian groups and are studied in [35, 34], but not by understanding $g_{1,u}(s)$. Let $a = (\ell-1)\ell$ and $b = (\ell-1)/[k(\zeta_\ell) : k]$. Using the method above, we can see that $g_{1,u}(s)' = \tilde{g}_{1,u}(s)'$ for $u = 1$ differ from $\zeta_{k(\zeta_\ell)}^b(as)$ by a holomorphic factor. The only difference is that inert primes $\mathfrak{P}$ in F/k with $|\mathfrak{P}| \equiv 1(\ell)$ can also contribute $\rho_\mathfrak{p}$ with $\mathrm{Disc}(\rho_\mathfrak{p}) = |\mathfrak{p}|^a$ in this case. For general u, the series $g_{1,u}(s)' = \tilde{g}_{1,u}(s)'$ differ from an Artin L-function $L(\chi_{K/k(\zeta)}, as)$ by a holomorphic factor where $K := F(\zeta_\ell, u_1^{1/\ell}, \dots, u_\ell^{1/\ell})$. Overall, the two series $g_1(s)$ and $\tilde{g}_1(s)$ both have a holomorphic continuation to $\Re(s) \ge 1/a$ and have at most a pole at $s = 1/a$ of order at most b.*

4.4 Asymptotic Behavior of $N_{F/k}(H(\ell, d), X)$ and $N_{F/k}(\tilde{H}(\ell, d), X)$

In this section, we give the asymptotic estimate for

$$N_{F/k}(H(\ell,d), X) := \sharp\{L/F \mid \mathrm{Gal}(L/k) = H(\ell,d) \le S_{\ell^2}, \mathrm{Gal}(L/F) = C_\ell, \mathrm{Disc}(L/F) \le X\},$$

and $N_{F/k}(\tilde{H}(\ell, d), X)$ defined similarly when $1 < \ell < d$. We first state a lemma on the existence of twisted Heisenberg extensions for any given F/k.

Proposition 4.4 ([11], Corollary 3.7)**.** *Let F/k be a C_ℓ-extension of (abstract) fields for an odd prime ℓ. Then there exists an extension L/F with* $\mathrm{Gal}(L/k) = \tilde{H}(\ell,1)$ *or* $\tilde{H}(\ell,2)$.

Note that this proposition also guarantees the existence of extensions L/F with $\mathrm{Gal}(L/k) = \tilde{H}(\ell,d)$ for $2 \le d < \ell$, e.g. see [11, Prop. 4.1] or consider the proof of the following theorem.

Theorem 4.5. *Let $a = a(H(\ell,d)) = a(\tilde{H}(\ell,d))$ and $b = b(H(\ell,d),k) = b(\tilde{H}(\ell,d),k)$ for $1 < d < \ell$ and an odd prime ℓ. Then for each C_ℓ-extension F/k there exist $C_{d,F} > 0$ and $\tilde{C}_{d,F} > 0$ such that*

$$N_{F/k}(H(\ell,d),X) \sim C_{d,F} X^{1/a} \log^{b-1} X,$$

and

$$N_{F/k}(\tilde{H}(\ell,d),X) \sim \tilde{C}_{d,F} X^{1/a} \log^{b-1} X.$$

Proof. The partial sum $N_{F/k}(H(\ell,d),X)$ has the Dirichlet series $g_d(s) - g_{d-1}(s)$ where $g_d(s) = \frac{1}{|\mathcal{A}|}\sum_{u\in\mathcal{A}} g_{d,u}(s)$ by Theorem 3.6, similarly for $N_{F/k}(\tilde{H}(\ell,d),X)$. It suffices to prove that both Dirichlet series have a pole at $s = 1/a$ of order b, then the theorem follows by a Tauberian theorem [27, p. 121].

Firstly, notice that $a(H(\ell,d-1)) > a(H(\ell,d))$ (for $d = 2$, we have $a(H(\ell,1)) = \ell(\ell-1)$ in Remark 4.3), therefore it suffices to show for each d, that the series $g_d(s)$ and $\tilde{g}_d(s)$ have a pole at $s = 1/a$ of exact order b. In Theorem 4.1, we have proved that for each $u \in \mathcal{A}$, the Euler products $g_{d,u}(s)'$ and $\tilde{g}_{d,u}(s)'$ have at most a pole at $s = 1/a$ of order at most b. The series $g_{d,u}(s)$ only differ from $g_{d,u}(s)'$ by finitely many holomorphic local factors at S when $s \ge 1/a$, thus the Dirichlet series $g_d(s)$ and $\tilde{g}_d(s)$ are also holomorphic at $\Re(s) \ge 1/a$ with at most a pole at $s = 1/a$ of order at most b. On the other hand, to show the pole at $s = 1/a$ for $g_d(u)$ has exactly order b, it suffices to show a lower bound for the number of $\rho \in C_F^\vee$ with $\mathrm{rk}(\rho) \le d$, $\rho(\pi) = 0$ and $\mathrm{Disc}(\rho) \le X$ in the order of $X^{1/a}\log^{b-1} X$ for $1 < d < \ell$, because otherwise we will get a contradiction from the Tauberian theorem. Similarly for $\tilde{g}_d(s)$.

Firstly, we consider the subset $\mathcal{S}$ of C_ℓ-extensions of F that are split at every prime in S. This corresponds to counting $\rho : I_{F,S}/\mathcal{O}_{F,S}^\times \to \mathbb{F}_\ell$ with $\mathrm{rk}(\rho) \le d$ and $\rho_\mathfrak{p}$ is trivial for all $\mathfrak{p} \in S_k$. Notice that this subset of ρ has generating series

$$g_d(s)' := \sum_{\rho,\mathrm{rk}(\rho)\le d,\forall \mathfrak{p}\in S_k:\rho_\mathfrak{p}=0} \frac{\chi(\rho)}{\mathrm{Disc}(\rho)^s} = \frac{1}{|\mathcal{A}|}\sum_{u\in\mathcal{A}} g_{d,u}(s)' = \frac{|\mathcal{A}_{\ell-d}|}{|\mathcal{A}|} g_{d,1}(s)' + \frac{1}{|\mathcal{A}|}\sum_{u\notin\mathcal{A}_{\ell-d}} g_{d,u}(s)', \tag{4.2}$$

where $g_{d,u}(s)'$ is exactly the truncated series of $g_{d,u}(s)$ defined in (4.1), and the last equality follows since $g_{d,u}(s)' = g_{d,1}(s)'$ when $u \in \mathcal{A}_{\ell-d}$ as shown in Theorem 4.1. By Theorem 4.1, the second term in (4.2) has at most a pole at $s = 1/a$ of order strictly smaller than b, and the first term has a pole of order exactly equal to b with $|\mathcal{A}_{\ell-d}| \ge 1$. Therefore by the Tauberian theorem, our subset of C_ℓ-extensions has an asymptotic distribution in the order of $X^{1/a}\log^{b-1} X$. The lower bound for $N_{F/k}(H(\ell,d),X)$ thus follows.

Next we consider the lower bound for $N_{F/k}(\tilde{H}(\ell,d),X)$. By Proposition 4.4, there exists L_0/F with $\mathrm{Gal}(L_0/F) \simeq \tilde{H}(\ell,1)$ or $\tilde{H}(\ell,2)$. Denote $\rho_0 : I_{F,S}/\mathcal{O}_{F,S}^\times \to \mathbb{F}_\ell$ to be the homomorphism corresponding to L_0/F, and $\tilde{\mathcal{S}} := \{\rho + \rho_0 : I_{F,S}/\mathcal{O}_{F,S}^\times \to \mathbb{F}_\ell \mid \rho \in \mathcal{S}\}$. Since $(\sigma-1)^d(\rho+\rho_0) = (\sigma-1)^d(\rho) + (\sigma-1)^d(\rho_0) = 0$ and $\rho + \rho_0(\pi_0) = \rho(\pi_0) + \rho_0(\pi_0) = \rho_0(\pi_0)$, we see that all $\tilde{\rho} = \rho + \rho_0 \in \tilde{\mathcal{S}}$ have $\mathrm{rk}(\tilde{\rho}) \le d$ and $\tilde{\rho}(\pi_0) \ne 0$. On the other hand, at every $\mathfrak{p}$ that is unramified in ρ_0 we have $\mathrm{Disc}(\tilde{\rho}_\mathfrak{p}) = \mathrm{Disc}(\rho_\mathfrak{p})$, therefore there exists a constant C depending at most on ρ_0 such that $\mathrm{Disc}(\tilde{\rho}) \ge C\,\mathrm{Disc}(\rho)$ for every $\rho \in \mathcal{S}$. It follows that the number of $\tilde{\rho} \in \tilde{\mathcal{S}}$ with $\mathrm{Disc}(\tilde{\rho}) \le X$ is at least $X^{1/a}\log^{b-1} X$. □

4.5 Summation

In this section, we sum up $N_{F/k}(H(\ell,d),X)$ and $N_{F/k}(\tilde{H}(\ell,d),X)$ over all F/k and prove our main theorem. We first give an upper bound for $N_{F/k}(H(\ell,d),X)$ and $N_{F/k}(\tilde{H}(\ell,d),X)$ with a uniform dependence on $\mathrm{Disc}(F)$. The method closely follows the idea in [29].

Lemma 4.6. *Let ℓ be an odd prime. For each $1<d<\ell$, let $a=a(H(\ell,d))=a(\tilde{H}(\ell,d))$ and $b=b(H(\ell,d),k)=b(\tilde{H}(\ell,d),k)$. Then we have for all $\epsilon>0$*

$$N_{F/k}(H(\ell,d),X)=O_{k,\epsilon}(\mathrm{Disc}(F)^{\epsilon}X^{1/a}\log^{b-1}X),$$

and

$$N_{F/k}(\tilde{H}(\ell,d),X)=O_{k,\epsilon}(\mathrm{Disc}(F)^{\epsilon}X^{1/a}\log^{b-1}X).$$

Proof. In order to determine an upper bound for both counting functions, it suffices to give an upper bound for the partial sum of $g_d(s)+\tilde{g}_d(s)$ with a uniform dependence on $\mathrm{Disc}(F)$. The series $g_d(s)+\tilde{g}_d(s)$ is the Dirichlet series for $\rho\in C_F^{\vee}$ with $\mathrm{rk}(\rho)\le d$.

Class field theory gives the following exact sequence

$$1\to\mathcal{O}_F^{\times}\to\prod_{\mathfrak{P}}\mathcal{O}_{\mathfrak{P}}^{\times}\to C_F\to\mathrm{Cl}_F\to 1,$$

which induces the sequence

$$0\to\mathrm{Cl}_F^{\vee}\to C_F^{\vee}\to(\prod_{\mathfrak{P}}\mathcal{O}_{\mathfrak{P}}^{\times})^{\vee},$$

where the left term in the sequence is bounded by $|\mathrm{Cl}_F^{\vee}|=|\mathrm{Cl}_F[\ell]|=O_{\epsilon,k}(\mathrm{Disc}(F)^{\epsilon})$ for all $\epsilon>0$ by [21]. Since the maps in the sequences above are all $\mathrm{Gal}(F/k)$-equivariant, for all $\rho\in(C_F^{\vee})_d$, their restriction to $(\prod_{\mathfrak{P}}\mathcal{O}_{\mathfrak{P}}^{\times})^{\vee}$ also has at most rank d. The Dirichlet series for $\rho\in(\prod_{\mathfrak{P}}\mathcal{O}_{\mathfrak{P}}^{\times})_d^{\vee}$ is

$$\prod_{\mathfrak{p}}\left(\sum_{\rho_{\mathfrak{p}}\in(\prod_{\mathfrak{P}\mid\mathfrak{p}}\mathcal{O}_{\mathfrak{P}}^{\times})_d^{\vee}}\frac{1}{\mathrm{Disc}(\rho_{\mathfrak{p}})^s}\right)=\zeta_{F(\zeta_\ell)}^b(as)\cdot q_d(s),\qquad \Re(s)>1/a,$$

where $q_d(s)$ is a holomorphic factor that can be bounded absolutely only in terms of $[k:\mathbb{Q}]$ and ℓ. Now we denote by a_n be the number of $\rho\in(\prod_{\mathfrak{P}}\mathcal{O}_{\mathfrak{P}}^{\times})_d^{\vee}$ with $\mathrm{Disc}(\rho)=n$. Then by Perron's formula we have

$$\sum_{n\le X}a_n\le\sum_n a_n e^{1-n/X}=\frac{e}{2\pi i}\int_{1+\epsilon-i\infty}^{1+\epsilon+i\infty}\Gamma(s)\cdot\zeta_{F(\zeta_\ell)}^b(as)\cdot q_d(s)\cdot X^s ds.$$

Next we shift the contour integral to $\Re(s)=1/a-\epsilon$. Using a similar argument as in [4], we apply the convexity bound for the Dedekind zeta function $\zeta_{F(\zeta_\ell)}$, see e.g. [16, Equation (5.20)],

$$(s-1)\zeta_{F(\zeta_\ell)}(s)=O_{[F(\zeta_\ell):\mathbb{Q}],\epsilon}(\mathrm{Disc}(F)^{(1-\sigma)/2+\epsilon}(1+|s|)^{[F(\zeta_\ell):\mathbb{Q}](1-\sigma)/2+1+\epsilon})\text{ for }0\le\Re(s)=\sigma\le 1,$$

and obtain

$$\begin{aligned}\sum_{n\le X}a_n&\le\mathrm{Res}(\Gamma(s)\cdot\zeta_{F(\zeta_\ell)}^b(as)\cdot q_d(s)'\cdot X^s)_{s=1/a}+O_{[F(\zeta_\ell):\mathbb{Q}],\epsilon}(\mathrm{Disc}(F)^{\epsilon/2}X^{1/a-\epsilon})\\&=O_{[F(\zeta_\ell):\mathbb{Q}],\epsilon}(\mathrm{Disc}(F)^{\epsilon}X^{1/a}\log^{b-1}X).\end{aligned}$$

□

Now we are ready to give the proof of the main theorem.

Proof of Theorem 1.1. Fix G to be $H(\ell,d) \leq S_{\ell^2}$ or $\tilde{H}(\ell,d) \leq S_{\ell^2}$ for $1 < d < \ell$. By Theorem 4.5, for each F/k, we get that the number of L/F with $\mathrm{Gal}(L/k) \simeq G$ and $\mathrm{Disc}(L/k) < X$ is

$$N_{F/k}(G, \frac{X}{\mathrm{Disc}(F)^{\ell}}) \sim \frac{C_F}{\mathrm{Disc}(F)^{\ell/a(G)}} X^{1/a(G)} \log^{b(G,k)-1} X.$$

For each $Y > 0$, we define an approximation of $N_k(G,X)$ by

$$N_Y(X) := \sum_{F, \mathrm{Disc}(F)<Y} N_{F/k}(G, \frac{X}{\mathrm{Disc}(F)^{\ell}}) \sim C_Y X^{1/a(G)} \log^{b(G,k)-1} X,$$

here the asymptotic estimate follows since it is a finite sum. The constant C_Y is monotonically increasing as Y increases, and is uniformly bounded from above by Lemma 4.6 via a partial summation over F, therefore $C := \lim_{Y\to\infty} C_Y$ exists.

By definition $N_Y(X) \leq N(X)$ gives a lower bound for $N(X)$. Therefore for any $Y > 0$,

$$C_Y = \lim_{X\to\infty} \frac{N_Y(X)}{X^{1/a(G)} \log^{b(G,k)-1} X} \leq \liminf_{X\to\infty} \frac{N_k(G,X)}{X^{1/a(G)} \log^{b(G,k)-1} X}. \tag{4.3}$$

Letting Y go to infinity, we have

$$C := \lim_{Y\to\infty} C_Y \leq \liminf_{X\to\infty} \frac{N_k(G,X)}{X^{1/a(G)} \log^{b(G,k-1} X}. \tag{4.4}$$

This gives a lower bound for $N_k(G,X)$.

For the upper bound on $N_k(G,X)$, notice that

$$\frac{N_k(G,X)}{X^{1/a(G)} \log^{b(G,k)-1} X} = \frac{N_Y(X)}{X^{1/a(G)} \log^{b(G,k)-1} X} + \frac{N_k(G,X) - N_Y(X)}{X^{1/a(G)} \log^{b(G,k)-1} X}.$$

By the uniform bound in Lemma 4.6 and a partial summation, we have

$$\begin{aligned} N_k(G,X) - N_Y(X) = &\sum_{F, \mathrm{Disc}(F)>Y} N_{F/k}(G, \frac{X}{\mathrm{Disc}(F)^{\ell}}) \leq \sum_{F, \mathrm{Disc}(F)>Y} O_{k,\epsilon}(\frac{X^{1/a(G)} \log^{b(G,k)-1} X}{\mathrm{Disc}(F)^{\ell/a(G)-\epsilon}}) \\ =&X^{1/a(G)} \log^{b(G,k)-1} X \cdot O_{k,\epsilon}(Y^{-\ell/a(G)+1/(\ell-1)+\epsilon}). \end{aligned} \tag{4.5}$$

When $1 < d < \ell$, we have $a(G) = (\ell - d + 1) \cdot (\ell - 1) < \ell(\ell - 1)$, therefore by letting Y go to infinity, we obtain

$$\lim_{Y\to\infty} \limsup_{X\to\infty} \frac{N_k(G,X)}{X^{1/a(G)} \log^{b(G,k)-1} X} \leq \lim_{Y\to\infty} C_Y = C. \tag{4.6}$$

The theorem follows by combining the lower bound and the upper bound on $N_k(G,X)$. □

References

[1] B. Alberts. The weak form of Malle's conjecture and solvable groups. *Res. Number Theory*, 6(1):Art. 10, 23, 2020.

[2] B. Alberts. Statistic of the first Galois cohomology group: A refinement of Malle's conjecture. *Algebra & Number Theory*, 15-10:2513–2569, 2021.

[3] B. Alberts and E. O'Dorney. Harmonic analysis and statistics of the first galois cohomology group. *Research in Mathematical Sciences*, 8(50), 2021.

[4] B. Alberts, R. J. L. Oliver, J. Wang, and M. M. Wood. Inductive methods for proving Malle's conjecture. Preprint, 2021.

[5] S. A. Altug, A. Shankar, I. Varma, and K. H. Wilson. The number of quartic D_4-fields ordered by conductor. *ArXiv: 1704.01729*, 2017.

[6] K. Belabas and E. Fouvry. Discriminants cubiques et progressions arithmetiqués. *Int. J. Number Theory*, 6(7):1491–1529, 2010.

[7] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math.*, 162(2):1031–1063, 2005.

[8] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math.*, 172(3):1559–1591, 2010.

[9] M. Bhargava, A. Shankar, and X. Wang. Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces. *ArXiv: 1512.03035*, 2015.

[10] M. Bhargava and M. M. Wood. The density of discriminants of S_3-sextic number fields. *Proc. Amer. Math. Soc.*, 136(5):1581–1587, 2008.

[11] S. Chebolu, J. Mináč, and A. Schultz. Galois p-groups and Galois modules. *Rocky Mountain J. Math.*, 46(5):1405–1446, 2016.

[12] H. Cohen, F. D. y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.*, 133(1):65–93, 2002.

[13] B. Datskovsky and D. J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math*, (386):116–138, 1988.

[14] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London. Ser. A*, 322(1551):405–420, 1971.

[15] E. Fouvry and P. Koymans. Malle's conjecture for nonic Heisenberg extensions. *ArXiv: 2102.09465*, 2021.

[16] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[17] J. Klüners. A counter example to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.

[18] J. Klüners. The distribution of number fields with wreath products as Galois groups. *Int. J. Number Theory*, (8):845–858, 2012.

[19] J. Klüners. The asymptotics of nilpotent Galois groups, 2020. ArXiv:2011.04325.

[20] J. Klüners and G. Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math*, 572:1–26, 2004.

[21] J. Klüners and J. Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group. *ArXiv: 2003.12161*, 2020.

[22] P. Koymans and C. Pagano. On Malle's conjecture for nilpotent groups, I. *ArXiv: 2103.17223*, 2021.

[23] S. Mäki. On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Diss. Series A I. Mathematica Dissertationes*, 54(104), 1985.

[24] G. Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[25] G. Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[26] R. Masri, F. Thorne, W. L. Tsai, and J. Wang. Malle's conjecture for $G \times A$, with $G = S_3, S_4, S_5$. *ArXiv:2004.04651*, 2020.

[27] W. Narkiewicz. *Number theory*. World Scientific Publishing Co., Singapore, 1983.

[28] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323. Springer-Verlag, Berlin, second edition, 2008.

[29] R. L. Oliver, J. Wang, and M. M. Wood. Average of 3-torsion in class groups of 2-extensions. *ArXiv: 2110.07712*, 2021.

[30] F. Thorne and H. Cohen. Dirichlet series associated to cubic fields with given quadratic resolvent. *Michigan Math Journal*, 63(2):253–273, 2014.

[31] F. Thorne and H. Cohen. Dirichlet series associated to quartic fields with given resolvent. *Research in Number Theory*, 2, 2016.

[32] J. Wang. Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$. *Compos. Math.*, 157(1):83–121, 2021.

[33] W. C. Waterhouse. The normal closures of certain Kummer extensions. *Canad. Math. Bull.*, 37(1):133–139, 1994.

[34] M. M. Wood. On the probabilities of local behaviors in abelian field extensions. *Compositio Math.*, 146(1):102–128, 2010.

[35] D. J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1):1300–1320, 1989.