Title
Distribution of Class Groups

Author
Wang, Weitong

Publication Date
2022

Peer reviewed|Thesis/dissertation

Distribution of Class Groups

by

Weitong Wang

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Melanie Wood, Co-chair
Professor Sug Woo Shin, Co-chair
Professor Kenneth Ribet

Spring 2022

Distribution of Class Groups

Abstract

Distribution of Class Groups

by

Weitong Wang

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Melanie Wood, Co-chair

Professor Sug Woo Shin, Co-chair

One goal of this thesis is to prove theorems that elucidate the Cohen-Lenstra-Martinet conjectures for the distributions of class groups of number fields, and further the understanding of their implications. We start by giving a simpler statement of the conjectures. We show that the probabilities that arise are inversely proportional to the number of automorphisms of structures slightly larger than the class groups. We find the moments of the Cohen-Lenstra-Martinet distributions and prove that the distributions are determined by their moments. In order to apply these conjectures to class groups of non-Galois fields, we prove a new theorem on the capitulation kernel (of ideal classes that become trivial in a larger field) to relate the class groups of non-Galois fields to the class groups of Galois fields. We then construct an integral model of the Hecke algebra of a finite group, show that it acts naturally on class groups of non-Galois fields, and prove that the Cohen-Lenstra-Martinet conjectures predict a distribution for class groups of non-Galois fields that involves the inverse of the number of automorphisms of the class group as a Hecke-module. The Cohen-Lenstra-Martinet Heuristics give a prediction for the distribution for the p-Sylow subgroups of the class groups of random Γ-number fields when $p \nmid |\Gamma|$. In this thesis, we prove several results on the distributions of the class groups for some $p||\Gamma|$, and show that the behaviour is qualitatively different than the predicted behaviour when $p \nmid |\Gamma|$. We do this by using genus theory and the invariant part of the class group to investigate the algebraic structure of the bad part of the class group. For general number fields, our result is conditional on a natural conjecture on field counting. For abelian or D_4 fields, our result is unconditional.

Contents

Acknowledgments

Chapter 2 is based on the joint work with Melanie Wood [59]. The author would like to thank Melanie Wood, Yuan Liu, and Jiuya Wang for useful conversations related to this work.

Chapter 1

Introduction

1.1 Introduction

In this paper we prove several results to help elucidate the Cohen-Lenstra-Martinet conjectures [12, 14] for the distributions of class groups of number fields, and to further the understanding of their implications. In Section 2.1, we explain the statement of the conjectures in the framework of probability theory. In Section 2.2, we prove a result about the terms appearing in the Cohen-Lenstra-Martinet conjectures. In particular, we prove certain expressions given by Cohen and Martinet are equal to simpler expressions, which allows us to conclude the following. (See Conjecture 2.1.3 and Theorem 2.2.1 for precise statements.)

Theorem 1.1.1. *For every finite group Γ and subgroup Γ_∞, among Galois number fields K with isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \simeq \Gamma$ (i.e. Γ-fields) and decomposition group Γ_∞ at ∞, the Cohen-Lenstra-Martinet conjectures predict that*

$$\mathrm{Prob}(\mathrm{Cl}_K \otimes_{\mathbb{Z}} \mathbb{Z}[|\Gamma|^{-1}] \cong H) = \frac{c}{|H^{\Gamma_\infty}||\operatorname{Aut}_\Gamma(H)|},$$

where Cl_K is the class group of K, and c is a constant, and H is any finite $\mathbb{Z}[|\Gamma|^{-1}, \Gamma]$-module with $H^\Gamma = 1$.

The original philosophy of the Cohen-Lenstra-Martinet conjectures, going back to Cohen and Lenstra [12], is that objects should appear with frequency inversely proportional to their number of automorphisms. So we naturally ask why there is an $|H^{\Gamma_\infty}|$ term in the above predictions. In Section 2.3, we slightly enlargen the class group to the Galois group over $\mathbb{Q}$ of the Hilbert class field of K, with the data of a decomposition group at ∞. We consider, for the first time, the distributions of these larger structures, which we call *class triples*. We show that a class triple is determined by the class group and decomposition group at ∞, and the number of automorphisms of the class triple is exactly $|H^{\Gamma_\infty}||\operatorname{Aut}_\Gamma(H)|$, explaining the probabilities above. Bartel and Lenstra [3] have given a different approach to this question by giving conjectures about the distribution of Arakelov class groups based on those groups appearing with frequency inversely proportional to their number of automorphisms

(which takes some work to make precise, see [2]). Their predicted distribution on Arakelov class groups then pushes forward to the Cohen-Lenstra-Martinet distribution, over any base number field.

In Section 2.4, we determine the moments, which are important averages of the Cohen-Lenstra-Martinet distributions on finite abelian Γ-modules.

Theorem 1.1.2 (Moments)**.** *For every finite group Γ and subgroup Γ_∞, if X is a random $\mathbb{Z}[|\Gamma|^{-1},\Gamma]$-module with the Cohen-Lenstra-Martinet distribution for Γ-fields with decomposition group Γ_∞ at ∞, then for every finite $\mathbb{Z}[|\Gamma|^{-1},\Gamma]$-module H with $H^\Gamma = 1$, we have the H-*moment *of X is*

$$\mathbb{E}(|\operatorname{Sur}_\Gamma(X,H)|) = |H^{\Gamma_\infty}|^{-1}.$$

Here $\operatorname{Sur}_\Gamma(X,H)$ denotes the surjective Γ-module homomorphisms from X to H. See Theorem 2.2.1 and Theorem 2.4.2 for precise statements. These moments are the most important averages of the Cohen-Lenstra-Martinet distributions. (See [11, Section 3.3] on why they are called moments.) The only non-trivial predicted averages of the Cohen-Lenstra-Martinet conjectures that have been proven are the $\mathbb{Z}/3\mathbb{Z}$-moment of the class groups of quadratic fields due to Davenport and Heilbronn [16] (and Datskovsky and Wright [15] for quadratic extensions of general global fields) and the $\mathbb{Z}/2\mathbb{Z}$-moment of the class groups of cubic fields due to Bhargava [5]. (There is also more known on the 2-Sylow subgroup of the class groups of quadratic fields; see [22, 55].) When working over $\mathbb{F}_q(t)$ instead of $\mathbb{Q}$, there are also results on the H-moments of class groups, including of Ellenberg, Venkatesh, and Westerland [20] and the second author [63] for quadratic extensions, and of Liu, the second author, and Zureick-Brown [38] for Γ-extensions, showing that as $q \to \infty$ the moments match those in Theorem 1.1.2. The paper [51] of Pierce, Turnage-Butterbaugh, and the second author explains how the Cohen-Lenstra-Martinet conjectures for the moments of class groups are related to other important conjectures in number theory, including the ℓ-torsion conjecture for class groups, the discriminant multiplicity conjecture, generalized Malle's conjecture, and the count of elliptic curves with fixed conductor. So given the relative accessibility and the centrality of these moments, Theorem 1.1.2 is useful because it tells us what moments the Cohen-Lenstra-Martinet conjectures predict.

Moreover, we show that moments determine the Cohen-Lenstra-Martinet distributions uniquely, which is particularly of interest because the moments are the statistics of class groups about which we seem most likely to be able to prove something.

Theorem 1.1.3 (Moments determine distribution)**.** *For every finite group Γ and subgroup Γ_∞, if X is a random $\mathbb{Z}[|\Gamma|^{-1},\Gamma]$-module such that for every finite $\mathbb{Z}[|\Gamma|^{-1},\Gamma]$-module H with $H^\Gamma = 1$, we have*

$$\mathbb{E}(|\operatorname{Sur}_\Gamma(X,H)|) = |H^{\Gamma_\infty}|^{-1}.$$

then X has the Cohen-Lenstra-Martinet distribution for Γ-fields with decomposition group Γ_∞ at ∞.

See Theorems 2.4.11 and 2.4.12 for precise statements. When we restrict to groups whose orders are only divisible by a finite set of primes, we also prove that a sequence of random

variables with these moments in the limit must have the Cohen-Lenstra-Martinet distribution as its limit distribution. Theorem 1.1.3 is part of a long line of work showing results in the same spirit for other categories of groups, including work of Heath-Brown [30, Lemma 17] for elementary abelian p-groups, Ellenberg, Venkatesh, and Westerland [20, Section 8] for finite abelian p-groups, the second author for finite abelian groups [42, Section 8], and Boston and the second author [8, Theorem 1.4] for pro-p groups with a $\mathbb{Z}/2\mathbb{Z}$ action. See [18, 21, 27, 63] for other examples.

Next, we consider the implications of the Cohen-Martinet conjecture for class groups of non-Galois fields. While these conjectures do not directly make claims about class groups of non-Galois fields, when the class groups of non-Galois fields can be given as a function of the class groups of Galois fields, then the Cohen-Martinet conjectures make a prediction for their average. For example, let Γ be a finite group and Γ' a subgroup of Γ. When L is a Γ-field and K is the fixed field $L^{\Gamma'}$, then, localizing away from primes dividing $|\Gamma|$, we have $\mathrm{Cl}_K \otimes_{\mathbb{Z}} \mathbb{Z}[|\Gamma|^{-1}] = (\mathrm{Cl}_L^{\Gamma'}) \otimes_{\mathbb{Z}} \mathbb{Z}[|\Gamma|^{-1}]$ (where the Γ' exponent denotes taking the fixed part). So a conjecture about the distribution of class groups of Γ-fields has a consequence for the distribution of class groups of their Γ'-fixed fields. However, there is also the possibility of using the Cohen-Martinet conjectures, for some primes $p \mid |\Gamma|$, to predict distributions of p-Sylow subgroups $\mathrm{Cl}_{K,p}$ of Cl_K. In order to realize this possibility, we prove a new result in algebraic number theory relating class groups of non-Galois fields to class groups of Galois fields, in particular at primes dividing the order of the Galois group.

Theorem 1.1.4 (Determination of class groups of non-Galois fields from Galois)**.** *Let L/K be an extension of number fields such that $L/\mathbb{Q}$ is Galois with Galois group Γ and let $\Gamma' = \mathrm{Gal}(L/K)$. Let $e_{\Gamma/\Gamma'}$ be the central idempotent of $\mathbb{Q}[\Gamma]$ for the augmentation character for Γ acting on Γ' cosets, and p a prime not dividing the denominator of $e_{\Gamma/\Gamma'}$ and such that $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$ is a maximal order. Then we have an isomorphism*

$$\mathrm{Cl}_{K,p} \xrightarrow{\sim} \left(e_{\Gamma/\Gamma'} \mathrm{Cl}_{L,p}\right)^{\Gamma'},$$

where the subscript p denotes taking the Sylow p-subgroup.

See Theorem 2.5.6 for a precise statement (for relative class groups over an arbitrary base number field). In particular, we note the restriction on p is exactly the condition on p for the Cohen-Martinet conjectures to say something about the distribution of $e_{\Gamma/\Gamma'} \mathrm{Cl}_{L,p}$. So Theorem 1.1.4 allows us to fully determine the implications of the Cohen-Martinet conjectures for the class groups of non-Galois fields.

Moreover, for p, K, L as in Theorem 1.1.4, we have the immediate corollary that the order of the kernel of the capitulation map $\mathrm{Cl}_K \to \mathrm{Cl}_L$ is not divisible by p. The capitulation kernel is very long-studied, but its structure is not well-known. Hilbert's Theorem 94 [31] proves that when L/K is finite, cyclic, and unramified, then the degree $[L : K]$ divides the order of the capitulation kernel. Hilbert then conjectured the Principal Ideal Theorem of class field theory, eventually proved by Artin and Fürtwangler, that every ideal class in K capitulates in the Hilbert class field. Suzuki [57] and Gruenberg and Weiss [29] proved further generalizations showing that the capitulation kernel for unramified abelian extensions

is large. Our theorem above is in the other direction, proving in some cases there is no p-part of the capitulation kernel.

Theorem 1.1.4 implies that the Cohen-Martinet conjectures in principle give a prediction for the distribution of class groups of fields K as above, but the predicted distribution for a finite abelian p-group H is then the sum over $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$-modules G such that $G^{\Gamma'} \simeq H$ (as groups) of the probability for G in the Galois predictions (see Equation (2.5.1)). This prediction does not have the appearance of objects appearing with frequency inversely proportional to their number of automorphisms. However, in Section 2.6, we prove new theorems to give such a perspective on these probabilities, which we now outline.

Of course when $L/\mathbb{Q}$ is Galois, we have that $\mathrm{Gal}(L/\mathbb{Q})$ acts on Cl_L. However, when $K/\mathbb{Q}$ has no automorphisms, one might at first guess that Cl_K has no particular structure other than that of a finite abelian group. We prove, however, that there is always a natural action of a certain ring $\mathfrak{o}$ on Cl_K (depending on the Galois groups of the Galois closure over $\mathbb{Q}$ and K). Given a representation V of finite group Γ over $\mathbb{Q}$ and a subgroup Γ' of Γ, the Hecke algebra $\mathbb{Q}[\Gamma'\backslash\Gamma/\Gamma']$ naturally acts on $V^{\Gamma'}$. We construct an integral model $\mathfrak{o}$ of the Hecke algebra so that the class group $\mathrm{Cl}_{K,p}$ (for K, p, Γ, Γ' as in Theorem 1.1.4) is naturally an $\mathfrak{o}$-module (see Lemma 2.6.4) and prove that our constructed $\mathfrak{o}$ is a maximal order (Corollary 2.6.8). This definition of $\mathfrak{o}$ is particularly delicate at the primes $p \mid |\Gamma'|$, but the proofs require similar work at all p. Note that $\mathfrak{o}$ can be bigger than $\mathbb{Z}$ even when the field K has no automorphisms; see Example 2.6.17 on degree 10 fields with Galois closure with group A_5 and Proposition 2.6.13 in which we prove $\mathfrak{o}$ is trivial if and only if the augmentation character for Γ acting on Γ' cosets is absolutely irreducible.

Moreover, Theorem 1.1.4 and the results in Section 2.6 show that the p-Sylow subgroup of the Γ-module $\mathrm{Cl}_{L,p}$ of a Galois field L containing K determines the $\mathfrak{o}$-module structure of $\mathrm{Cl}_{K,p}$. That shows that the Cohen-Martinet conjectures imply some prediction for the distribution of the $\mathfrak{o}$-modules $\mathrm{Cl}_{K,p}$, and we further prove a simple expression for the prediction in terms of $|\operatorname{Aut}_{\mathfrak{o}}(H)|^{-1}$ by way of the following result.

Theorem 1.1.5 (Cohen-Martinet predicts $|\operatorname{Aut}_{\mathfrak{o}}(H)|^{-1}$ for non-Galois fields)**.** *Given a finite group Γ and subgroup Γ', for every prime p satisfying the condition of Theorem 1.1.4, and every p-group $\mathfrak{o}$-module H, there is a unique finite $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$-module G such that $G^{\Gamma'} \cong H$ as $\mathfrak{o}$-modules. We also have*

$$\operatorname{Aut}_{e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}}(G) \simeq \operatorname{Aut}_{\mathfrak{o}}(H).$$

See Theorem 2.6.12 for a related statement precisely on the implications of the Cohen-Martinet conjecture. The key result we prove that allows us to prove Theorem 1.1.5 is Theorem 2.6.7, which gives a Morita equivalence between the categories of $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$-modules and $\mathfrak{o}$-modules. This is the fundamental algebraic property of our integral model $\mathfrak{o}$ of the Hecke algebra.

Note that Theorem 1.1.4 does not require L to be the Galois closure of K. So actually, the Cohen-Lenstra-Martinet heuristics give infinitely many different predictions for the distribution of non-Galois (or Galois) class groups, by taking fixed fields of larger and larger

fields. In Section 2.7, we prove that all of the predicted distributions agree, which is an important internal consistency check on the conjectures.

Theorems 1.1.1, 1.1.2, 1.1.3, and 1.1.5 are theorems in the theory of finite Γ-modules, including in the probability theory of random finite Γ-modules. Even though we have proven them to specifically elucidate conjectures about class groups, we expect them, especially Theorems 1.1.2 and 1.1.3 to have applications in other contexts. Distributions related to the Cohen-Lenstra distribution have arisen for predicting the distribution of Tate-Shafarevich groups of elliptic curves [17, 7], and so in order to generalize the predictions of [50] on the asymptotics of elliptic curves of a given rank over $\mathbb{Q}$ to other base global fields, one will need to use an analog of the Cohen-Martinet distributions. Also, beyond number theory, the Cohen-Lenstra distributions on finite abelian groups, and related distributions, have many interesting connections in algebraic combinatorics; see the recent work of Fulman and Kaplan [27] and also [9, 11, 10, 24, 25, 26, 28, 35, 35, 36, 49, 56, 60]. Further, the theorems that moments determine the distribution have been used for determining distributions arising in the theory of random graphs, such as the sandpile groups of Erdös-Rényi and random regular graphs [34, 43, 61]. These theorems on the moments have also been used to show that certain random matrices have cokernels in the Cohen-Lenstra distribution [47, 48, 65], and as an application determine the probability that a random 0/1 rectangular matrix gives a surjective map to $\mathbb{Z}^n$. The Cohen-Lenstra and related distributions have also arisen in questions about random topological spaces [19, 33]. The more general Cohen-Lenstra-Martinet distributions may be relevant in many of these contexts.

Then we are focused on the statistical results of class groups of number fields in comparison with the *Cohen-Lenstra-Martinet Heuristics* (see Cohen and Martinet [14, Hypothèse 6.6] for the original statement), which predict the distribution of p-Sylow subgroups of class groups when p does not divide the order of the Galois group. The heuristics Theorem 1.1.1 imply that for all $r = 0, 1, 2, \ldots$

$$\mathbb{P}(\mathrm{rk}_p \operatorname{Cl}_K \leq r) := \lim_{x\to\infty} \frac{\sum_{P(K)<x} \mathbf{1}_{\mathrm{rk}_p \leq r}(K)}{\sum_{P(K)<x} 1} = \mathbb{P}(\mathrm{rk}_p X \leq r) > 0,$$
$$\text{and } \lim_{r\to\infty} \mathbb{P}(\mathrm{rk}_p \operatorname{Cl}_K \leq r) = \lim_{r\to\infty} \mathbb{P}(\mathrm{rk}_p X \leq r) = 1,$$

where $\mathbf{1}_{\mathrm{rk}_p \leq r}(K)$ is the indicator of $\mathrm{rk}_p \operatorname{Cl}_K \leq r$. For Galois number fields, Wood and the author [59] compute $\mathbb{E}(|\operatorname{Hom}(X, A)|)$, the A-moments for X, which shows that the heuristics imply that

$$\mathbb{E}(|\operatorname{Hom}(\operatorname{Cl}_K, A)|) := \frac{\sum_{P(K)<x} |\operatorname{Hom}(\operatorname{Cl}_K, A)|}{\sum_{P(K)<x} 1} < \infty,$$

for all finite abelian p-groups A. Note that here we forget the Γ-module structure for the convenience of our discussion. Moreover, Wood and the author [59] have shown that the analogous statements for all non-Galois number fields $K/\mathbb{Q}$ follow from the Cohen-Lenstra-Martinet Heuristics. To be precise, if the conjecture holds for the Galois closure Γ-extensions $L/\mathbb{Q}$ with some $p \nmid |\Gamma|$, then the statistical distribution of $\operatorname{Cl}_K[p^\infty]$ is given by a particular

random module X, and that for all $r = 0, 1, 2, \ldots$, we have

$$\mathbb{P}(\mathrm{rk}_p \mathrm{Cl}_K \leq r) := \lim_{x\to\infty} \frac{\sum_{P(K)<x} \mathbf{1}_M(K)}{\sum_{P(K)<x} 1} > 0$$
$$\text{and } \mathbb{E}(|\operatorname{Hom}(\mathrm{Cl}_K, A)|) := \frac{\sum_{P(K)<x} |\operatorname{Hom}(\mathrm{Cl}_K, A)|}{\sum_{P(K)<x} 1} < \infty,$$

for all finite abelian p-group A, where K runs over all number fields $K/\mathbb{Q}$ such that its Galois closure $\hat{K}/\mathbb{Q}$ is a Γ-extension and that $K = \hat{K}^{\Gamma'}$ for a fixed subgroup $\Gamma' \subseteq \Gamma$.

Remark. In the original Cohen-Lenstra-Martinet heuristics, fields are ordered by discriminant, which was an obvious ordering for number fields. Now we have the question of what kind of ordering one should put on the fields, see for example [64]. In some cases, ordering fields by discriminant will contradict what is predicted by the heuristics. See [3] for example. The invariants of number fields that have been used for ordering all rely on the combination of ramified primes, and we are mainly focused on the product of ramified primes, which is denoted by $P(K)$.

In this paper, we are going to discuss the distribution of $\mathrm{Cl}_K[q^\infty]$ where the prime $q||\Gamma|$. We first explain why there is no prediction for such primes in their original statement. Recall the genus theory for quadratic number fields, which says that

$$\omega(P(K)) - 1 \leq \mathrm{rk}_2 \mathrm{Cl}_K \leq \omega(P(K)),$$

where $P(K)$ is the product of ramified primes of $K/\mathbb{Q}$ and $\omega(n)$ is the number of distinct prime divisors for $n \in \mathbb{Z}$. The group $\mathrm{Cl}_K[2^\infty]$ then cannot be described by the approach of the Cohen-Lenstra-Martinet Heuristics. Because, first, given a quadratic number field (say, in terms of its minimal polynomial), we can tell quickly how large its 2-rank should be (up to 1), which is not the case for $\mathrm{Cl}_K[p^\infty]$ where p is odd. This phenomena could be thought of as "predictable", hence contradicting the spirit of the Cohen-Lenstra-Martinet Heuristics. Second, for all $r = 0, 1, 2, \ldots$, we have

$$\mathbb{P}(\mathrm{rk}_2 \mathrm{Cl}_K \leq r) = 0 \quad \text{and} \quad \mathbb{E}(|\operatorname{Hom}(\mathrm{Cl}_K, C_2)|) = +\infty,$$

which is qualitatively different from what is prediceted by the heuristics. According to this example, first, the statistical behaviour of $\mathrm{Cl}_K[2^\infty]$ should be reconsidered, see [23, 55] for example. Second, we want to generalize the genus theory above to all number fields, whose details are given in § 3.1 following the idea of Ishida [32, Chapter 4]. Here we present the main result in a brief way. Given a number field $K/\mathbb{Q}$, and a prime q. If we have ideal factorization $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ such that $\gcd(e_1, \ldots, e_r) \equiv 0 \bmod q$, then we call p a *ramified prime of type* q. For any number field $K/\mathbb{Q}$, define its *genus group* $\mathcal{G}$ to be the Galois group of the maximal unramified extension Kk/K obtained by composing with an abelian extension $k/\mathbb{Q}$. Then genus theory implies the following.

Theorem 1.1.6. *Let $K/\mathbb{Q}$ be a number field with maximal abelian subextension $K_0/\mathbb{Q}$. Fix a rational prime q dividing $n := [K : \mathbb{Q}]$. Then the q-rank of the genus group $\mathcal{G}$ admits the following inequality*

$$\mathrm{rk}_q \mathcal{G} \geq \#\{p \text{ is a ramified prime of type } q \text{ and } p \equiv 1 \bmod q\} - \mathrm{rk}_q \mathrm{Gal}(K_0/\mathbb{Q}).$$

In fact, genus theory is not the only way that can associate ramified primes with ideal classes. P.Roquette and H.Zassenhaus ([54]) construct a subgroup of the class group that is associated to ramified primes. The main theorem of their paper says the following.

Theorem 1.1.7. *Let K be a number field of degree n over $\mathbb{Q}$ and q be a given prime number, then*

$$\mathrm{rk}_q \mathrm{Cl}_K \geq \#\{p \text{ is a ramified prime of type } q\} - 2(n-1)$$

The main difference here compared to genus theory is that we do not require that p has to be 1 mod q to contribute to the lower bound. For more details and comparison between these two theories, see § 3.1.

Since the splitting type of a prime in a field extension $K/\mathbb{Q}$ is determined by its decomposition group, it is then a purely group theoretical problem to find out all primes q so that we can apply the above Theorems 1.1.6 and 1.1.7 and expect to get nontrivial estimate for $\mathrm{rk}_q \mathrm{Cl}_K$.

Definition 1.1.8. Let $1 \leq G \leq S_n$ be a finite transitive permutation group. Let $\sigma \in G$ be any permutation. Define $e(\sigma) := \gcd(|\langle\sigma\rangle \cdot 1|, \ldots, |\langle\sigma\rangle \cdot n|)$, i.e., the greatest common divisor of the size of orbits. We call q a *non-random prime* for G if $q|e(\sigma)$ for some $\sigma \in G$. On the other hand, for a permutation $\sigma \in G$, if $q^l \| e(\sigma)$, then we call σ an element *of inertia type* q^l. Define $\Omega(G, q^l)$ to be the subset of G consisting of all elements of inertia type q^l. We denote $\bigcup_{l=1}^{\infty} \Omega(G, q^l)$ by $\Omega(G, q^\infty)$.

Example 1.1.9. First let $G = S_3$. If K is a non-Galois cubic number field, then the permutation action of G on $K \to \mathbb{C}$ is exactly the conventional action of S_3 on $\{1, 2, 3\}$, which induces the isomorphism $G \cong \mathrm{Gal}(\hat{K}/\mathbb{Q})$. By checking the elements of S_3, we see that 3 is a non-random prime for G, e.g., 3 divides the length of (123). Using the language in Theorem 1.1.7, totally ramified primes satisfy the condition that $e_K(p) \equiv 0 \bmod 3$, in other words totally ramified primes are just ramified primes of type 3, hence

$$\mathrm{rk}_3 \mathrm{Cl}_K \geq \#\{p \text{ is totally ramified}\} - 4.$$

This example explains the terminology, "non-random primes", from the aspect of Theorem 1.1.7.

Given a transitive permutation group $1 \leq G \leq S_n$, and a non-random prime q for G, we first make the following conjecture on counting fields based on the Malle-Bhargava Heuristics (see [41, 4, 62] for example) for counting fields with fixed number of ramified primes. For an extension K/k of number fields, we denote its Galois closure by $\hat{K}$.

Definition 1.1.10. Let $1 \leq G \leq S_n$ be a transitive permutation group, and let k be a number field. Let $\mathcal{S}$ be the set of all number fields $(K/k, \psi)$ such that its Galois closure $(\hat{K}/k, \psi)$ is a G-extension (see Definition 1.2.2), and that $K = \hat{K}^{G_1}$ where G_1 is the stabilizer of 1. Suppose that Ω is a (nonempty) subset of G that is closed under invertible powering, i.e., if $g^a = h$, $h^b = g$, then $g \in \Omega$ if and only if $h \in \Omega$. Define for the set Ω, and for all $r = 0, 1, 2, \ldots,$

$$\mathbf{1}_{(\Omega,r)}(K) := \begin{cases} 1 & \text{if there are exactly } r \text{ primes} p \nmid |G| \\ & \text{s.t. } I(p) \cap \Omega \neq \emptyset; \\ 0 & \text{otherwise.} \end{cases}$$

where $I(p)$ here means the inertia subgroup of p. If the set Ω is clear in the context, we may also denote the function $\mathbf{1}_{(\Omega,r)}(L)$ by $\mathbf{1}_r(L)$ for short.

Conjecture 1.1.11. *Keep $G, k, \mathcal{S}$ as above. Suppose that* $\mathrm{id} \notin \Omega$ *is a (nonempty) subset of G that is closed under invertible powering.*

1. *For all $r = 0, 1, 2, \ldots,$ there exists some r', such that*

$$\sum_{\substack{K \in \mathcal{S} \\ P(K) < x}} \mathbf{1}_{(\Omega,r)}(K) = o\left(\sum_{\substack{K \in \mathcal{S} \\ P(K) < x}} \mathbf{1}_{(\Omega,r')}(K) \right),$$

   In this case we say that the conjecture 1 holds for the pair $(\mathcal{S}, \Omega)$.

2. *For all $r = 0, 1, 2, \ldots,$*

$$\sum_{\substack{K \in \mathcal{S} \\ P(K) < x}} \mathbf{1}_{(\Omega,r)}(K) = o\left(\sum_{\substack{K \in \mathcal{S} \\ P(K) < x}} 1 \right)$$

   In this case we say that the conjecture 2 holds for the pair $(\mathcal{S}, \Omega)$.

Using the conjecture on counting fields, we can present our main statistical result.

Theorem 1.1.12. *Let $1 \leq G \leq S_n$ be a transitive permutation group, and let k be a number field. Let $\mathcal{S}$ be the set of all number fields $(K/k, \psi)$ such that its Galois closure $(\hat{K}/k, \psi)$ is a G-extension, and that $K = \hat{K}^{G_1}$. Let $H \subseteq G$ be a subgroup such that $\hat{K}^H \subseteq K$ for $K \in \mathcal{S}$. If q is a non-random prime for G such that $q | [K : \hat{K}^H]$, and Conjecture 1.1.11(2) holds for $(\mathcal{S}, \Omega)$, where $\Omega := \Omega(G, q^\infty)$, then*

$$\mathbb{P}(\mathrm{rk}_q \mathrm{Cl}(K/\hat{K}^H) \leq r) = 0 \quad \textit{and} \quad \mathbb{E}(|\mathrm{Hom}(\mathrm{Cl}(K/\hat{K}^H), C_q)|) = +\infty,$$

where K runs over fields in $\mathcal{S}$ for the product of ramified primes in $K/\mathbb{Q}$, and $\mathrm{Cl}(K/\hat{K}^H)$ denotes the relative class group.

The zero-probability and infinite moment, that are qualitatively different from the Cohen-Lenstra-Martinet Heuristics, justify the notion "non-random prime" from another point of view. With the help of Class Field Theory and Tauberain Theorems, we can prove the Conjecture 1.1.11(1) for abelian extensions. To be precise, we have the following.

Theorem 1.1.13. *Let Γ be a finite abelian group with a subgroup Λ, and let $\mathcal{S}$ be the set of all abelian Γ-extensions $K/\mathbb{Q}$. If q is a prime number such that $q||\Gamma/\Lambda|$, then the Conjecture 1 holds for $(\mathcal{S}, \Omega)$, where $\Omega := \Omega(\Gamma, q^\infty)$. In addition, we have*

$$\mathbb{P}(\mathrm{rk}_q \mathrm{Cl}(K/K^\Lambda) \leq r) = 0 \quad \textit{and} \quad \mathbb{E}(|\mathrm{Hom}(\mathrm{Cl}(K/K^\Lambda), C_q)|) = +\infty,$$

where K runs over fields in $\mathcal{S}$ for the product of ramified primes in $K/\mathbb{Q}$.

For non-abelian extensions, the first obstacle is counting fields. We present here an example, D_4-fields. Let D_4 be the dihedral group of order 8, and we are going to consider quartic number fields $L/\mathbb{Q}$ whose Galois closure $M/\mathbb{Q}$ are D_4-fields. According to the work of S.A.Altug, A.Shankar, I.Varma, K.H.Wilson [1], the result of counting such fields by *the Artin conductor of 2-dimensional irreducible representation of D_4* is proven. So, the main result in this case can be summarized as follows.

Theorem 1.1.14. *Let $\mathcal{S}$ be the set of quartic number fields $L/\mathbb{Q}$ whose Galois closure are D_4-extensions $M/\mathbb{Q}$. We have*

$$\mathbb{E}_C(|\mathrm{Hom}(\mathrm{Cl}_L, C_2)|) = +\infty,$$

where the subscript C means that the fields $L \in \mathcal{S}$ are ordered by the Artin conductor of 2-dimensional irreducible representation of D_4.

Because of the famous genus theory for quadratic number fields, it is not difficult to prove that

$$\mathbb{P}(\mathrm{Cl}_K \leq r) = 0 \quad \text{and} \quad \mathbb{E}(\mathrm{Hom}(\mathrm{Cl}_K, C_2)|) = +\infty$$

where K runs through all quadratic number fields for discriminant or product of ramified primes. So, it raises the question of the so-called "capitulation". To be precise, the map $i(I) = I\mathscr{O}_L$, where I is an ideal of K, induces the map $i_* : \mathrm{Cl}_K \to \mathrm{Cl}_L$. The kernel $\ker i_*$ is eliminated by 2 in this case. So it is a question how to describe $i_*(\mathrm{Cl}_K[2^\infty])$ and how to estimate it. For the other direction, we can consider the map $\mathbb{Z}_{(p)} \otimes \mathrm{Nm}_{K/L} : \mathrm{Cl}_L[p^\infty] \to \mathrm{Cl}_K[p^\infty]$. It is surjective for every odd prime p. So, the kernel $\mathrm{Cl}(L/K)[p^\infty] := \ker(\mathbb{Z}_{(p)} \otimes \mathrm{Nm}_{K/L})$ can tell us the difference between $\mathrm{Cl}_L[p^\infty]$ and $\mathrm{Cl}_K[p^\infty]$. In the case of 2-Sylow subgroup, the norm map $\mathbb{Z}_{(2)} \otimes \mathrm{Nm}_{K/L}$ is no longer surjective, but $\mathrm{Cl}(L/K)[2^\infty]$ remains a notion that tells the difference between Cl_L and Cl_K philosophically. See also [14, Théorème 7.6] for the discussions on relative class groups. In § 3.5, we will order quartic fields by product of ramified primes and try to discuss this problem under additional hypothesis. We here give the following result. Write $D_4 = \langle \tau, \sigma | \tau^2 = \sigma^4, \tau\sigma\tau^{-1} = \sigma^3 \rangle$.

Lemma 1.1.15. *Let $L/\mathbb{Q}$ be a quartic number field with Galois D_4-closure $M/\mathbb{Q}$, let K be the quadratic subfield of L, and let $I(p)$ be the inertia subgroup of p.*

(i) Let Ω_1 be the set $\{\sigma, \sigma^3, \sigma\tau, \sigma^3\tau\}$. Then we have

$$\mathrm{rk}_2\, i_* \mathrm{Cl}_K \geq |\{p \neq 2 : I(p) \cap \Omega_1 \neq \emptyset\}| - 6.$$

(ii) Let $\Omega_2 := \Omega(D_4, 2^\infty) = \{\sigma, \sigma^3, \sigma^2, \sigma\tau, \sigma^3\tau\}$. Then we have

$$\mathrm{rk}_2\, \mathrm{Cl}(L/K) \geq |\{p \neq 2 : I(p) \cap \Omega_2 \neq \emptyset\}| - 6.$$

We can see from the above result that the concepts non-random prime for G and $\Omega(G, q^l)$ give an estimate of the map $i_* : \mathrm{Cl}_K \to \mathrm{Cl}_L$ and $\mathbb{Z}_{(2)} \otimes \mathrm{Nm}_{L/K} : \mathrm{Cl}_L \to \mathrm{Cl}_K$.

To summarize this section, the notion "good prime" in [14, Définition 6.1] (see also [59, §7]) gives a criterion for us to apply the Cohen-Martinet-Lenstra Heuristics so that we can predict the statistical behaviour of the class groups. In this paper, the notion "non-random prime" predicts the cases when we expect nontrivial subgroup of Cl_K from ramified primes and qualitatively different statistical results from "good prime" cases. However, Example 3.2.2 shows that there are primes p that are neither good in the sense of the heuristics nor non-random in this paper. So, it raises a question: what does $\mathrm{Cl}_K[p^\infty]$ look like, in different point of views?

1.2 Notation

We first attach a list of notions used in the paper here. Throughout the whole chapter, Γ is always a finite group and S is always a set of (possibly infinitely many) rational primes.

Definition 1.2.1. Let K be a number field and $K_0/\mathbb{Q}$ be a subextension of K. We write Cl_K for the class group of K. Then we define the *relative class group* Cl_{K/K_0} to be the subgroup of Cl_K consisting of ideal classes α with trivial norm $\mathrm{Nm}_{K/K_0}\, \alpha$ in Cl_{K_0}. Also, let I_K be the group of fractional ideals and P_K the group of principal fractional ideals of K.

Definition 1.2.2. For a field K_0, by a Γ-*extension of* K_0, we mean an isomorphism class of pairs (K, τ), where K is a Galois extension of K_0, and $\tau : \mathrm{Gal}(K/K_0) \simeq \Gamma$ is an isomorphism. An isomorphism of pairs (K, τ), (K', τ') is an isomorphism $\alpha : K \to K'$ such that the map $m_\alpha : \mathrm{Gal}(K/K_0) \to \mathrm{Gal}(K'/K_0)$ sending ϕ to $\alpha \circ \phi \circ \alpha^{-1}$ satisfies $\tau' \circ m_\alpha = \tau$. We sometimes leave the τ implicit, but this is always what we mean by a Γ-extension. We also call Γ-extensions of $\mathbb{Q}$ Γ-*fields*.

Definition 1.2.3. Define $\mathbb{Z}_S$ to be the localization of $\mathbb{Z}$ by the subset of non-zero integers not divisible by any primes in S, so the maximal ideals of $\mathbb{Z}_S$ are given by the primes in S. For any finite abelian group G, define its S part G^S as the subgroup generated by all p-Sylow subgroups with $p \in S$. (Note that our definition for S-part of G is the opposite of G^S in [14].) We will also use the usual notation $\mathbb{Z}_{(p)}$ for $\mathbb{Z}_S$ when $S = \{p\}$.

Definition 1.2.4. If f is a measurable function on a probability space, we let $\mathbb{P}$ denote the probability measure and $\mathbb{E}(f)$ denote the expected value of f. In this paper, our probability spaces will always be discrete and countable and

$$\mathbb{E}(f) = \sum_{i=1}^{\infty} f(G_i)\mathbb{P}(G_i).$$

Throughout the paper, we often have a ring R, a central idempotent e of R, and then consider the ring eR. The reader is warned that eR is *not* a subring of R in the usual sense, as R and eR do not share an identity. One could consider eR as notation for the quotient $R/(1-e)R$. Then we introduce some notions from analytic number theory.

(i) We use some standard notation coming from analytic number theory. For example, write a complex number as $s = \sigma + it$. Denote the Euler function by $\varphi(n)$. Let $\omega(n)$ counts the number of distinct prime divisors of n and so on.

(ii) If A is an abelian group, then let $\mathrm{rk}_q A$ denote the q-rank of A where q is a given prime number.

(iii) If K is a number field, let rk_K denote the rank of global units of K.

(iv) Let $v_q(n)$ denote the exponent of q in n, i.e., the valuation at q.

Since there are more than one ways to describe field extensions, we give the following two definitions to make the term like "the set of all non-Galois cubic number fields" precise.

Definition 1.2.5. Let Γ be a finite group, and let Γ' be a subgroup of Γ. Let k be a fixed number field. Define $\mathcal{S}(\Gamma, \Gamma'; k)$ to be the set of all pairs (K, ψ), where K/k is a finite extension whose Galois closure L/k is a Γ-extension via $\psi : \mathrm{Gal}(L/\mathbb{Q}) \cong \Gamma$ such that $K = L^{\Gamma'}$. When $k = \mathbb{Q}$, we omit k.

The second definition uses permutation group.

Definition 1.2.6. Given a finite group $G \subseteq S_n$ whose action on $\{1, 2, \ldots, n\}$ is transitive. Let k be a number field. Let $\mathcal{S}(G; k)$ be the set of pairs (K, ψ) such that $[K : k] = n$ and that the group isomorphism $\psi : \mathrm{Gal}(L/k) \cong G$, where L is the Galois closure of K/k, defines the Galois action of G on the k-embeddings $K \to \mathbb{Q}$. If the base field $k = \mathbb{Q}$, then we just omit it and write $\mathcal{S}(G) := \mathcal{S}(G, \mathbb{Q})$.

Intuitively these two definitions make sure that when we count Galois cubic fields in $\bar{\mathbb{Q}}$ we are counting them once. And when we count non-Galois cubic fields, say fixed fields of $(12) \in S_3$, we are counting them without considering their conjugates in a fixed S_3-field. Next, we give the probability notions over a discrete space.

Definition 1.2.7. Let $T = \{a, b, c, \dots\}$ be a set of at most countable objects. If $d : T \to \mathbb{R}^+$ is a map such that for all $N > 0$ the preimage $T_N := d^{-1}[0, N)$ is finite, then for all large enough $N > 0$, one has a discrete probability space (T_N, μ_N) with uniform distribution μ_N. For all function $f : T \to \mathbb{R}$, it induces functions $f : T_N \to \mathbb{R}$ for all large enough $N > 0$. We then define its expectation $\mathrm{E}(f)$ over T for d as

$$\mathrm{E}(f) = \lim_{N\to\infty} \mathrm{E}_N(f) = \lim_{N\to\infty} \int_{T_N} f \,\mathrm{d}\,\mu_N,$$

provided that the limit exists in the sense of $\mathbb{R} \cup \{\pm\infty\}$. The asymptotic of f over T for d is denoted as

$$N(T, d; f; x) := \sum_{s\in T, d(s)<x} f(s).$$

Then we give the notation of counting number fields.

Definition 1.2.8. Let $\mathcal{S} = \mathcal{S}(G; k)$ where G is a transitive permutation group, and let $d : \mathcal{S} \to \mathbb{R}^+$ be an invariant of number fields (e.g. discriminant or product of ramified primes). Define

$$N(\mathcal{S}, d; x) := \sum_{K\in\mathcal{S}, d(K)<x} 1.$$

If f is a function defined over $\mathcal{S}$, then we define

$$N(\mathcal{S}, d; f; x) := \sum_{K\in\mathcal{S}, d(K)<x} f(K).$$

In particular, if $f = \mathbf{1}_{(\Omega,r)}$ (see Definition 1.1.10), then just write

$$N(\mathcal{S}, d; (\Omega, r); x) := N(\mathcal{S}, d; \mathbf{1}_{(\Omega,r)}; x).$$

Using the idea of the expectation, we can define some functions over the set of fields $\mathcal{S}$ and study their expectations.

Definition 1.2.9. Let q be a rational prime, and let $r \geq 0$ be an integer. Define for finite abelian groups with respect to q and r as follows. If A is a finite abelian group, then

$$\mathbf{1}_{\mathrm{rk}_q\leq r}(A) = \begin{cases} 1 & \text{if } \mathrm{rk}_q A \leq r \\ 0 & \text{otherwise.} \end{cases}$$

Definition 1.2.10. Let G be a transitive permutation group, and let $\mathcal{S} := \mathcal{S}(G; k)$, and let q be a rational prime. Let $d : \mathcal{S} \to \mathbb{R}^+$ be an invariant of the number fields, such that $d^{-1}[0, N)$ is finite for all $N > 0$. Given a pair $(K, \psi) \in \mathcal{S}$, we can view Cl as a map $\mathcal{S} \to \mathfrak{Mod}_{\mathbb{Z}}$ according to $(K, \psi) \mapsto \mathrm{Cl}(K/k)$. For all $r = 0, 1, 2, \dots$, define the probability of the q-rank of the class group less than r to be

$$\mathbb{P}(\mathrm{rk}_q \mathrm{Cl}(K/k) \leq r) := \mathrm{E}(\mathbf{1}_{\mathrm{rk}_q\leq r} \circ \mathrm{Cl}(K/k)),$$

provided that the limit exists, where the expectation is over $\mathcal{S}$ for d. Define the A-moment of the relative class groups to be

$$\mathbb{E}(|\operatorname{Hom}(\operatorname{Cl}(K/k), A)|) := \mathrm{E}(|\operatorname{Hom}(\operatorname{Cl}(K/k), A)|),$$

provided that the limit exists where A is any finite abelian q-group, where the expectation is over $\mathcal{S}$ for d.

Note that the definition of the probability and A-moment can be translated to the ratios of asymptotics according to the definition of expectation. For example,

$$\mathbb{E}(|\operatorname{Hom}(\operatorname{Cl}(K/k), A)|) = \lim_{x\to\infty} \frac{N(\mathcal{S}, d; |\operatorname{Hom}(\operatorname{Cl}(K/k), A)|; x)}{N(\mathcal{S}, d; x)}$$

Chapter 2

Moments and interpretations of the Cohen-Lenstra-Martinet heuristics

2.1 Explanation of the Cohen-Lenstra-Martinet Heuristics in the Galois case

The goal of this section is to state Cohen, Lenstra, and Martinet's conjectures on the distribution of relative class groups of Galois extensions. This requires introducing many pieces of notation.

Notations for semisimple $\mathbb{Q}$-algebras

Let A be a finite dimensional semisimple $\mathbb{Q}$-algebra; we denote by $\{e_i\}_{1\leq i\leq m}$ its irreducible *central* idempotents, and $A_i = e_i A$ its simple factors. The algebra A is thus identified with a product $\prod_{i=1}^m A_i$, where each algebra A_i is isomorphic to an algebra of matrices $M_{l_i}(D_i)$, where D_i is a division algebra of finite rank over $\mathbb{Q}$ of which the center is a number field K_i. We let $h_i^2 = \dim_{K_i} A_i$. Let $\mathfrak{O}$ be a maximal order in A and G a finite $\mathfrak{O}$-module. For any $\underline{u} \in \mathbb{Q}^m$, we define

$$|G|^{\underline{u}} := \prod_{i=1}^{m} |e_i G|^{u_i}.$$

(See [52, §10] for basic results on semisimple $\mathbb{Q}$-algebras and maximal orders.)

Notations for the Heuristics

In the rest of this section, we let $A = \mathbb{Q}[\Gamma]$, and continue with the notation above. In particular, we let

$$e_1 = \frac{1}{|\Gamma|} \sum_{\sigma\in\Gamma} \sigma.$$

Each e_i corresponds to a distinct irreducible $\mathbb{Q}$-representation of Γ with character χ_i. We choose a fixed absolutely irreducible character φ_i contained in χ_i.

Now let K_0 be a number field, and K/K_0 a Galois extension with Galois group Γ. If v is an infinite place v of K_0, then let Γ_v be the decomposition group at v. We also define

$$\chi_K = -1 + \sum_{v|\infty} \mathrm{Ind}_{\Gamma_v}^{\Gamma} 1_{\Gamma_v},$$

which is a character of Γ associated to K/K_0.

Definition 2.1.1. We define the rank of K/K_0 to be an $m-1$-tuple in $\mathbb{Q}^{m-1}$ given by the formula

$$\underline{u} = (u_2, \ldots, u_m),\ u_i = \frac{1}{h_i}\langle \chi_K, \varphi_i \rangle \qquad \forall i = 2, \ldots, m. \tag{2.1.1}$$

Remark. For the original definition of rank of K, see [14, Definition 6.4]. These two definitions are equivalent by [14, Theorem 6.7].

Let S be a finite set of primes. We will next define a random module to model the class groups Cl_K^S, which are naturally $(1-e_1)\mathbb{Z}_S[\Gamma]$-modules. Cohen and Martinet did not directly consider the distribution that we will define below. However, as we will prove in this paper, building on tools from [14], the distributions we will now define turn out to be equivalent to the ones considered in [14]. We think there are advantages of viewing the conjecture in multiple equivalent but differently presented forms.

Definition 2.1.2. If $p \in S$ implies that $p \nmid |\Gamma|$, then for $\underline{u} = (u_2, \ldots, u_m) \in \mathbb{Q}^{m-1}$, we define a random variable $X = X((1-e_1)\mathbb{Q}[\Gamma], \underline{u}, (1-e_1)\mathbb{Z}_S[\Gamma])$ to be a random $(1-e_1)\mathbb{Z}_S[\Gamma]$-module such that for all finite $(1-e_1)\mathbb{Z}_S[\Gamma]$-modules G_1, G_2, we have

$$\frac{\mathbb{P}(X \cong G_1)}{\mathbb{P}(X \cong G_2)} = \frac{|G_2|^{\underline{u}}|\ \mathrm{Aut}_\Gamma(G_2)|}{|G_1|^{\underline{u}}|\ \mathrm{Aut}_\Gamma(G_1)|}$$

(where, of course, we order the irreducible central idempotents of $(1-e_1)\mathbb{Q}[\Gamma]$ by the order in $\mathbb{Q}[\Gamma]$).

Remark. It follows from [14, Theorem 3.6] (with their $\underline{u}$ as $\underline{\infty}$ and their $\underline{s}$ as our $\underline{u}$) that this definition is well-defined, i.e., the series

$$\sum_G \frac{1}{|G|^{\underline{u}}|\ \mathrm{Aut}_\Gamma(G)|},$$

is convergent, where G runs through all isomorphism classes of finite $(1-e_1)\mathbb{Z}_S[\Gamma]$-modules. Even when $|S| = \infty$, the series is still convergent as long as $u_i > 0$ for all $i = 1, \ldots, m$. So the above definition can be extended to the case $|S| = \infty$ as long as all the u_i's are positive.

Statement of the Conjecture

The conjecture of Cohen-Martinet [14, Hypothesis 6.6] says the following.

Conjecture 2.1.3 (Cohen and Martinet [14])**.** *Let S be a finite set of prime numbers such that the primes in S are relatively prime to $|\Gamma|$, and $\underline{u} \in \mathbb{Q}^{m-1}$, and $X = X((1-e_1)\mathbb{Q}[\Gamma], \underline{u}, (1-e_1)\mathbb{Z}_S[\Gamma])$ the random module defined above. Then, for every "reasonable" non-negative function f defined on the set of isomorphism classes of finite $(1-e_1)\mathbb{Z}_S[\Gamma]$-modules, we have*

$$\lim_{x\to\infty} \frac{\sum_{|\operatorname{Disc} K|\leq x} f((1-e_1)\operatorname{Cl}_K^S)}{\sum_{|\operatorname{Disc} K|\leq x} 1} = \mathbb{E}(f(X)),$$

where the sum is over all Γ-extensions K/K_0 and the rank of K/K_0 is $\underline{u}$ (and no conjecture is made if the sums are empty).

The cases when $K_0 = \mathbb{Q}$ and either Γ is abelian and K is totally real, or $|\Gamma| = 2$, are the earlier conjecture of Cohen-Lenstra [12, Fundamental Assumptions 8.1].

Remark. In [14], a quantity $M_{\underline{u}}^S(f)$ appears in place of $\mathbb{E}(f(X))$. The identity $M_{\underline{u}}^S(f) = \mathbb{E}\big(f(X)\big)$ is proved in Proposition 2.4.5. Also the S-part of the relative class group $\operatorname{Cl}_{K/K_0}^S$ appears in place of $(1-e_1)\operatorname{Cl}_K^S$. In Lemma 2.5.10, we show that these are actually the same. Note that $e_1 \operatorname{Cl}_K^S = \operatorname{Cl}_{K_0}^S$. Therefore we only consider the $(1-e_1)$-part as a random object.

Cohen and Martinet actually make further conjectures for some primes dividing $|\Gamma|$ and for infinite S. We will give the conjecture for $p \mid |\Gamma|$ in Conjecture 2.5.2.

Remark. In Conjecture 2.1.3, we give the conjecture made by Cohen and Martinet, with the addition of the hypotheses that $p \nmid |\Gamma|$ and S is finite, except that we have replaced some mathematical expressions in the original conjecture with equivalent mathematical expressions. In particular, we have replaced them with equivalent expressions that we think shed more light on the nature of the conjecture. However, there are several problems with the content of the conjecture that we briefly mention here, and are mostly orthogonal to the work in this paper. First, given the example of [3, Theorem 1.1] of Bartel and Lenstra, it is probably best to keep the conjecture to finite sets S. Second, the ordering of the fields needs to be changed in the conjecture, given the example of [3, Theorem 1.2] of Bartel and Lenstra, who suggest ordering fields by the radical of their discriminant based on work on the second author [64] that shows this ordering has nice statistical properties for abelian Galois groups. Third, Malle's work [39, 40] suggests that we should also require that S does not contain any primes dividing the order of the roots of unity of K_0. The function field results in [38] suggest that these are all the corrections that need to be made. Finally, we need to find an appropriate meaning of "reasonable" for the conjecture (which is never specified by Cohen and Martinet). See [7, Section 5.6] and [3, Section 7] for some possible notions of "reasonable."

Even though the conjectures of Cohen, Lenstra, and Martinet do not include the cases of function fields, as mentioned in the introduction there has been significant recent work in proving partial results towards their function field analogs. In this analogy the $\underline{u} = 0$

distribution provides the conjectural distribution for Pic^0 of random Γ-covers of $\mathbb{P}^1_{\mathbb{F}_q}$, and when one wants to consider some points of the curve at infinity and the distribution of the class groups of the corresponding affine curves, then distributions with $\underline{u} \neq 0$ arise. See [63, Section 1] and [37, Section 3.5] for specific discussion of this aspect of the analogy.

2.2 The $|G|^{\underline{u}}$ in Cohen-Martinet

In this section, we will find a simpler expression for the $|G|^{\underline{u}}$ term that appears in the conjecture of Cohen and Martinet. We continue the notation from Section 2.1.

Theorem 2.2.1. *Let K/K_0 be a Γ-extension of number fields. For each infinite prime v of K_0, let Γ_v be a decomposition group at v. We assume that the set S only contains primes not dividing $|\Gamma|$. If H is a finite $(1-e_1)\mathbb{Z}_S[\Gamma]$-module, then*

$$|H|^{\underline{u}} = \prod_{v|\infty} |H^{\Gamma_v}|,$$

where v runs over all infinite primes of K_0.

Proof. By the definition of $|H|^{\underline{u}}$, the theorem reduces to the case of a $\mathbb{Z}_S[\Gamma]$-module H such that $H = e_i H$ for some $i > 1$. Let $e \neq e_1$ be a central irreducible idempotent of $\mathbb{Q}[\Gamma]$ associated to the $\mathbb{Q}$-irreducible character χ and rank u, and let H be a finite $e\mathbb{Z}_S[\Gamma]$-module. We first show the following identity

$$|H^{\Gamma_v}| = |H|^{\frac{\langle \chi, a_{\Gamma/\Gamma_v}\rangle}{\langle \chi, a_\Gamma\rangle}}$$

for each infinite place v of K_0, where for a subgroup $\Delta \subseteq \Gamma$ we define $a_{\Gamma/\Delta} := -1 + \mathrm{Ind}_\Delta^\Gamma 1_\Delta$ to be the augmentation character of Δ and $a_\Gamma := a_{\Gamma/1}$. By [14, Theorem 7.3], for each v, there exists some abelian group G_v such that, as abelian groups, we have

$$H = eH \cong G_v^{\langle \chi, a_\Gamma\rangle} \quad \text{and} \quad H^{\Gamma_v} = (eH)^{\Gamma_v} \cong G_v^{\langle \chi, a_{\Gamma/\Gamma_v}\rangle},$$

hence the identity.

Note that $\chi_K = -1 + \sum_{v|\infty}(a_{\Gamma/\Gamma_v} + 1)$, and that $\langle \chi, 1\rangle = 0$. We then know that

$$\prod_{v|\infty} |H^{\Gamma_v}| = \prod_{v|\infty} |H|^{\frac{\langle \chi, a_{\Gamma/\Gamma_v}\rangle}{\langle \chi, a_\Gamma\rangle}} = |H|^{\frac{\langle \chi, \chi_K\rangle}{\langle \chi, a_\Gamma\rangle}}.$$

If we denote by φ a fixed absolutely irreducible character contained in χ and let $\{\varphi_1, \ldots, \varphi_j\}$ be the set of all the distinct conjugates of φ, then

$$\chi = d \sum_{i=1}^{j} \varphi_i.$$

where d is the Schur index. So we have

$$\langle \chi, \chi_K \rangle = d \sum_{i=1}^{j} \langle \varphi_i, \chi_K \rangle = dj \langle \varphi, \chi_K \rangle.$$

On the other hand, since the character φ is absolutely irreducible,

$$\langle \chi, a_\Gamma \rangle = d \sum_{i=1}^{j} \langle \varphi_i, a_\Gamma \rangle = dj\varphi(1) = djh$$

where h is the h_i of Section 2.1, and one can check $h = \dim \varphi$. We then know that

$$\prod_{v|\infty} |H^{\Gamma_v}| = |H|^{\frac{\langle \chi, \chi_K \rangle}{\langle \chi, a_\Gamma \rangle}} = |H|^{\frac{1}{h}\langle \varphi, \chi_K \rangle} = |H|^u = |H|^{\underline{u}}$$

completing the proof. □

Remark. Actually the statement of Theorem 2.2.1 can be extended to some primes dividing $|\Gamma|$. Let e be a central idempotent in $\mathbb{Q}[\Gamma]$ such that $e_1 \cdot e = 0$ and S be a set of primes such that $e \in \mathbb{Z}_S[\Gamma]$ and $e\mathbb{Z}_S[\Gamma]$ is a maximal order in $e\mathbb{Q}[\Gamma]$ (i.e. S only contains *good primes* for e, see the definition in Section 2.5). If H is a finite $e\mathbb{Z}_S[\Gamma]$-module, then

$$|H|^{\underline{u}} = \prod_{v|\infty} |H^{\Gamma_v}|.$$

The proof is the same as above because Theorem 7.3 in [14] still holds in this case.

2.3 Probabilities inversely proportional to automorphisms

Since the Cohen-Lenstra and Cohen-Martinet conjectures are rooted in the philosophy that objects appear inversely proportional as often as their number of automorphisms, it is natural to ask why there is a term $|G|^{\underline{u}}$ in the conjectures at all. One answer is that it was necessary to match computational evidence, and other heuristic explanations are given in [12, Section 8]. In this section, we give another perspective, over the base field $\mathbb{Q}$, in which we see class groups as a part of a larger structure where $|G|^{\underline{u}}|\operatorname{Aut}(G)|$ is the number of automorphisms of the larger structure. Bartel and Lenstra [3] have given a different perspective on interpreting these probabilities, over a general number field, as inversely proportional to the automorphisms of a larger object, in their case, the Arakelov class groups. In contrast, our larger objects below are only slightly larger than the class groups, and in particular, finite.

Let Γ be a fixed finite group. We choose an embedding $\bar{\mathbb{Q}} \subset \mathbb{C}$ so that $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ has a canonical decomposition group $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ at ∞. We fix a map $s : \operatorname{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma$, let $K \subset \bar{\mathbb{Q}}$

be a Galois extension of $\mathbb{Q}$ with an isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \simeq \Gamma$, and let the decomposition group at ∞ given by s (under the isomorphism).

Let K' be the maximal unramified abelian extension of K in $\bar{\mathbb{Q}}$ of order prime to $|\Gamma|$. The structure we consider is the finite group $G := \mathrm{Gal}(K'/\mathbb{Q})$ with given maps

$$c : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to G \qquad \text{and} \qquad \pi : G \to \mathrm{Gal}(K/\mathbb{Q}) = \Gamma,$$

where π is a surjection with abelian kernel. Of course, $\ker(\pi) = \mathrm{Cl}_K^S$ (where S is the set of primes not dividing $|\Gamma|$) is naturally a Γ-module, but the data (G, c, π) is a little more. In fact, it is a *class triple* as defined below.

Definition 2.3.1. For a given map $s : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma$, we call (G, c, π) a *class triple* (for s) if G is a finite group satisfying the following conditions:

i) $\pi : G \to \Gamma$ is a surjective homomorphism such that $\ker \pi$ is an abelian group whose order is coprime to $|\Gamma|$;

ii) $c : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to G$ is a homomorphism such that $\pi \circ c = s$;

iii) $\ker \pi^\Gamma = 1$ (where Γ acts by conjugation by preimages in G);

iv) $\mathrm{im}\, c \cap \ker \pi = 1$.

Then for two class triples (G_1, c_1, π_1) and (G_2, c_2, π_2), a morphism τ is a group homomorphism $G_1 \to G_2$ such that $\pi_1 = \pi_2 \circ \tau$ and that $\tau \circ c_1 = c_2$.

Theorem 2.3.2. *For a given map $s : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma$ and a class triple (G, c, π), we have*

$$|\mathrm{Aut}(G, c, \pi)| = |\ker \pi^{\mathrm{im}(s)}||\mathrm{Aut}_\Gamma(\ker \pi)|.$$

Further, given a finite Γ-module H of order relatively prime to $|\Gamma|$ with $H^\Gamma = 1$, there is a unique isomorphism class of class triples for s with $\ker \pi$ isomorphic to H as a Γ-module.

Proof. Let A be the group of automorphisms of (G, c, π), and since each such automorphism preserves $\ker \pi$ (set-wise) and respects π, we have a homomorphism

$$A \to \mathrm{Aut}_\Gamma(\ker \pi).$$

By the Schur-Zassenhaus theorem, we can write $G = \ker \pi \rtimes \Gamma$ (non-canonically), and so in this notation an element $\tau \in A$ is determined by where it sends $\ker \pi$ and Γ. Further, since $\pi = \pi \circ \tau$, it follows that τ sends Γ to another splitting of $G \to \Gamma$. By Schur-Zassenhaus all the splittings of $G \to \Gamma$ are conjugate by elements of $\ker \pi$.

This gives a map from $\ker \pi$ to the set of splittings of $G \to \Gamma$. We claim this gives $|\ker \pi|$ distinct splittings. In $\ker \pi \rtimes \Gamma$, we have

$$(n, 1)(1, \gamma)(n, 1)^{-1} = (n(n^{-1})^{\gamma^{-1}}, \gamma).$$

Suppose that $(n_1, 1)$ and $(n_2, 1)$ give the same splitting for some $n_1, n_2 \in \ker \pi$. Then for all $\gamma \in \Gamma$ we have

$$n_1(n_1^{-1})^{\gamma^{-1}} = n_2(n_2^{-1})^{\gamma^{-1}},$$

i.e., $n_2^{-1}n_1 = (n_2^{-1}n_1)^{\gamma^{-1}}$. By the definition of class triple, this implies $n_1 = n_2$. Thus we have $|\ker \pi|$ splittings.

Any element $\mathrm{Aut}_\Gamma(\ker \pi)$ and any splitting $\Gamma \to H$ combine to give an automorphism of (G, π) by the definition of semi-direct product. We next determine which of these automorphisms preserves c. Let $K \subset G$ be $K := \pi^{-1}(\mathrm{im}\, \pi \circ c)$. So we have

$$1 \to \ker \pi \to K \to \mathrm{im}\, \pi \circ c \to 1.$$

Since $\mathrm{im}\, c \cap \ker \pi = 1$, one splitting of the above is $\mathrm{im}\, \pi \circ c \to \mathrm{im}\, c$. Another splitting is $\mathrm{im}\, \pi \circ c \to 1 \times \mathrm{im}\, \pi \circ c \subset \ker \pi \rtimes \Gamma$ according to our chosen splitting above. By Schur-Zassenhaus, these two splittings are conjugate by an element $(n, 1)$ for some $n \in \ker \pi$.

So let $I = \mathrm{im}\, \pi \circ c$. Then the elements of $\mathrm{im}\, c$ are $(n, 1)(1, \gamma)(n^{-1}, 1) = (n(n^{-1})^{\gamma^{-1}}, \gamma)$ for $\gamma \in I$. These elements are fixed by the element of $\mathrm{Aut}(G, \pi)$ that comes from $\psi \in \mathrm{Aut}_\Gamma(\ker \pi)$ and conjugation of Γ by $(m, 1)$ if and only if for all $\gamma \in I$,

$$(m, 1)(\psi(n(n^{-1})^{\gamma^{-1}}), \gamma)(m^{-1}, 1) = (n(n^{-1})^{\gamma^{-1}}, \gamma)$$

i.e.

$$n^{-1}m\psi(n) = (n^{-1}m\psi(n))^{\gamma^{-1}}$$

i.e. $n^{-1}m\psi(n)$ is fixed by I, i.e $m \in n^{-1}(\ker \pi)^I\psi(n)$. Thus we conclude that exactly $|\mathrm{Aut}_\Gamma(\ker \pi)||(\ker \pi)^I|$ elements of $\mathrm{Aut}(H, \pi)$ preserve c. This gives the first statement of the theorem.

For the second statement of the theorem, by Schur-Zassenhaus, any class triple giving H has $G \simeq H \rtimes \Gamma$. Choosing c to be s composed with the trivial splitting $\Gamma \to H \rtimes \Gamma$ gives at least one class triple giving H. As we saw above, any other choice of c differs by conjugation by an element of H, i.e. differs by an automorphism of $H \rtimes \Gamma$ fixing the map to Γ. □

Corollary 2.3.3. *Let $K \subset \bar{\mathbb{Q}}$ be a Galois extension of $\mathbb{Q}$ with Galois group Γ and decomposition group Γ_∞ at ∞ and map $s : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma_\infty \subset \Gamma$. Let $G := \mathrm{Gal}(K'/\mathbb{Q})$ with given maps*

$$c : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to G \qquad \text{and} \qquad \pi : G \to \mathrm{Gal}(K/\mathbb{Q}) = \Gamma,$$

Let S be the set of primes not dividing $|\Gamma|$. Then

$$|\mathrm{Aut}(G, c, \pi)| = |(\mathrm{Cl}_K^S)^{\Gamma_\infty}||\mathrm{Aut}_\Gamma(\mathrm{Cl}_K^S)|.$$

So, combining with Theorem 2.2.1, we see that the probabilities in the Cohen-Lenstra and Cohen-Martinet conjectures are inversely proportional to the number of automorphisms of the class triples associated to the fields (which are determined up to isomorphism by their class groups and decomposition groups but have a different number of automorphisms from their class groups).

2.4 Moments of the Cohen-Lenstra-Martinet Random Groups

In this section, we will find the moments of the Cohen-Lenstra-Martinet random Γ-modules, and moreover show that their distributions are determined by their moments.

Moments for Galois Extensions

We keep the notation from Section 2.1. However, in this section, we will take the set S of prime to be not necessarily finite. We will also define a slightly more general notion of random modules.

Definition 2.4.1. (Random $\mathfrak{O}$-modules) Let A be any finite dimensional semisimple $\mathbb{Q}$-algebra with m simple factors. Let S be a set of prime numbers, $\mathfrak{O}$ be a $\mathbb{Z}_S$-maximal order of A, and $\underline{u} \in \mathbb{Q}^m$ be a fixed m-tuple. If either S contains finitely many primes or $u_i > 0$ for all $i = 1, \ldots, m$, then we define $X = X(A, \underline{u}, \mathfrak{O})$ to be a random finite $\mathfrak{O}$-module such that for all finite $\mathfrak{O}$-module G_1 and G_2, we have

$$\frac{\mathbb{P}(X \cong G_1)}{\mathbb{P}(X \cong G_2)} = \frac{|G_2|^{\underline{u}}|\operatorname{Aut}_{\mathfrak{O}}(G_2)|}{|G_1|^{\underline{u}}|\operatorname{Aut}_{\mathfrak{O}}(G_1)|}.$$

When S does not contain any primes dividing $|\Gamma|$, then $\mathbb{Z}_S[\Gamma]$ is a maximal order in $\mathbb{Q}[\Gamma]$ (and so $(1-e_1)\mathbb{Z}_S[\Gamma]$ is a maximal order in $(1-e_1)\mathbb{Q}[\Gamma]$), and our previous definition of X is a special case of the above. As in Remark 2.1, X is well-defined.

Now given H a finite $\mathfrak{O}$-module, consider the function $|\operatorname{Sur}_{\mathfrak{O}}(G, H)|$ counting the number of surjective $\mathfrak{O}$-morphisms from G to H. Then we have the following formula to compute the moments of X.

Theorem 2.4.2. *Given a finite $\mathfrak{O}$-module H, we have*

$$\mathbb{E}\left(|\operatorname{Sur}_{\mathfrak{O}}(X, H)|\right) = \frac{1}{|H|^{\underline{u}}}.$$

Proof. In this proof a summation over $G/\sim$ always means the sum is over all isomorphism classes of finite $\mathfrak{O}$-modules, with G a representative from each class. For finite $\mathfrak{O}$-modules G, H, we have

$$|\operatorname{Sur}_{\mathfrak{O}}(G, H)| = \#\{G' \subset G | \, G/G' \cong H\} \cdot |\operatorname{Aut}_{\mathfrak{O}}(H)|.$$

where $G' \subset G$ denotes G' a sub-$\mathfrak{O}$-module of G. For G_1 and G_2 finite $\mathfrak{O}$-modules, [14, Proposition 3.3] gives

$$\sum_{G/\sim} |\operatorname{Aut}_{\mathfrak{O}}(G)|^{-1} \#\{H \subseteq G : H \cong G_1 \text{ and } G/H \cong G_2\} = |\operatorname{Aut}_{\mathfrak{O}}(G_1)|^{-1} |\operatorname{Aut}_{\mathfrak{O}}(G_2)|^{-1}.$$

Let

$$Z(\underline{u}) = \sum_{G/\sim} \frac{1}{|G|^{\underline{u}} |\mathrm{Aut}_{\mathfrak{O}}(G)|}. \tag{2.4.1}$$

Then we deduce that

$$\begin{aligned}
\mathbb{E}\big(|\mathrm{Sur}_{\mathfrak{O}}(X,H)|\big) &= \sum_{G/\sim} \mathbb{P}(X \cong G) |\mathrm{Sur}_{\mathfrak{O}}(G,H)| \\
&= \sum_{G/\sim} \frac{1}{|G|^{\underline{u}} |\mathrm{Aut}_{\mathfrak{O}}(G)| Z(\underline{u})} |\mathrm{Aut}_{\mathfrak{O}}(H)| \sum_{G_1/\sim} \#\{G' \subseteq G \,|\, G' \cong G_1,\, G/G' \cong H\} \\
&= \frac{|\mathrm{Aut}_{\mathfrak{O}}(H)|}{Z(\underline{u})} \sum_{G_1/\sim} \frac{1}{|G_1|^{\underline{u}} |H|^{\underline{u}}} \sum_{G/\sim} \frac{1}{|\mathrm{Aut}_{\mathfrak{O}}(G)|} \#\{G' \subseteq G \,|\, G' \cong G_1,\, G/G' \cong H\} \\
&= |\mathrm{Aut}_{\mathfrak{O}}(H)| \sum_{G_1/\sim} \frac{1}{|\mathrm{Aut}_{\mathfrak{O}}(G_1)| \cdot |G_1|^{\underline{u}} Z(\underline{u})} \frac{1}{|\mathrm{Aut}_{\mathfrak{O}}(H)| \cdot |H|^{\underline{u}}} \\
&= \frac{1}{|H|^{\underline{u}}} \sum_{G_1/\sim} \mathbb{P}(X \cong G_1) = \frac{1}{|H|^{\underline{u}}}.
\end{aligned}$$

□

When applying the results to class groups, it is always the case that we only consider the e-component of $\mathbb{Q}[\Gamma]$ where e is some central idempotent. Suppose that e is some central idempotent in $A = \mathbb{Q}[\Gamma]$, then $eA \subseteq \mathbb{Q}[\Gamma]$ is also a semisimple $\mathbb{Q}$-algebra and $e\mathfrak{O}$ is a maximal order in eA. We could build a random module directly from $e\mathfrak{O}$, or we could multiply our original random module by e. The following shows these two constructions are the same.

Lemma 2.4.3. *Let $e = e_2 + \cdots + e_k$ be some central idempotent of A, and let $X_1 = X(A, \underline{u} = (u_1, \ldots, u_m), \mathfrak{O})$ and $X_2 = X(eA, \underline{v} = (v_2, \ldots, v_k), e\mathfrak{O})$ be the random modules defined in Section 1.2 such that $u_i = v_i$ for all $i = 2, \ldots, k$. Then eX_1 and X_2 have the same probability distribution, i.e., for all finite $e\mathfrak{O}$-modules G, we have*

$$\mathbb{P}(eX_1 \cong G) = \mathbb{P}(X_2 \cong G).$$

Proof. Let $\mathcal{S}$ be the set of isomorphism classes of finite $(1-e)\mathfrak{O}$-modules. For all finite $e\mathfrak{O}$-modules G_1, G_2, we have

$$\frac{\mathbb{P}(eX_1 \cong G_1)}{\mathbb{P}(eX_1 \cong G_2)} = \frac{\sum_{H \in \mathcal{S}} \mathbb{P}(X_1 \cong G_1 \oplus H)}{\sum_{H \in \mathcal{S}} \mathbb{P}(X_1 \cong G_2 \oplus H)}$$

Since all the terms defining the probabilities factor over G_i and H, we conclude the lemma. □

Therefore Theorem 2.4.2 can be applied to eX directly.

Corollary 2.4.4. *Let $e \in \mathfrak{O}$ be any central idempotent. Given a finite $\mathfrak{O}$-module H, we have*

$$\mathbb{E}\left(|\operatorname{Sur}_{\mathfrak{O}}(eX, H)|\right) = \begin{cases} \dfrac{1}{|H|^{\underline{u}}} & \text{if } eH = H, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $eH \neq H$, then there is no surjective homomorphism from any $e\mathfrak{O}$-module to H. If $eH = H$, then $\mathfrak{O}$-morphisms from eG to H are the same as $e\mathfrak{O}$-module homomorphisms from eG to H. So the corollary follows from Lemma 2.4.3 and Theorem 2.4.2. □

Now we will show that the expected values of functions of X agree with the averages that appear in the conjectures of [14].

Remark. The original definition of $M_{\underline{u}}^S(f)$, the average appearing the the conjectures in [14], is given by their Definition 5.1 and Conjecture 6.6. However, note that in the original paper, the definition of $M_{\underline{u}}^S(f)$ must be corrected to involve e, e.g. $M_{\underline{u}}^S(f)$ should be defined with the implicit algebra $e\mathbb{Q}[\Gamma]$ instead of $\mathbb{Q}[\Gamma]$.

Proposition 2.4.5. *Let $|S| < \infty$, and let f be a non-negative function defined on the isomorphism classes of finite $\mathfrak{O}$-modules. For $X = X(A, \underline{u}, \mathfrak{O})$, we have*

$$\mathbb{E}\big(f(X)\big) = \lim_{\underline{x} \to \underline{\infty}} \frac{\sum_{|G| \leq \underline{x}} |G|^{-\underline{u}} \sum_{\varphi \in \operatorname{Hom}(P,G)} |\operatorname{Aut}_{\mathfrak{O}}(G)|^{-1} f(G/\operatorname{Im}\varphi)}{\sum_{|G| \leq \underline{x}} |G|^{-\underline{u}} \sum_{\varphi \in \operatorname{Hom}(P,G)} |\operatorname{Aut}_{\mathfrak{O}}(G)|^{-1}}$$

where the sum is over finite $\mathfrak{O}$-modules G and P is a projective $\mathfrak{O}$-module of rank $\underline{u}$ (as defined in [14, Definition 3.1]). Here $\underline{x} \in \mathbb{Z}^m$, and $|G| \leq \underline{x}$ means that for every i, we have $|e_i G| \leq x_i$, and the limit means all $x_i \to \infty$.

Proof. In this proof a summation over $G/\sim$ always means the sum is over all isomorphism classes of finite $\mathfrak{O}$-modules, with G a representative from each class. By [14, Theorem 4.6 (ii)] with $\psi(G) = |\operatorname{Aut}_{\mathfrak{O}}(G)|^{-1}$ and $\underline{s} = \underline{u}$, if $g_{G_1}(G) = \#\{\varphi \in \operatorname{Hom}_{\mathfrak{O}}(P, G) : G/\operatorname{im}\varphi \cong G_1\}$ and P is projective of rank $\underline{u}$, then

$$\sum_{G/\sim} \frac{g_{G_1}(G)}{|\operatorname{Aut}_{\mathfrak{O}}(G)||G|^{\underline{u}}} = \frac{Z(\underline{0})}{|\operatorname{Aut}_{\mathfrak{O}}(G_1)||G_1|^{\underline{u}} Z(\underline{u})},$$

where Z is defined in (2.4.1) (and see Remark 2.1 for the convergence). Then we have

$$\begin{aligned} &\sum_{G/\sim} |G|^{-\underline{u}} \sum_{\varphi \in \operatorname{Hom}_{\mathfrak{O}}(P,G)} |\operatorname{Aut}_{\mathfrak{O}}(G)|^{-1} f(G/\operatorname{im}\varphi) \\ &= \sum_{G_1/\sim} f(G_1) \sum_{G/\sim} \frac{g_{G_1}(G)}{|\operatorname{Aut}_{\mathfrak{O}}(G)||G|^{\underline{u}}} \\ &= \sum_{G_1/\sim} f(G_1) \frac{Z(\underline{0})}{|\operatorname{Aut}_{\mathfrak{O}}(G_1)||G_1|^{\underline{u}} Z(\underline{u})} = Z(\underline{0}) \mathbb{E}\big(f(X)\big) \end{aligned}$$

We can also apply this to the constant function $f(G) = 1$, and deduce the proposition. □

Moments Determine the Distribution

So the random $\mathfrak{O}$-module X has H-moment $|H|^{-u}$ for every finite $\mathfrak{O}$-module H. Now we ask: given a random finite $\mathfrak{O}$-module Y with H-moment $|H|^{-u}$ for all H, does Y have the same probability distribution as X? In this section, we will see the answer is yes.

Recall the notations from Section 2.1: $A = \prod_{i=1}^{m} A_i$ and K_i is the center of A_i. Now for each pair $(i, \mathfrak{p})$ where $i = 1, \ldots, m$ and $\mathfrak{p}$ is a prime of K_i, we can consider the completion $A_{i,\mathfrak{p}} \cong M_{l_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}})$ of A_i at $\mathfrak{p}$ (where $D_{i,\mathfrak{p}}$ is the completion of D_i at $\mathfrak{p}$ and $l_{i,\mathfrak{p}}$ is some positive integer). Note that in this notation that the choices of $\mathfrak{p}$ depend on i. If $\mathfrak{O}$ is a maximal $\mathbb{Z}_S$-order in A, then $e_i\mathfrak{O}$ also admits a completion $\mathfrak{O}_{i,\mathfrak{p}} = e_i\mathfrak{O} \otimes_{\mathbb{Z}_{K_i}} \mathbb{Z}_{K_{i,\mathfrak{p}}}$ (where $\mathbb{Z}_{K_i}$ is the ring of integers of K_i and $\mathbb{Z}_{K_{i,\mathfrak{p}}}$ is the valuation ring of $K_{i,\mathfrak{p}}$). In particular, $\mathfrak{O}_{i,\mathfrak{p}}$ is a maximal order in $A_{i,\mathfrak{p}}$. Then in this case (unlike in the global case), there always exists an isomorphism

$$\mathfrak{O}_{i,\mathfrak{p}} \cong M_{l_{i,\mathfrak{p}}}(\mathcal{o}_{i,\mathfrak{p}}),$$

where $\mathcal{o}_{i,\mathfrak{p}}$ is *the* maximal order in $D_{i,\mathfrak{p}}$, which is given by a valuation.

If G is a finite $\mathfrak{O}$-module, and $(i, \mathfrak{p})$ some prime ideal of $\mathfrak{O}$ (i.e. $\mathfrak{p}$ is a prime ideal of K_i), then let $G_{\mathfrak{p}}$ denote the part of G annihilated by a power of $\mathfrak{p}$ and we know that $G_{\mathfrak{p}}$ is naturally a finite $\mathfrak{O}_{i,\mathfrak{p}}$-module. For any two finite $\mathfrak{O}$-modules G_1 and G_2, we have

$$|\operatorname{Aut}_{\mathfrak{O}}(G_1)| = \prod_{(i,\mathfrak{p})} |\operatorname{Aut}_{\mathfrak{O}_{i,\mathfrak{p}}}(G_{1,\mathfrak{p}})| \quad \text{and} \quad |\operatorname{Sur}_{\mathfrak{O}}(G_1, G_2)| = \prod_{(i,\mathfrak{p})} |\operatorname{Sur}_{\mathfrak{O}_{i,\mathfrak{p}}}(G_{1,\mathfrak{p}}, G_{2,\mathfrak{p}})|.$$

Moreover, the category of $\mathfrak{O}_{i,\mathfrak{p}}$-modules is equivalent to the category of $\mathcal{o}_{i,\mathfrak{p}}$-modules, because they are both matrix algebras over $\mathcal{o}_{i,\mathfrak{p}}$. So the question of counting surjective morphisms is then reduced to the following case: let D be a division algebra over $\mathbb{Q}_p$ with the maximal $\mathbb{Z}_p$-order $\mathcal{o}$ and we consider the category of finite $\mathcal{o}$-modules. Given any (finite) partition $\lambda : \lambda_1 \geq \lambda_2 \geq \ldots$, there exists a unique (up to isomorphism) finite $\mathcal{o}$-module G such that

$$G \cong \bigoplus_i \mathcal{o}/\mathfrak{p}^{\lambda_i},$$

where $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{o}$, see, e.g. [14, Lemma 2.7]. Then we write $G = G_\lambda$ and call it the $\mathcal{o}$-module of type λ. Also let $q = |\mathcal{o}/\mathfrak{p}|$ be the cardinality of the simple $\mathcal{o}$-module.

Definition 2.4.6. Given a partition $\lambda : \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, it can be represented by a Young diagram whose number of boxes in the ith row represents the number λ_i. Then the *transpose* λ' of λ is the partition such that λ'_j equals to the number of boxes in the jth column in the diagram of λ. We have a *partial ordering* on partitions as follows, Given two partitions μ, λ, we say that $\mu \leq \lambda$ when $\mu_i \leq \lambda_i$ for each $i = 1, 2, \ldots$.

Lemma 2.4.7. *Let D be a division algebra over $\mathbb{Q}_p$ with maximal $\mathbb{Z}_p$-order $\mathcal{o}$. Given two $\mathcal{o}$-modules G_λ, G_μ of type λ and μ. Then*

$$|\operatorname{Hom}_{\mathcal{o}}(G_\lambda, G_\mu)| = q^{\sum_{i=1}^{\infty} \lambda'_i \mu'_i}.$$

Proof. By Lemma 2.7 (and more generally §2) in [CM90], we only need to check the formula for the case when G_λ, G_μ are both cyclic, which is clear, i.e.,

$$|\operatorname{Hom}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}^m, \mathcal{O}/\mathfrak{p}^n)| = q^{\min(m,n)} = q^{\lambda_1'\mu_1'}.$$

□

Lemma 2.4.8. *Let $G = G_\lambda$ be a $\mathcal{O}$-module of type λ. If $\mu \leq \lambda$, then the number of submodules of type μ, denoted by $\alpha_\lambda(\mu; q)$, satisfies*

$$\alpha_\lambda(\mu; q) \leq \prod_{j \geq 1} \frac{1}{(1-2^{-j})^{\lambda_1}} \cdot q^{\sum_{i=1}^{\lambda_1} \mu_i'\lambda_i' - (\mu_i')^2}.$$

Proof. First we claim

$$\alpha_\lambda(\mu; q) \leq \frac{|\operatorname{Hom}_{\mathcal{O}}(G_\mu, G_\lambda)|}{|\operatorname{Aut}_{\mathcal{O}}(G_\mu)|},$$

i.e., if $f : G_\mu \to G_\lambda$ happens to be an injective map, then $f \circ g$ where $g \in \operatorname{Aut}_{\mathcal{O}}(G_\mu)$ clearly gives us the same subgroup in G_λ. Then by Theorem 2.11 in [CM90], if $\pi_1, \ldots, \pi_t$ are the distinct (nonzero) values of $\{\mu_i\}$ with multiplicities $k_1, \ldots, k_t$, then

$$|\operatorname{Aut}_{\mathcal{O}}(G_\mu)| = q^{\sum_i (\mu_i')^2} \prod_{i=1}^{t} (k_i)_q \geq q^{\sum_i (\mu_i')^2} \prod_{i=1}^{t} (\infty)_q \geq q^{\sum (\mu_i')^2} \prod_{j=1}^{\infty} (1-q^{-j})^{\mu_1},$$

where the notion $(k)_q$ means $\prod_{i=1}^{k}(1-q^{-i})$ if $k > 0$. Since $\mu_1 \leq \lambda_1$, we have

$$\alpha_\lambda(\mu; q) \leq \frac{|\operatorname{Hom}_{\mathcal{O}}(G_\mu, G_\lambda)|}{|\operatorname{Aut}_{\mathcal{O}}(G_\mu)|} \leq \prod_{j=1}^{\infty} \frac{1}{(1-q^{-j})^{\mu_1}} q^{\sum \mu_i'\lambda_i' - (\mu_i')^2} \leq \prod_{j} \frac{1}{(1-2^{-j})^{\lambda_1}} \cdot q^{\sum \mu_i'\lambda_i' - (\mu_i')^2}.$$

□

Lemma 2.4.9. *For any given $\mathcal{O}$-module G of type λ, there exists a constant C such that*

$$\#\{H \subseteq G\} \leq C^{\lambda_1} q^{\frac{1}{4}\sum (\lambda_i')^2}.$$

Proof. To prove this lemma, we sum the result in Lemma 2.4.8 over all $\mu \leq \lambda$, and a bound for this sum is given in [42, Lemma 7.5]. □

Now using the lemmas above and results from [42], we can prove that the Cohen-Lenstra-Martinet distributions are determined by their moments, and in fact even a sequence of random variables with moments converging to moments described in Theorem 2.4.2 must converge to the Cohen-Lenstra-Martinet distribution.

Theorem 2.4.10. *Take $A, \mathfrak{O}, m$ as in Section 2.1 and let $\underline{u} \in \mathbb{Q}^m$ be an m-tuple. Assume that either that $|S| < \infty$ and $\underline{u} \geq \underline{0}$, or, that $|S| = \infty$ and $u_i > 0$ for all i. Let K_i be the center of each component A_i and R_i the integral closure of $\mathbb{Z}_S$ in K_i. Then $R := \bigoplus R_i$ is the center of $\mathfrak{O}$ and each $\mathfrak{O}_i$ is a maximal R_i-order in A_i (see [52, Theorem 10.5]).*

Let $\{X_n\}$ be a sequence of random variables taking values in finite $\mathfrak{O}$-modules. For each prime $\mathfrak{p}$ of $\mathfrak{O}$, let $n_\mathfrak{p} \geq 0$ such that $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$. Let $\mathcal{S}$ be the set of all finite $\mathfrak{O}$-modules H such that the annihilator of $H_\mathfrak{p}$ divides $\mathfrak{p}^{n_\mathfrak{p}}$. Moreover let N be the $\mathfrak{O}$-module such that $N_\mathfrak{p}$ is of type $(n_\mathfrak{p}, 0, 0, \dots)$.

Suppose that for every $G \in \mathcal{S}$, we have

$$\lim_{n\to\infty} \mathbb{E}\big(|\mathrm{Sur}_\mathfrak{O}(X_n, G)|\big) = \frac{1}{|G|^{\underline{u}}}.$$

Then for every $H \in \mathcal{S}$, the limit

$$\lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)$$

exists and for all $G \in \mathcal{S}$ we have

$$\sum_{H\in\mathcal{S}} \lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)|\mathrm{Sur}_\mathfrak{O}(H, G)| = \frac{1}{|G|^{\underline{u}}}.$$

Suppose $\{Y_n\}$ is another sequence of random variables taking values in finite $\mathfrak{O}$-modules such that for every $G \in \mathcal{S}$, we have

$$\lim_{n\to\infty} \mathbb{E}\big(|\mathrm{Sur}(Y_n, G)|\big) = \frac{1}{|G|^{\underline{u}}}.$$

Then for every $H \in A$, we have

$$\lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H) = \lim_{n\to\infty} \mathbb{P}(Y_n \otimes_R N \cong H).$$

Proof. The proof is very similar to [42, Theorem 8.3], so we only present a sketch and highlight the differences. First we suppose that the limit

$$\lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)$$

exists for all $H \in \mathcal{S}$ and we are going to show that for all $G \in \mathcal{S}$ we have

$$\sum_{H\in\mathcal{S}} \lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)|\,\mathrm{Sur}_\mathfrak{O}(H, G)| = \frac{1}{|G|^{\underline{u}}}.$$

By Lemma 2.4.7 and the same argument as in [42, Theorem 8.3], for each $G \in \mathcal{S}$, there exists $G' \in \mathcal{S}$ such that

$$\sum_{H\in\mathcal{S}} \frac{|\mathrm{Hom}_\mathfrak{O}(H, G)|}{|\mathrm{Hom}_\mathfrak{O}(H, G')|} < \infty.$$

Then the same argument as in in [42, Theorem 8.3] using the Lebesgue Dominated Convergence Theorem concludes that

$$\sum_{H\in\mathcal{S}} \lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)|\mathrm{Sur}(H,G)|$$
$$= \lim_{n\to\infty} \sum_{H\in\mathcal{S}} \mathbb{P}(X_n \otimes_R N \cong H)|\mathrm{Sur}(H,G)| = \frac{1}{|G|^{\underline{u}}}$$

i.e., if for all $H \in \mathcal{S}$ the limit $\lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)$ exists, then the moments agree with $\mathbb{E}\big(|\mathrm{Sur}(X,G)|\big)$ for all $G \in \mathcal{S}$.

Next we show that if the limits $\lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)$ and $\lim_{n\to\infty} \mathbb{P}(Y_n \otimes_R N \cong H)$ exist for all H then

$$\sum_{H\in\mathcal{S}} \lim_{n\to\infty} \mathbb{P}(Y_n \otimes_R N \cong H)|\mathrm{Sur}(H,G)| \;\; = \sum_{H\in\mathcal{S}} \lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)|\mathrm{Sur}(H,G)| = \frac{1}{|G|^{\underline{u}}}$$

implies

$$\lim_{n\to\infty} \mathbb{P}(Y_n \otimes_R N \cong H) = \lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H).$$

Note that the averages $|\operatorname{Hom}_{\mathfrak{O}}(X,H)|$ and $|\operatorname{Sur}_{\mathfrak{O}}(X,H)|$ over all H, are determined from one another by finitely many steps of addition and subtraction. We'll apply [42, Theorem 8.2] with distinct primes p_i's in the assumption replaced by not necessarily distinct real numbers q_i's. The proof of the theorem actually proves the statement in this generality.

Now let M be the set defined in [42, Theorem 8.2] where the choice of q_i comes from the following: there are only finitely many primes $\mathfrak{p}_{ij} \subseteq \mathbb{Z}_{K_i}$ such that $n_{\mathfrak{p}_{ij}} > 0$ for all $i = 1, \ldots, m$, so we can let $q_k = |\mathcal{O}_k/\mathfrak{p}'_k|$ where $\mathcal{O}_k \subseteq D_{i,\mathfrak{p}_k}$ is the maximal order in $D_{i,\mathfrak{p}_k}$ and $\mathfrak{p}'_k$ is the unique maximal ideal. We say that an $\mathfrak{O}$-module $G \in \mathcal{S}$ corresponds to $\mu \in M$ if the type of G is exactly μ' where μ' is obtained by $(\mu')_k = (\mu_k)'$. We then define

$$x_\mu = \lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong G_{\mu'})$$

for all $\mu \in M$. And similarly for y_μ. If we let C_λ denote the expected value of the number of homomorphisms into $G_{\lambda'}$, then by Lemma 2.4.9, we know that C_λ satisfies the condition in [42, Theorem 8.2]. Then [42, Theorem 8.2] tells us that x_μ and y_μ are determined by C_λ.

Finally, the same diagonal argument at the end of the proof [42, Theorem 8.3] shows that when the limit moments are $|G|^{-\underline{u}}$, the limit $\lim_{n\to\infty} \mathbb{P}(X_n \otimes_R N \cong H)$ exists for all $H \in \mathcal{S}$. □

The above theorem is the most flexible for applications, but we will state now simpler versions to emphasize the main point.

Theorem 2.4.11. *Keep the notations in Theorem 2.4.10. Assume that $|S| < \infty$. If $\{X_n\}$ is a sequence of random variables taking values in finite $\mathfrak{O}$-modules such that*

$$\lim_{n\to\infty} \mathbb{E}\big(|\operatorname{Sur}_{\mathfrak{O}}(X_n,G)|\big) = \frac{1}{|G|^{\underline{u}}}$$

for all finite $\mathfrak{O}$-module G, then

$$\lim_{n\to\infty} \mathbb{P}(X_n \cong G) = \frac{1}{|\operatorname{Aut}_{\mathfrak{O}}(G)||G|^{\underline{u}} Z(\underline{u})},$$

i.e., the limit of the random variables exists and has the same probability distribution as the random variable $X = X(A, \underline{u}, \mathfrak{O})$.

Proof. If $|S| < \infty$, we can take into account all the prime ideals of $\mathfrak{O}$ at one time. Provided that G is a finite module such that $G_{i,\mathfrak{p}}$ is of type $\lambda^{i,\mathfrak{p}}$ where $\lambda^{i,\mathfrak{p}}$ is a partition, then in Theorem 2.4.10 we take $n_{i,\mathfrak{p}} = (\lambda^{i,\mathfrak{p}})'_1 + 1$. If H is any $\mathfrak{O}$-module such that

$$H \otimes_R N \cong G,$$

then H has to be isomorphic to G, i.e., $\mathbb{P}(X_n \cong G) = \mathbb{P}(X_n \otimes N \cong G)$, and it is determined by the limit moments. □

Theorem 2.4.12. *Assume that $|S| = \infty$ and $u_i > 0$ for all $i = 1, \dots, m$, and $X = X(A, \underline{u}, \mathfrak{O})$ is the random variable we've defined. If Y is a random variable taking values in finite $\mathfrak{O}$-modules such that*

$$\mathbb{E}\big(|\operatorname{Sur}_{\mathfrak{O}}(Y, G)|\big) = \frac{1}{|G|^{\underline{u}}} = \mathbb{E}\big(|\operatorname{Sur}_{\mathfrak{O}}(X, G)|\big).$$

Then

$$\mathbb{P}(Y \cong G) = \mathbb{P}(X \cong G),$$

for all finite $\mathfrak{O}$-modules G.

Proof. We let $\mathfrak{p}_i$ be the primes of $\mathfrak{O}$. By Theorem 2.4.11, for every n we have

$$\mathbb{P}(Y_{\mathfrak{p}_i} \cong G_{\mathfrak{p}_i} | \, i = 0, 1, \dots, n) = \mathbb{P}(X_{\mathfrak{p}_i} \cong G_{\mathfrak{p}_i} | \, i = 0, 1, \dots, n).$$

Then by basic properties of measures, we have

$$\begin{aligned}
\mathbb{P}(Y \cong G) &= \mathbb{P}(Y_{\mathfrak{p}_i} \cong G_{\mathfrak{p}_i} | \, i = 0, 1, 2, \dots) \\
&= \lim_{n\to\infty} \mathbb{P}(Y_{\mathfrak{p}_i} \cong G_{\mathfrak{p}_i} | \, i = 0, 1, \dots, n) \\
&= \lim_{n\to\infty} \mathbb{P}(X_{\mathfrak{p}_i} \cong G_{\mathfrak{p}_i} | \, i = 0, 1, \dots, n) \\
&= \mathbb{P}(X_{\mathfrak{p}_i} \cong G_{\mathfrak{p}_i} | \, i = 0, 1, 2, \dots) = \mathbb{P}(X \cong G).
\end{aligned}$$

□

However the statement on limit moments determining the limit distributions does not hold if S contains infinitely many primes.

Example 2.4.13. Let S contain infinitely many prime numbers which are relatively prime to $|\Gamma|$ (so that $\mathfrak{O} = \mathbb{Z}_S[\Gamma]$) and $u_i > 0$ for all i. Let H be any finite $\mathfrak{O}$-module. Then $\mathbb{P}(X \cong H) > 0$.

For every rational prime p, there is a $\mathfrak{O}$-module G_p whose underlying abelian group is a p-group, say $(\mathbb{Z}_S/p\mathbb{Z}_S)^n \cong (\mathbb{Z}/p\mathbb{Z})^n$ which is a representation of Γ over the finite field $\mathbb{F}_p$. Let Y_p be a random $\mathfrak{O}$-module such that

$$\mathbb{P}(Y_p \cong G) = \begin{cases} \mathbb{P}(X \cong G) & \forall\, G \neq H \text{ or } H \times G_p; \\ 0 & \text{if } G = H; \\ \mathbb{P}(X \cong H) + \mathbb{P}(X \cong H \times G_p) & \text{if } G = H \times G_p. \end{cases}$$

Since $|\operatorname{Sur}_{\mathfrak{O}}(H, G)| = |\operatorname{Sur}_{\mathfrak{O}}(H \times G_p, G)|$ whenever $p > |G|$, for every $\mathfrak{O}$-module G, we have

$$\lim_{p\to\infty} \mathbb{E}(|\operatorname{Sur}_{\mathfrak{O}}(Y_p, G)|) = \mathbb{E}(|\operatorname{Sur}_{\mathfrak{O}}(X, G)|).$$

However $\lim_{p\to\infty} \mathbb{P}(Y_p \cong H) = 0$. This shows there is no analog of Theorem 2.4.11 for infinite S.

2.5 Explanation of the Cohen-Martinet Heuristics in the non-Galois case

Cohen and Martinet [14] do not specifically make a conjecture about the distribution of class groups of non-Galois fields. However, they do show that by expressing class groups of non-Galois fields in terms of Galois fields, such conjectures can be obtained as consequences of their conjectures in some cases. The goal of this section is to deduce the entire consequence of the Cohen-Martinet conjectures for class groups of non-Galois fields. Interestingly, in the non-Galois case, one can sometimes also say something about the p-Sylow subgroup of the class group for p dividing the order of the Galois group of the Galois closure. So first, we must state a more complete version of the conjecture of [14] that includes these primes.

In this section we continue the notations introduced in Section 2.1 and Section 2.1. In particular, Γ is a fixed finite group.

Definition 2.5.1. Let e be any central idempotent of $\mathbb{Q}[\Gamma]$. We say that a prime number p is *good for* e if $e \in \mathbb{Z}_{(p)}[\Gamma]$ and $e\mathbb{Z}_{(p)}[\Gamma]$ is a maximal $\mathbb{Z}_{(p)}$-order in $e\mathbb{Q}[\Gamma]$, and it is *bad for* e otherwise.

This definition is stated slightly different from the original one in [14, p. 6.1], but they are equivalent (see [52, Theorem 10.5]). A prime p such that $p \nmid |\Gamma|$ is good for any central idempotents e, including $e = 1$. For a central idempotent e in $\mathbb{Q}[\Gamma]$, and S a set of primes good for e, [14, Hypothesis 6.6] is a conjecture for the distribution of $e\operatorname{Cl}_K^S$. Proposition 2.4.5 and Lemma 2.5.10 show that this conjecture is equivalent to the following.

Conjecture 2.5.2 (Cohen and Martinet [14]). *Let e be a fixed central idempotent in $(1-e_1)\mathbb{Q}[\Gamma]$, such that $e = e_2 + \cdots + e_k$, where the e_i are irreducible central idempotents. Let S be a set of prime numbers such that if $p \in S$ then p is a good prime for e, and $\underline{u} \in \mathbb{Q}^{k-1}$. Let $X = X(e(1-e_1)\mathbb{Q}[\Gamma], \underline{u}, e\mathbb{Z}_S[\Gamma])$. Then, for every "reasonable" non-negative function f defined on the set of isomorphism classes of finite $e\mathbb{Z}_S[\Gamma]$-modules, we have:*

$$\lim_{x\to\infty} \frac{\sum_{|\operatorname{Disc} L|\leq x} f(e\operatorname{Cl}_L^S)}{\sum_{|\operatorname{Disc} L|\leq x} 1} = \mathbb{E}\big(f(X)\big)$$

where L runs through all Γ-extensions of K_0 such that $|\operatorname{Disc} L| \leq x$ and the rank of L/K_0 restricted to the coordinates $2, \ldots, k$ is $\underline{u}$.

Note that all of the caveats of Remark 2.1 still apply, including the fact that the term "reasonable" is left undefined.

For a field extension L/K of number fields with groups of fractional ideals I_L and I_K, the embedding $i : I_K \to I_L$ defined on fractional ideals induce, by passing to the classes, the homomorphism:

$$i_* : \operatorname{Cl}_K \to \operatorname{Cl}_L\,.$$

For this homomorphism, we have the following.

Theorem 2.5.3 ([14, Theorem 7.6]). *Let L/K be a Γ'-extension of number fields. The kernel (resp. the cokernel) of*

$$i_* : \operatorname{Cl}_K \to \operatorname{Cl}_L^{\Gamma'} \text{ is annihilated by } |\Gamma'| \text{ (resp. } |\Gamma'|^2\text{).}$$

The direct corollary is the following.

Corollary 2.5.4 ([14, Corollary 7.7]). *Let $K_0 \subseteq K \subseteq L$ be a tower of number fields such that L/K_0 is a Γ-extension and that K is the fixed field of the subgroup Γ' of Γ. If every prime in S is not a prime divisor of $|\Gamma'|$, the homomorphism*

$$i_* : \operatorname{Cl}_{K/K_0}^S \to \big(\operatorname{Cl}_{L/K_0}^S\big)^{\Gamma'} \quad \text{is an isomorphism.}$$

When $p \nmid |\Gamma|$, the above results mean that Conjecture 2.5.2 implies a distribution on the class group of the fields $K/\mathbb{Q}$ with Galois closure $L|\mathbb{Q}$ (ordered by the discriminant of the Galois closure).

Now consider the primes $p \mid |\Gamma|$. We'll see below (Lemma 2.5.11) that if p is a good prime for $e_{\Gamma/\Gamma'}$ which is defined below, then $p \mid |\Gamma'|$, which implies that Corollary 2.5.4 is not useful if we want to make predictions on the distribution of p-Sylow subgroups of class groups of non-Galois fields for $p \mid |\Gamma|$. However, in this section we will prove Theorem 2.5.6 that allows us to deduce consequences Conjecture 2.5.2 for p-Sylow subgroups of class groups of non-Galois fields and $p \mid |\Gamma|$.

Definition 2.5.5. Let $1_{\Gamma'}$ be the unit character of Γ', and

$$r_{\Gamma/\Gamma'} = \mathrm{Ind}_{\Gamma'}^{\Gamma} 1_{\Gamma'} \text{ and } a_{\Gamma/\Gamma'} = r_{\Gamma/\Gamma'} - 1_{\Gamma}.$$

Then define $e_{\Gamma/\Gamma'}$ to be the central idempotent associated to $a_{\Gamma/\Gamma'}$, i.e., if V is a representation of Γ over $\mathbb{Q}$ with character $a_{\Gamma/\Gamma'}$, then $e_{\Gamma/\Gamma'}$ is the minimal central idempotent of $\mathbb{Q}[\Gamma]$ that acts on V as identity.

Theorem 2.5.6. *Let $K_0 \subseteq K \subseteq L$ be a tower of number fields such that L/K_0 is Galois with Galois group Γ and that K is the fixed field of the subgroup Γ' of Γ. If every prime $p \in S$ is a good prime for $e_{\Gamma/\Gamma'}$, then*

(i) $p \nmid [K : K_0]$ for all $p \in S$, and we have the following split short exact sequence

$$1 \longrightarrow \mathrm{Cl}_{K/K_0}^S \longrightarrow \mathrm{Cl}_K^S \xrightarrow{\mathrm{Nm}} \mathrm{Cl}_{K_0}^S \longrightarrow 1,$$

hence $\mathrm{Cl}_K^S = \mathrm{Cl}_{K_0}^S \times \mathrm{Cl}_{K/K_0}^S$ where we view $\mathrm{Cl}_{K_0}^S$ as a subgroup of Cl_K^S;

(ii) the induced homomorphism $i_* : \mathrm{Cl}_{K/K_0}^S \to \mathrm{Cl}_L^S$ is injective with image $\left(e_{\Gamma/\Gamma'} \mathrm{Cl}_L^S\right)^{\Gamma'} \subseteq \mathrm{Cl}_L^S$, i.e.,

$$i_* : \mathrm{Cl}_{K/K_0}^S \xrightarrow{\sim} \left(e_{\Gamma/\Gamma'} \mathrm{Cl}_L^S\right)^{\Gamma'} \text{ is an isomorphism.}$$

Remark. Cohen and Martinet give another result [14, Theorem 7.8] that could be used to relate the class groups of non-Galois fields to Galois fields, but [14, Theorem 7.8] is incorrect as stated. Their result instead should require that Γ' has a normal complement Δ such that Γ' acts on Δ (by conjugation) with trivial stabilizers on each non-identity orbit. For example, this hypothesis and the theorem fails for the example $\Gamma = S_4$ and $\Gamma' = S_3$, which is an example that appears in [13]. However, our Theorem 2.5.6 can be applied in this case and in every case in which the Cohen-Martinet heuristics make a prediction.

Note that Theorem 7.4, applied in the case $K_0 = \mathbb{Q}$, has the following corollary.

Corollary 2.5.7. *Let $L/\mathbb{Q}$ be a Γ-field and K be the fixed field of Γ'. If p is good for $e_{\Gamma/\Gamma'}$, then the order of the capitulation kernel*

$$\ker i_* = \ker(\mathrm{Cl}_K \to \mathrm{Cl}_L)$$

is not divisible by p.

For many pairs (Γ, Γ'), there is at least one prime $p \mid |\Gamma'|$ that is good for $e_{\Gamma/\Gamma'}$, e.g. p is good for (S_{p+1}, S_p), and 2 is good for (A_5, A_4), and 5 is good for S_5 or A_5 with a certain subgroup of index 6 (a stabilizer of the action on $\mathbb{P}^1_{\mathbb{F}_5}$). For these primes, Corollary 2.5.7 appears to be a new result on the capitulation kernel.

From Theorem 2.5.6, we see that Conjecture 2.5.2 implies a conjecture on averages of functions on class groups of non-Galois fields, in which the finite abelian group H appears with weight proportional to

$$\sum_{\substack{G/\sim \\ G^{\Gamma'}\cong H}} \frac{1}{|G|^{\underline{u}}|\mathrm{Aut}_\Gamma(G)|}, \tag{2.5.1}$$

where G runs through all finite $e_{\Gamma/\Gamma'}\mathbb{Z}_S[\Gamma]$-modules, up to isomorphism, such that $G^{\Gamma'} \cong H$ as abelian groups. We'll spend the rest of this section proving Theorem 2.5.6. In the next section we will give a simple expression for (2.5.1) and an interpretation of the values appearing in (2.5.1). We start with a useful statement that we will use repeatedly.

Lemma 2.5.8. *Let e be a central idempotent in $\mathbb{Q}[\Gamma]$ such that $e \in \mathbb{Z}_S[\Gamma]$ and that $e\mathbb{Z}_S[\Gamma]$ is a maximal order in $e\mathbb{Q}[\Gamma]$. Then any $e\mathbb{Z}_S[\Gamma]$-module G is cohomologically trivial as a Γ-module, i.e., for every subgroup Λ of Γ and every integer $n \in \mathbb{Z}$, we have*

$$\hat{H}^n(\Lambda, G) = 0,$$

where $\hat{H}$ denotes Tate cohomology.

Proof. Note that via the ring homomorphism $e : \mathbb{Z}_S[\Gamma] \to e\mathbb{Z}_S[\Gamma]$ given by $x \mapsto ex$, all $e\mathbb{Z}_S[\Gamma]$-modules are also Γ-modules.

Let G be any $e\mathbb{Z}_S[\Gamma]$-module. We can find a projective $e\mathbb{Z}_S[\Gamma]$-module P with surjective homomorphism $\varphi : P \to G$. Then we have a short exact sequence of $e\mathbb{Z}_S[\Gamma]$-modules

$$0 \to L \to P \to G \to 0,$$

where L is the kernel of φ. Since maximal orders are hereditary (e.g., see [52, Theorem 21.4]) the submodule L of P is also a projective $e\mathbb{Z}_S[\Gamma]$-module. Since $e \in \mathbb{Z}_S[\Gamma]$, we know that, as Γ-modules, $e\mathbb{Z}_S[\Gamma]$ is a direct summand of $\mathbb{Z}_S[\Gamma]$. Therefore P and L, as summands of the module $(e\mathbb{Z}_S[\Gamma])^m$ for some m, are summands of the module $(\mathbb{Z}_S[\Gamma])^m$. Note that $\mathbb{Z}_S[\Gamma]$ is an induced Γ-module and hence cohomologically trivial. So P and L, as summands of some induced Γ-module, are both cohomologically trivial. Then the short exact sequence implies that G is also cohomologically trivial. □

Next, we note the following property of the central idempotent $e_{\Gamma/\Gamma'}$ and its relationship to

$$e'_1 = \frac{1}{|\Gamma'|}\sum_{\tau\in\Gamma'} \tau.$$

Lemma 2.5.9. *If V is any $\mathbb{Q}$-representation of Γ of character χ, then*

$$\dim_{\mathbb{Q}} V^{\Gamma'} = \langle 1_{\Gamma'}, \mathrm{Res}^{\Gamma}_{\Gamma'}\, \chi\rangle_{\Gamma'} = \langle r_{\Gamma/\Gamma'}, \chi\rangle_{\Gamma}.$$

In particular, if $\chi_1, \ldots, \chi_m$ are all the $\mathbb{Q}$-irreducible characters of Γ such that e_i is associated to χ_i for all $i = 1, \ldots, m$, then for all $i = 1, \ldots, m$ we have

$$e_i e'_1 \neq 0 \iff e_i = e_1 \text{ or } e_i \cdot e_{\Gamma/\Gamma'} = e_i.$$

Proof. The first identity is exactly given by Frobenius reciprocity. For the second statement, note that $e_i\mathbb{Q}[\Gamma]$ is a representation of character $n_i\chi_i$ for some $n_i \geq 1$, and that $(e_i\mathbb{Q}[\Gamma])^{\Gamma'} = e_1' e_i \mathbb{Q}[\Gamma]$. □

Remark. We let $e_1, e_2, \ldots, e_k$ be all the distinct irreducible central idempotents of $\mathbb{Q}[\Gamma]$ such that $e \cdot e_1' \neq 0$. By the above lemma,

$$e_{\Gamma/\Gamma'} = e_2 + \cdots + e_k,$$

which could be taken as an alternative definition for $e_{\Gamma/\Gamma'}$.

Lemma 2.5.10. *Let L/K_0 be a Γ-extension of number fields. If e is a central idempotent of $\mathbb{Q}[\Gamma]$ such that $e_1 \cdot e = 0$ and p is a prime number that is good for e, then*

$$e \operatorname{Cl}_L[p^\infty] = e \operatorname{Cl}_{L/K_0}[p^\infty].$$

Remark. This lemma shows that taking the relative class group has no effect if one only cares about good primes for some central idempotent $e \in \mathbb{Q}[\Gamma]$. Therefore in the statement of the Cohen-Lenstra-Martinet Conjectures (see Conjecture 2.1.3 and 2.5.2) we do not need to use the concept of relative class group.

Proof. First of all let's introduce some notations. For a number field k, let I_k be the group of fractional ideals and P_k the group of principal ideals. Then for any prime p, let $I_{k,p} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} I_k$ and $P_{k,p} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} P_k$. Note that we have a short exact sequence

$$1 \to P_{k,p} \to I_{k,p} \to \operatorname{Cl}_k[p^\infty] \to 1.$$

Since $e \in \mathbb{Z}_{(p)}[\Gamma]$, the notion $e \operatorname{Cl}_L[p^\infty]$ and $e \operatorname{Cl}_{L/K_0}[p^\infty]$ are well-defined. It is clear that $e \operatorname{Cl}_{L/K_0}[p^\infty] \subseteq e \operatorname{Cl}_L[p^\infty]$. Our goal is to show that $\operatorname{Nm}_{L/K_0}(I)$ is indeed a principal ideal of K_0 for all ideals $I \in I_L$ such that the ideal class $[I]$ is contained in $e \operatorname{Cl}_L[p^\infty]$.

For any $x \in \operatorname{Cl}_L[p^\infty]$, we have

$$\operatorname{Nm}_{L/K_0}(ex) = \sum_{\gamma \in \Gamma} \gamma e x = \big(|\Gamma| e_1\big) e \cdot x = 0 \cdot x = 0.$$

Therefore $\operatorname{Nm}_{L/K_0} : e \operatorname{Cl}_L[p^\infty] \to e \operatorname{Cl}_L[p^\infty]$ is actually the zero map. Claim: $(eP_{L,p})^\Gamma = P_{K_0,p} \cap eP_{L,p}$. We first prove the claim. Recall that if $e\mathbb{Z}_{(p)}[\Gamma]$ is a maximal order then any $e\mathbb{Z}_{(p)}[\Gamma]$-module is cohomologically trivial by Lemma 2.5.8. In particular

$$1 = \widehat{H}^0(\Gamma, eP_{L,p}) = (eP_{L,p})^\Gamma / \operatorname{Nm}_{L/K} eP_{L,p}$$

This shows that if a "principal ideal" $I \in eP_{L,p}$ is fixed by Γ, then it is represented by a "principal ideal" of K_0, hence the claim.

By cohomological triviality again, we know that $e \operatorname{Cl}_L[p^\infty], eI_{L,p}, eP_{L,p}$ are all cohomologically trivial, so

$$(e \operatorname{Cl}_L[p^\infty])^\Gamma = (eI_{L,p})^\Gamma / (eP_{L,p})^\Gamma = (eI_{L,p})^\Gamma / (P_{K,p} \cap eI_{L,p}).$$

This implies that for any $ex \in (e\,\mathrm{Cl}_L[p^\infty])^\Gamma$, we have $ex = 1$ if and only if it is represented by a "principal ideal" of K (an element in $P_{K,p}$), hence $e\,\mathrm{Cl}_L[p^\infty]$ is indeed generated by ideals whose norm in Cl_{K_0} is 0, i.e., $e\,\mathrm{Cl}_L[p^\infty] = e\,\mathrm{Cl}_{L/K_0}[p^\infty]$. □

We need one more lemma for the proof of the theorem.

Lemma 2.5.11. *If p is a prime such that $e_{\Gamma/\Gamma'} \in \mathbb{Z}_{(p)}[\Gamma]$, then p does not divide $|\Gamma/\Gamma'|$. In particular, if $p \mid |\Gamma/\Gamma'|$, then p is bad.*

Proof. Let

$$P := \mathbb{Z}_{(p)}[\Gamma]e_1' = \{xe_1' \mid x \in \mathbb{Z}_{(p)}[\Gamma]\}$$

be a left $\mathbb{Z}_{(p)}[\Gamma]$-module. We know that $e_{\Gamma/\Gamma'}e_1'$ is contained in P, because $e_{\Gamma/\Gamma'}$ is already contained in $\mathbb{Z}_{(p)}[\Gamma]$. This implies that $e_1 = e_1 \cdot e_1'$ is also contained in P, for the idempotent e_1' is contained in P and could be written as

$$e_1' = 1 \cdot e_1' = (e_1 + \cdots + e_m) \cdot e_1' = e_1 + e_2e_1' + \cdots + e_ke_1' = e_1 + e_{\Gamma/\Gamma'}e_1'.$$

Let $\{\sigma_1, \ldots, \sigma_q\}$ be a fixed set of representatives of left cosets Γ/Γ'. Then every element $x \in P$ can be written uniquely as

$$x = \sum_{i=1}^{q} a_i\sigma_i e_1',$$

where $a_i \in \mathbb{Z}_{(p)}$. If in addition, x is fixed by Γ, then all the a_i must be the same, which implies that if we let

$$x_0 := \sum_{i=1}^{s} 1 \cdot \sigma_i e_1' = |\Gamma/\Gamma'| \cdot e_1,$$

then $P^\Gamma = \mathbb{Z}_{(p)}x_0$. Since $e_1 \in P^\Gamma$, we know that there exists some $a \in \mathbb{Z}_{(p)}$ such that $ax_0 = e_1$, i.e.,

$$a \cdot |\Gamma/\Gamma'| = 1.$$

So $|\Gamma/\Gamma'|$ is a unit in $\mathbb{Z}_{(p)}$, i.e., p does not divide $|\Gamma/\Gamma'|$. □

Finally let's prove Theorem 2.5.6.

Proof of Theorem 2.5.6. It is clear that we can reduce to the case where the set S is the singleton $\{p\}$ with p a good prime for $e_{\Gamma/\Gamma'}$.

For (i), by Lemma 2.5.11, we know that $p \nmid |\Gamma/\Gamma'| = [K : K_0]$. Then let's view $\mathrm{Cl}_{K_0}[p^\infty]$ as a subgroup of $\mathrm{Cl}_K[p^\infty]$ via the induced map $i_* : \mathrm{Cl}_{K_0} \to \mathrm{Cl}_K$. We have the following short exact sequence

$$1 \to \mathrm{Cl}_{K/K_0}[p^\infty] \to \mathrm{Cl}_K[p^\infty] \xrightarrow{n_*} \mathrm{Cl}_{K_0}[p^\infty] \to 1$$

where n_* is induced by the norm map Nm_{K/K_0}, because $n_*(\mathrm{Cl}_{K_0}[p^\infty]) = [K : K_0] \cdot \mathrm{Cl}_{K_0}[p^\infty] = \mathrm{Cl}_{K_0}[p^\infty]$. Then by $i_* \circ n_* = [K : K_0]$, we see that $\dfrac{1}{[K : K_0]}i_*$ is well-defined for $\mathrm{Cl}_{K_0}^S$ and splits n_*. This shows (i).

Then let's prove (ii). For a number field k, let I_k denote the group of fractional ideals, and P_k the group of principal ideals. Then for k, we have the short exact sequence

$$1 \to P_k \to I_k \to \mathrm{Cl}_k \to 1,$$

Tensoring with $\mathbb{Z}_{(p)}$ gives us a short exact sequence

$$1 \to \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} P_k \to \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} I_k \to \mathrm{Cl}_k[p^\infty] \to 1.$$

Let $P_{k,p} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} P_k$ and $I_{k,p} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} I_k$. And for an element $x_k \in I_{k,p}$, we let $[x_k]$ denote its image in the class group.

Recall the set-up in the statement: Let $K_0 \subseteq K \subseteq L$ be a tower of extensions such that $\mathrm{Gal}(L/K_0) = \Gamma$ and that $\mathrm{Gal}(L/K) = \Gamma' \subseteq \Gamma$.

Claim 1: By viewing $I_{K,p}$ as a subgroup of $I_{L,p}$ via the embedding $i : I_K \to I_L$, we have an exact sequence

$$I_{K,p} \cap I_{L,p}^{\Gamma} \to \mathrm{Cl}_K[p^\infty] \to \mathrm{Cl}_{K/K_0}[p^\infty] \to 1, \tag{2.5.2}$$

where the map $\mathrm{Cl}_K[p^\infty] \to \mathrm{Cl}_{K/K_0}[p^\infty] = \mathrm{Cl}_K[p^\infty]/\mathrm{Cl}_{K_0}[^\infty]$ is the quotient map given by (i). Let's prove the claim. First of all $I_{K_0,p} \subseteq I_{L,p}^{\Gamma}$, therefore the image of $I_{K,p} \cap I_{L,p}^{\Gamma}$ in $\mathrm{Cl}_K[p^\infty]$ must contain $\mathrm{Cl}_{K_0}[p^\infty]$. If $x \in I_{K,p} \cap I_{L,p}^{\Gamma}$ gives an ideal class $[x]$, then by (i), we can write $[x] = [y] \cdot [z]$ with $[y] \in \mathrm{Cl}_{K_0}[p^\infty]$ and $[z] \in \mathrm{Cl}_{K/K_0}[p^\infty]$. The computation

$$[x]^{[K:K_0]} = \mathrm{Nm}_{K/K_0}[x] = \mathrm{Nm}_{K/K_0}[y] \cdot \mathrm{Nm}_{K/K_0}[z] = [y]^{[K:K_0]}$$

shows that $[z] = 1$ and $[x] \in \mathrm{Cl}_{K_0}[p^\infty]$. Therefore the image of $I_{K,p} \cap I_{L,p}^{\Gamma}$ is exactly $\mathrm{Cl}_{K_0}[p^\infty]$, the kernel of $\mathrm{Cl}_K[p^\infty] \to \mathrm{Cl}_{K/K_0}[p^\infty]$.

Claim 2: We have a short exact sequence

$$1 \to P_{K,p} \cap e_{\Gamma/\Gamma'} P_{L,p} \to I_{K,p} \cap e_{\Gamma/\Gamma'} I_{L,p} \to \mathrm{Cl}_{K/K_0}[p^\infty] \to 1. \tag{2.5.3}$$

We prove this claim now. First of all, the ideal classes given by $I_{K,p} \cap e_{\Gamma/\Gamma'} I_{L,p}$ are contained in the relative class group $\mathrm{Cl}_{K/K_0}[p^\infty]$, because

$$\mathrm{Nm}_{K/K_0}[y] = \mathrm{Nm}_{K/K_0} e_{\Gamma/\Gamma'}[y] = \sum_{\sigma \in \Gamma/\Gamma'} \sigma(e_{r_{\Gamma/\Gamma'}} - e_1) \cdot [y] = |\Gamma/\Gamma'|(e_1 e_{r_{\Gamma/\Gamma'}} - e_1) \cdot [y] = 1.$$

We then only need to show the surjectivity. As a $\mathbb{Z}_{(p)}[\Gamma]$-module, $I_{L,p}$ admits the following decomposition

$$I_{L,p} = e_{\Gamma/\Gamma'} I_{L,p} \times (1 - e_{\Gamma/\Gamma'}) I_{L,p}.$$

Consequently $I_{L,p}^{\Gamma'} = \left(e_{\Gamma/\Gamma'} I_{L,p}\right)^{\Gamma'} \times \left((1 - e_{\Gamma/\Gamma'}) I_{L,p}\right)^{\Gamma'}$. By $I_{L,p} \hookrightarrow V := \mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} I_{L,p}$, we know that $x \in I_{L,p}$ is fixed by Γ' if and only if $e_1' \cdot x = x$ where the action happens in V. Since

$$e_1' \cdot (1 - e_{\Gamma/\Gamma'}) = e_1' \cdot (e_1 + e_{k+1} + \cdots + e_m) = e_1' \cdot e_1 = e_1,$$

for any element $z \in (1 - e_{\Gamma/\Gamma'})V$, it is fixed by Γ' if and only if it is fixed by Γ. Therefore if $x \in I_{L,p}^{\Gamma'}$, then

$$x = y \cdot z$$

with $y \in \left(e_{\Gamma/\Gamma'} I_{L,p}\right)^{\Gamma'}$ and $z \in I_{L,p}^{\Gamma}$. By Lemma 2.5.8, the $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$-module $e_{\Gamma/\Gamma'} I_{L,p}$ is cohomologically trivial, hence

$$(e_{\Gamma/\Gamma'} I_{L,p})^{\Gamma'} / \operatorname{Nm}_{L/K} e_{\Gamma/\Gamma'} I_{L,p} = \hat{H}^0(\Gamma', e_{\Gamma/\Gamma'} I_{L,p}) = 1.$$

Therefore, y is always an element in $I_{K,p}$. If the element above $x = y \cdot z$ is contained in $I_{K,p}$, then z is also contained in $I_{K,p}$, i.e.,

$$I_{K,p} = \left(I_{K,p} \cap e_{\Gamma/\Gamma'} I_{L,p}\right) \times \left(I_{K,p} \cap I_{L,p}^{\Gamma}\right),$$

where the direct product is the direct product as abelian groups. Then by (2.5.2), $[z] \in \operatorname{Cl}_{K_0}[p^\infty]$, and $[x] \equiv [y]$ in the relative class group $\operatorname{Cl}_{K/K_0}[p^\infty] = \operatorname{Cl}_K[p^\infty] / \operatorname{Cl}_{K_0}[p^\infty]$, which proves Claim 2. Moreover, the claim also tells us that $i_*(\operatorname{Cl}_{K/K_0}[p^\infty]) \subseteq e_{\Gamma/\Gamma'} \operatorname{Cl}_{L/K_0}[p^\infty]$.

Final Step: Since p is a good prime for $e_{\Gamma/\Gamma'}$, we know that $e_{\Gamma/\Gamma'} \in \mathbb{Z}_{(p)}[\Gamma]$ and $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$ is a maximal order of $e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]$, hence obtain the following short exact sequence

$$1 \to e_{\Gamma/\Gamma'} P_{L,p} \to e_{\Gamma/\Gamma'} I_{L,p} \to e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty] \to 1,$$

where every object showing up is an $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma]$-module. Then by Lemma 2.5.8, we know that $e_{\Gamma/\Gamma'} P_{L,p}$, $e_{\Gamma/\Gamma'} I_{L,p}$ and $e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty]$ are all cohomologically trivial as Γ-modules. So the identity

$$\left(e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty]\right)^{\Gamma'} / \operatorname{Nm}_{L/K} e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty] = \hat{H}^0(\Gamma', e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty]) = 1$$

holds. This immediately implies that if $[x] \in (e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty])^{\Gamma'}$, then $[x]$ is represented by an ideal coming from K, and $i_* : \operatorname{Cl}_{K/K_0}[p^\infty] \to (e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty])^{\Gamma'}$ is surjective. Similarly, by

$$\hat{H}^0(\Gamma', e_{\Gamma/\Gamma'} I_{L,p}) = 1, \text{ and } \hat{H}^0(\Gamma', e_{\Gamma/\Gamma'} P_{L,p}) = 1$$

we know that

$$(e_{\Gamma/\Gamma'} I_{L,p})^{\Gamma'} = I_{K,p} \cap e_{\Gamma/\Gamma'} I_{L,p}, \text{ and } (e_{\Gamma/\Gamma'} P_{L,p})^{\Gamma'} = P_{K,p} \cap e_{\Gamma/\Gamma'} P_{L,p}.$$

Also by $\hat{H}^1(\Gamma', e_{\Gamma/\Gamma'} P_{L,p}) = 1$, we have the short exact sequence

$$1 \to (e_{\Gamma/\Gamma'} P_{L,p})^{\Gamma'} \to (e_{\Gamma/\Gamma'} I_{L,p})^{\Gamma'} \to (e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty])^{\Gamma'} \to 1.$$

Then these identities together with the short exact sequence (2.5.3) gives the following commutative diagram which concludes the proof:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & P_{K,p} \cap e_{\Gamma/\Gamma'} P_{L,p} & \longrightarrow & I_{K,p} \cap e_{\Gamma/\Gamma'} I_{L,p} & \longrightarrow & \operatorname{Cl}_{K/K_0}[p^\infty] & \longrightarrow & 1 \\
 & & \| & & \| & & \downarrow{\scriptstyle i_*} & & \\
1 & \longrightarrow & (e_{\Gamma/\Gamma'} P_{L,p})^{\Gamma'} & \longrightarrow & (e_{\Gamma/\Gamma'} I_{L,p})^{\Gamma'} & \longrightarrow & (e_{\Gamma/\Gamma'} \operatorname{Cl}_L[p^\infty])^{\Gamma'} & \longrightarrow & 1.
\end{array}$$

□

2.6 Reinterpretation of the Cohen-Martinet Heuristics in the non-Galois case

In this section, we reinterpret the distribution on abelian groups from (2.5.1) that we have shown are predicted by the Cohen-Martinet heuristics to be the distribution of class groups of non-Galois fields. Returning to the principle that objects should appear inversely as often as their number of automorphisms, we will see that these class groups of non-Galois fields have certain structure and the distribution is given as inverse to the number of automorphisms of that structure. We end the sections with several examples for different groups Γ.

We first define some notation used in this section. Let Γ' be a fixed subgroup of Γ. We've defined the trivial idempotent e_1 in Section 2.1, the augmentation character $a_{\Gamma/\Gamma'}$ and the central idempotent $e_{\Gamma/\Gamma'}$ of $\mathbb{Q}[\Gamma]$ associated to it in Section 2.4. Let $e_{r_{\Gamma/\Gamma'}} = e_1 + e_{\Gamma/\Gamma'}$ be the central idempotent associated to the character $r_{\Gamma/\Gamma'}$, and e_1' be the irreducible central idempotent associated to the unit character $1_{\Gamma'}$ of Γ' in $\mathbb{Q}[\Gamma']$. Note that e_1' is naturally an idempotent in $\mathbb{Q}[\Gamma]$ via the embedding $\Gamma' \hookrightarrow \Gamma$, but it is not necessarily central. Throughout this section, let S be a fixed finite set of *good primes* for $e_{\Gamma/\Gamma'}$ (see definition in Section 2.5), and $\mathfrak{O} \subseteq \mathbb{Q}[\Gamma]$ be a maximal $\mathbb{Z}_S$-order containing the group ring $\mathbb{Z}_S[\Gamma]$. By our assumption, $e_{\Gamma/\Gamma'}\mathfrak{O}$ is exactly $e_{\Gamma/\Gamma'}\mathbb{Z}_S[\Gamma]$.

Definition 2.6.1. For any (Γ,Γ)-bimodule M and any subgroup Λ of Γ, let ${}^{\Lambda}M$ be the subgroup of M fixed by the action of Λ on the left. Similarly M^{Λ} is the subgroup fixed by the action of Λ on the right.

Caution: The notation M^{Λ} is *different* from the use in previous sections, as before we only considered left actions. The reason for these two notations is that objects like $\mathfrak{O}$ are (Γ,Γ)-bimodules and we have to distinguish left and right Γ'-invariant parts.

Integral model for the Hecke algebra and Morita equivalence

First of all, $\mathbb{Q}[\Gamma]$ is a (Γ,Γ)-bimodule, we can consider the subspace ${}^{\Gamma'}\mathbb{Q}[\Gamma]^{\Gamma'}$, which is also called the Hecke algebra, written as $\mathbb{Q}[\Gamma'\backslash\Gamma/\Gamma']$, and which we will write as $e_1'\mathbb{Q}[\Gamma]e_1'$. Note that $e_1'\mathbb{Q}[\Gamma]e_1'$ is a $\mathbb{Q}$-algebra, but its identity e_1' is not the identity of $\mathbb{Q}[\Gamma]$. If V is any left $\mathbb{Q}[\Gamma]$-module, then ${}^{\Gamma'}V$ is naturally a left $e_1'\mathbb{Q}[\Gamma]e_1'$-module. Let $e_1'xe_1' \in e_1'\mathbb{Q}[\Gamma]e_1'$ and $v \in {}^{\Gamma'}V$, then for all $\tau \in \Gamma'$, we have

$$\tau \cdot (e_1'xe_1' \cdot v) = (\tau e_1'xe_1') \cdot v = e_1'xe_1' \cdot v.$$

This shows that $e_1'xe_1'v$ is still fixed by Γ', hence $e_1'xe_1' \cdot {}^{\Gamma'}V \subseteq {}^{\Gamma'}V$. Also for a left $\mathbb{Q}[\Gamma]$-module V, we always have

$${}^{\Gamma'}V = {}^{\Gamma'}(e_{r_{\Gamma/\Gamma'}}V).$$

So we see that for $\mathbb{Q}[\Gamma]$-module V, the invariants ${}^{\Gamma'}V$ are naturally a $e_1'\mathbb{Q}[\Gamma]e_1'$-module. Our goal is now to construct an integral version of this kind of structure. Given a finite $\mathfrak{O}$-module G, one has a natural action of $\mathcal{P} := {}^{\Gamma'}\mathfrak{O}^{\Gamma'} = \mathfrak{O} \cap e_1'\mathbb{Q}[\Gamma]e_1'$ on ${}^{\Gamma'}G$ by reasoning as

above. However, in general $\mathcal{P}$ is not even a ring, because if S contains any primes dividing $|\Gamma'|$, then $\mathcal{P}$ does not contain a multiplicative identity. Even if S does not contain any primes dividing $|\Gamma'|$, it is not clear what kind of ring $\mathcal{P}$ is. We will construct a ring $\mathfrak{o}$, agreeing with $\mathcal{P}$ when S does not contain primes dividing $|\Gamma|$ and larger than $\mathcal{P}$ otherwise, and show that this larger ring $\mathfrak{o}$ still acts on ${}^{\Gamma'}G$. After proving several results, in Corollary 2.6.8, we will see that $\mathfrak{o}$ is actually a maximal order.

Definition 2.6.2. We define

$$\mathfrak{o} = {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}e_1').$$

We include the factor $e_{\Gamma/\Gamma'}$ because of our intended application to (relative) class groups. When $\Gamma = S_n$ and $\Gamma' = S_{n-1}$ is the stabilizer of an element, then we have $e_{\Gamma/\Gamma'}\mathfrak{O} = M_{n-1}(\mathbb{Z}_S)$ and $\mathfrak{o} = \mathbb{Z}_S$ (see Example 2.6.15). When $\Gamma = D_4$ and Γ' is a non-central order 2 subgroup, we have $e_{\Gamma/\Gamma'}\mathfrak{O} = \mathbb{Z}_S \times M_2(\mathbb{Z}_S)$, and $\mathfrak{o} = \mathbb{Z}_S^2$ (see Example 2.6.16). When $\Gamma = A_5$, we let Γ act on $\{1,2,3,4,5\}$ in the usual way and let Γ' be the subgroup fixing 1. Then $e_{\Gamma/\Gamma'}\mathfrak{O} = M_4(\mathbb{Z}_S)$ and $\mathfrak{o} = \mathbb{Z}_S$. As suggested by these examples, we will show in general that $e_{\Gamma/\Gamma'}\mathfrak{O}$ and $\mathfrak{o}$ are Morita equivalent in Theorem 2.6.7, even though in general in they can have more complicated structures as arbitrary maximal orders in sums of matrix algebras over division algebras. This Morita equivalence will play a central role in our reinterpretation of the prediction of the Cohen-Martinet heuristics in the non-Galois case.

We start by showing that $\mathfrak{o}$ is an order of the semisimple $\mathbb{Q}$-algebra $e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$.

Proposition 2.6.3. *Let $e_1, \dots, e_m$ be the distinct irreducible central idempotents of $\mathbb{Q}[\Gamma]$ and $e_{\Gamma/\Gamma'} = e_2 + \cdots + e_k$. The $\mathbb{Q}$-algebra $e_1'\mathbb{Q}[\Gamma]e_1' = {}^{\Gamma'}\mathbb{Q}[\Gamma]^{\Gamma'}$ is a semisimple $\mathbb{Q}$-algebra whose decomposition into simple components is given by*

$$e_1'\mathbb{Q}[\Gamma]e_1' = \prod_{i=1}^{k} e_1'e_i\mathbb{Q}[\Gamma]e_1'.$$

The category of $e_1'\mathbb{Q}[\Gamma]e_1'$-modules is equivalent to the category of $e_{r_{\Gamma/\Gamma'}}\mathbb{Q}[\Gamma]$-modules. The subgroup ${}^{\Gamma'}(\mathfrak{O}e_1')$ is a $\mathbb{Z}_S$-order of $e_1'\mathbb{Q}[\Gamma]e_1'$, and $\mathfrak{o}$ is a $\mathbb{Z}_S$-order of $e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$.

Proof. In the proof, let $A = \mathbb{Q}[\Gamma]$ and $A' = e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$. Note that $e_1'\mathbb{Q}[\Gamma]e_1e_1' = e_1A$ and ${}^{\Gamma'}\big((1-e_{\Gamma/\Gamma'})\mathfrak{O}e_1'\big) = {}^{\Gamma}\mathfrak{O}$, c.f. Lemma 2.5.9. We can focus on $e_{\Gamma/\Gamma'}A$, A' and $\mathfrak{o}$ (the "nontrivial parts") in the rest of the proof.

The irreducible central idempotents of A give a decomposition of A'

$$A' = e_2e_1'A' \times \cdots \times e_me_1'A',$$

with each component a $\mathbb{Q}$-algebra because e_ie_1' is central in A'. Note that $e_1' \cdot e_i \neq 0$ if and only if $e_i = e_1$ or $e_i \cdot e_{\Gamma/\Gamma'} \neq 0$ by Lemma 2.5.9. So we have

$$A' = e_2e_1'A' \times \cdots \times e_ke_1'A'.$$

For any simple $\mathbb{Q}$-algebra $B \cong M_l(D)$ where D is an division algebra and any idempotent $f \in B$, we have $fBf \cong M_{l'}(D)$ for some $l' \leq l$. This can be shown using the decomposition of

the identity into mutually orthogonal primitive idempotents by the Krull-Schmidt-Azumaya Theorem, see e.g. [53, p. 6.12].

We apply this result to $e_i e_1'$ for each $i = 2, \ldots, k$ as follows. The $\mathbb{Q}$-algebra $e_i A$ is simple, and $e_i e_1'$ is an idempotent in $e_i A$. Therefore if $e_i A \cong M_{l_i}(D_i)$ where D_i is some division algebra, then there exists some integer $0 < l_i' < l$, such that $e_i e_1' A' = e_i e_1' A e_i e_1' \cong M_{l_i'}(D_i)$, hence $e_1' e_i A'$ is a simple $\mathbb{Q}$-algebra for all $i = 1, \ldots, k$. Since A' is the direct sum of finitely many simple $\mathbb{Q}$-algebras, it is a semisimple $\mathbb{Q}$-algebra.

The equivalence of the category of $e_1' e_i A'$-modules and the category of $e_i A$-modules follows from the fact that they are both matrix algebras over D_i, hence A' is Morita equivalent to $e_{\Gamma/\Gamma'} A$. Finally by $e_1' e_1 \mathbb{Q}[\Gamma] e_1' = e_1 A \cong \mathbb{Q}$, the statements on $e_1' \mathbb{Q}[\Gamma] e_1'$ are all proved.

We now check that $\mathfrak{o}$ is indeed a subring of A'. By definition, $\mathfrak{o}$, as the Γ'-invariant part of an Γ-module, is an additive abelian group. For all $x, y \in e_{\Gamma/\Gamma'}\mathfrak{O}$ such that $xe_1', ye_1' \in \mathfrak{o}$, since $\sigma x e_1' = x e_1'$ for all $\sigma \in \Gamma'$, we know that $e_1' x e_1' = x e_1'$, i.e., $xe_1' \in A'$ and $\mathfrak{o} \subseteq A'$ is an additive subgroup. For $xe_1', ye_1' \in \mathfrak{o}$, we have $xe_1' ye_1' = x(e_1' ye_1') = xye_1'$, which is still an element in $\mathfrak{o}$ because $xy \in e_{\Gamma/\Gamma'}\mathfrak{O}$ and $(xe_1')ye_1'$ is fixed by Γ' on the left. In particular, $e_1' e_{\Gamma/\Gamma'}$ is contained in $\mathfrak{o}$ and is the identity for A', hence $\mathfrak{o}$ is indeed a subring of A'.

Then let's show that $\mathfrak{o}$ is a $\mathbb{Z}_S$-order in A'. We've already showed that $\mathfrak{o}$ is a subring of A'. Then we check that $\mathbb{Q} \otimes_{\mathbb{Z}_S} \mathfrak{o} = A'$. Let $x \in e_{\Gamma/\Gamma'} A$, then we can write it as $x = \frac{1}{n} y$ with some $n \in \mathbb{Z}$ and $y \in |\Gamma'|^2 e_{\Gamma/\Gamma'}\mathfrak{O}$ because $\mathbb{Q} \otimes e_{\Gamma/\Gamma'}\mathfrak{O} = e_{\Gamma/\Gamma'} A$. Therefore

$$e_1' x e_1' = \frac{1}{n} \otimes e_1' y e_1'$$

where $e_1' y e_1' \in {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O})^{\Gamma'} \subseteq \mathfrak{o}$ by our construction. This shows that $\mathbb{Q} \otimes \mathfrak{o} = A'$.

Finally we show that $\mathfrak{o}$ is finitely generated as a $\mathbb{Z}_S$-module. Since $e_{\Gamma/\Gamma'}\mathfrak{O}$ is finitely generated as a $\mathbb{Z}_S$-module, say $e_{\Gamma/\Gamma'}\mathfrak{O} = \mathbb{Z}_S \cdot x_1 + \cdots + \mathbb{Z}_S \cdot x_N$, then

$$\mathfrak{o} \subseteq \mathfrak{O} e_1' = \mathbb{Z}_S \cdot x_1 e_1' + \cdots + \mathbb{Z}_S \cdot x_N e_1',$$

is a submodule of a finitely generated $\mathbb{Z}_S$-module, hence itself finitely generated over $\mathbb{Z}_S$. □

Now we will show that the Γ'-invariant part of an $e_{\Gamma/\Gamma'}\mathfrak{O}$-module is naturally an $\mathfrak{o}$-module.

Lemma 2.6.4. *For any finitely generated $e_{\Gamma/\Gamma'}\mathfrak{O}$-module G, its Γ'-invariant part ${}^{\Gamma'}G$ is an $\mathfrak{o}$-module via the action*

$$(\sigma e_1') \cdot g := \sigma \cdot g,$$

where the right-hand side is the action of $e_{\Gamma/\Gamma'}\mathfrak{O}$ on G, for all $g \in {}^{\Gamma'}G$ and $\sigma e_1' \in \mathfrak{o}$ with $\sigma \in e_{\Gamma/\Gamma'}\mathfrak{O}$.

Remark. As the identity of $\mathfrak{o}$, the element $e_{\Gamma/\Gamma'} e_1'$ acts as identity on ${}^{\Gamma'}G$ for any $e_{\Gamma/\Gamma'}\mathfrak{O}$-module G despite the fact that $e_{\Gamma/\Gamma'} e_1'$ is not even contained $e_{\Gamma/\Gamma'}\mathfrak{O}$ in general.

Remark. We can immediately see from Theorem 2.5.6 that Cl^S_{K/K_0} is naturally an $\mathfrak{o}$-module. This will be the key to our interpretation of (2.5.1).

Proof. If $\sigma e_1' = \tau e_1'$ with $\sigma, \tau \in e_{\Gamma/\Gamma'}\mathfrak{O}$, then the sum of the coefficients of elements in the same left coset of Γ' must be the same, hence $\sigma \cdot g = \tau \cdot g$ for all $g \in {}^{\Gamma'}G$. This shows that the definition does not depend on the choice of $\sigma \in e_{\Gamma/\Gamma'}\mathfrak{O}$. Moreover, since $\sigma e_1'$ is fixed by Γ' on the left, we know that $\sigma e_1' g \in {}^{\Gamma'}G$. So we've shown that $\sigma e_1' \cdot g = \sigma g$ gives a well-defined map.

Note that $e_1' \cdot \sigma e_1' = \sigma e_1'$ for all $\sigma e_1' \in \mathfrak{o}$ by definition. If $\sigma_1 e_1', \sigma_2 e_1' \in \mathfrak{o}$ with $\sigma_1, \sigma_2 \in e_{\Gamma/\Gamma'}\mathfrak{O}$, then $\sigma_1 e_1' \sigma_2 e_1' = \sigma_1 \sigma_2 e_1'$ which shows that the action is associative. Finally, $\sigma_1 e_1' g + \sigma_2 e_1' g = (\sigma_1 + \sigma_2) g = (\sigma_1 + \sigma_2) e_1' g = (\sigma_1 e_1' + \sigma_2 e_1') g$. So this definition turns ${}^{\Gamma'}G$ into an $\mathfrak{o}$-module. □

We then prove the equivalence of the category of $e_{\Gamma/\Gamma'}\mathfrak{O}$-modules and the category of $\mathfrak{o}$-modules in the rest of this subsection.

Lemma 2.6.5. *Given a finitely generated left $e_{\Gamma/\Gamma'}\mathfrak{O}$-module G, the left $\mathfrak{o}$-module ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \otimes_{e_{\Gamma/\Gamma'}\mathfrak{O}} G$ is isomorphic to ${}^{\Gamma'}G$ as $\mathfrak{o}$-modules.*

Proof. It suffices to prove this for each component of G, for eG is a left Γ-module via the composition $\mathbb{Z}_S[\Gamma] \to \mathfrak{O} \to e\mathfrak{O}$ for each irreducible central idempotent e of $e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]$. We then fix e and assume $eG = G$. There is a natural $e\mathfrak{O}$-isomorphism $\varphi : e\mathfrak{O} \otimes_{e\mathfrak{O}} G \xrightarrow{\sim} G$ given by $\sigma \otimes g = \sigma \cdot g$. Note that $\sigma g \in {}^{\Gamma'}G$ for all $\sigma \in {}^{\Gamma'}(e\mathfrak{O})$. We then obtain an $ee_1'\mathfrak{o}$-morphism $\psi : {}^{\Gamma'}(e\mathfrak{O}) \otimes_{e\mathfrak{O}} G \to {}^{\Gamma'}G$ by restricting φ on the subgroup ${}^{\Gamma'}(e\mathfrak{O}) \otimes_{e\mathfrak{O}} G$. Because for all $\tau e_1' \in ee_1'\mathfrak{o}$ where $\tau \in e\mathfrak{O}$ we have

$$\tau e_1' \varphi(\sigma \otimes g) = \tau e_1'(\sigma g) = \tau\sigma g \qquad \varphi\big(\tau e_1'(\sigma \otimes g)\big) = \varphi(\tau\sigma \otimes g) = \tau\sigma g.$$

Claim: $\psi : {}^{\Gamma'}(e\mathfrak{O}) \otimes_{e\mathfrak{O}} G \to {}^{\Gamma'}G$ is an $ee_1'\mathfrak{o}$-isomorphism.

The morphism ψ is injective because φ is. For the proof of surjectivity, we first recall that a morphism $f : H_1 \to H_2$ of abelian groups is surjective if and only if $f_p : H_{1,p} \to H_{2,p}$ is surjective for all prime p where f_p and $H_{i,p}$ denote the localization at p. In addition, f_p is surjective if and only if $\hat{f}_p : \widehat{H}_{1,p} \to \widehat{H}_{2,p}$ is surjective where $\hat{f}_p$ and $\widehat{H}_{i,p}$ denote the completion at p.

Since $\widehat{\mathfrak{O}} := \mathfrak{O} \otimes_{\mathbb{Z}_S} \mathbb{Z}_p$ is a maximal $\mathbb{Z}_p$-order in $\mathbb{Q}_p[\Gamma]$ (see [52, p. 11.6]) and $\widehat{\mathfrak{o}} := \mathfrak{o} \otimes_{\mathbb{Z}_S} \mathbb{Z}_p$ is the same as ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\widehat{\mathfrak{O}}e_1')$, the results above go through similarly. In particular, the additive subgroup ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\widehat{\mathfrak{O}})$ of $e_{\Gamma/\Gamma'}\widehat{\mathfrak{O}}$ is a left $\widehat{\mathfrak{o}}$-module by the analogue of Lemma 2.6.4, hence an $(\widehat{\mathfrak{o}}, e_{\Gamma/\Gamma'}\widehat{\mathfrak{O}})$-bimodule. So we can reduce the problem to proving

$$\widehat{\psi}_p : {}^{\Gamma'}(e\widehat{\mathfrak{O}}) \otimes_{e\widehat{\mathfrak{O}}} \widehat{G} \to {}^{\Gamma'}\widehat{G}$$

is surjective for all $p \in S$.

By abuse of notation, let $\mathfrak{O}$ be a maximal $\mathbb{Z}_p$-order in $\mathbb{Q}_p[\Gamma]$ with p a good prime for $e_{\Gamma/\Gamma'}$, and let $\mathfrak{o} := {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}e_1')$ just like above. Let $e\mathbb{Q}_p[\Gamma] \cong M_l(D)$ be an isomorphism such that $e\mathfrak{O} \cong M_l(\mathcal{O})$ where D is a division algebra over $\mathbb{Q}_p$ and $\mathcal{O} \subseteq D$ is the unique maximal $\mathbb{Z}_p$-order in D with the unique two-sided maximal ideal $\mathfrak{p}$, c.f. [52, (12.8), (17.3)]. Then the

finitely generated $e\mathfrak{O}$-module G admits the following matrix representation

$$G \cong \begin{pmatrix} \mathcal{O} & \cdots & \mathcal{O} \\ \mathcal{O} & \cdots & \mathcal{O} \\ \vdots & \vdots & \vdots \\ \mathcal{O} & \cdots & \mathcal{O} \end{pmatrix}_{l\times m} \oplus \begin{pmatrix} \mathcal{O}/\mathfrak{p}^{r_1} & \mathcal{O}/\mathfrak{p}^{r_2} & \cdots & \mathcal{O}/\mathfrak{p}^{r_n} \\ \mathcal{O}/\mathfrak{p}^{r_1} & \mathcal{O}/\mathfrak{p}^{r_2} & \cdots & \mathcal{O}/\mathfrak{p}^{r_n} \\ \vdots & \vdots & \vdots & \vdots \\ \mathcal{O}/\mathfrak{p}^{r_1} & \mathcal{O}/\mathfrak{p}^{r_2} & \cdots & \mathcal{O}/\mathfrak{p}^{r_n} \end{pmatrix}_{l\times n}$$
$$= \big(M_{l\times 1}(\mathcal{O})\big)^m \oplus M_{l\times 1}(\mathcal{O}/\mathfrak{p}^{r_1}) \oplus \cdots \oplus M_{l\times 1}(\mathcal{O}/\mathfrak{p}^{r_n}),$$

such that the action of $e\mathfrak{O} \cong M_l(\mathcal{O})$ on G is exactly the left matrix multiplication. We may therefore assume without loss of generality that G is indecomposable, i.e., $G \cong M_{l\times 1}(\mathcal{O})$ if G is projective or $G \cong M_{l\times 1}(\mathcal{O}/\mathfrak{p}^r)$ with $r \geq 1$ if G is torsion. Let f be the primitive idempotent such that

$$f \mapsto \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

via $e\mathbb{Q}_p[\Gamma] \cong M_l(D)$. There exists a surjective morphism $\pi : e\mathfrak{O} \to G$ given by the composition of $e\mathfrak{O} \to \mathfrak{O}f$ defined by $x \mapsto xf$ and the quotient map $\mathcal{O} \to \mathcal{O}/\mathfrak{p}^r$. Since $e\mathfrak{O}$ is projective, by Lemma 2.5.8, the induced map ${}^{\Gamma'}(e\mathfrak{O}) \to {}^{\Gamma'}G$ is also surjective. For any $g \in {}^{\Gamma'}G$, there exists $\sigma e \in {}^{\Gamma'}(e\mathfrak{O})$ such that $\pi(\sigma e) = g$. In particular, by definition of π, we may assume that $\sigma e = \sigma f \in \mathfrak{O}f$, hence

$$\psi\big(\sigma f \otimes \pi(f)\big) = \sigma f \cdot \pi(f) = \pi(\sigma f) = g.$$

This proves the surjectivity of ψ, hence the lemma. □

Lemma 2.6.6. *If e is a central irreducible idempotent contained in $e_{\Gamma/\Gamma'}$, then the subgroup $e\mathfrak{O}e'_1$ of $e\mathbb{Q}[\Gamma]$ consisting of elements of the form exe'_1 with $x \in \mathfrak{O}$ is an $(e\mathfrak{O}, ee'_1\mathfrak{o})$-bimodule where the right $ee'_1\mathfrak{o}$-action is given by right multiplication in $\mathbb{Q}[\Gamma]$. Then the $(e\mathfrak{O}, e\mathfrak{O})$-bimodule homomorphism $e\mathfrak{O}e'_1 \otimes_{ee'_1\mathfrak{o}} {}^{\Gamma'}(e\mathfrak{O}) \to e\mathfrak{O}$ defined by $exe'_1 \otimes y \mapsto exe'_1y$, where the right-hand side is the multiplication in $\mathbb{Q}[\Gamma]$, is surjective.*

Proof. The map is well-defined because $e'_1 \cdot y = y$ by multiplication in the group algebra $\mathbb{Q}_p[\Gamma]$, hence the product is actually exy which is contained in $e\mathfrak{O}$. Just like in the proof of Lemma 2.6.5, we will check the surjectivity locally and use the same abuse of notations for $\mathfrak{O}$ and $\mathfrak{o}$. Let $e\mathbb{Q}_p[\Gamma] \cong M_l(D)$ be an isomorphism of $\mathbb{Q}_p$-algebras with D a division algebra over $\mathbb{Q}_p$ such that $e\mathfrak{O} \cong M_l(\mathcal{O})$ under the isomorphism where $\mathcal{O} \subseteq D$ is the unique maximal $\mathbb{Z}_p$-order of D with the unique maximal two-sided ideal $\mathfrak{p}$ generated by a prime element π.

Since $\mathcal{O}$ is given by the valuation on D extended from the valuation on $\mathbb{Q}_p$, there exists a smallest integer $n \in \mathbb{Z}$ such that $e'_1\pi^n \in e\mathfrak{O}$. In particular, there exists at least one unit element in the matrix representation of $e'_1\pi^n$.

Claim: $e'_1\pi^n$ can generate the whole of $e\mathfrak{O} = M_l(\mathcal{O})$ as $(e\mathfrak{O}, e\mathfrak{O})$-bimodule. This can be shown by constructing the usual basis $\{E_{ij}\}$ from $e'_1\pi^n$ via finitely many row/column operations.

Since $e_1'\pi^n$ is contained in the image, the claim shows that $e\mathfrak{O}e_1' \otimes_{ee_1'\mathfrak{o}} {}^{\Gamma'}(e\mathfrak{O}) \to e\mathfrak{O}$ is surjective, and we prove the lemma. □

We finally have the following.

Theorem 2.6.7. *The category of $e_{\Gamma/\Gamma'}\mathfrak{O}$-modules and the category of $\mathfrak{o}$-modules are Morita equivalent via the functors:*

$$
\begin{aligned}
&{}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \otimes_{e_{\Gamma/\Gamma'}\mathfrak{O}} - : e_{\Gamma/\Gamma'}\mathfrak{O}\text{−Mod} \to \mathfrak{o}\text{−Mod} \\
&e_{\Gamma/\Gamma'}\mathfrak{O}e_1' \otimes_{\mathfrak{o}} - : \mathfrak{o}\text{−Mod} \to e_{\Gamma/\Gamma'}\mathfrak{O}\text{−Mod}
\end{aligned}
$$

Proof. Let's denote by $(\ ,\ )$ the $e_{\Gamma/\Gamma'}\mathfrak{O}$-balanced bilinear map ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \times e_{\Gamma/\Gamma'}\mathfrak{O}e_1' \to \mathfrak{o}$ defined by $(x, ye_1') \mapsto xye_1'$. This map is well-defined because $xye_1' \in \mathfrak{O}e_1'$ and $e_1'xye_1' = xye_1'$ is contained in the Γ'-invariant part.

Similarly let $[\ ,\ ]$ denote the $\mathfrak{o}$-balanced bilinear map $e_{\Gamma/\Gamma'}\mathfrak{O}e_1' \times {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \to e_{\Gamma/\Gamma'}\mathfrak{O}$ given by $[xe_1', y] \mapsto xe_1'y = xy$. Since these bilinear maps are defined using the multiplication in $\mathbb{Q}_p[\Gamma]$, they satisfy the condition for a Morita context, i.e.,

$$
ze_1' \cdot (x, ye_1') = [ze_1', x] \cdot ye_1', \text{ and } z \cdot [xe_1', y] = (z, xe_1') \cdot y.
$$

Then $\{e_{\Gamma/\Gamma'}\mathfrak{O}, \mathfrak{o}, {}_{\mathfrak{o}}\big({}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O})\big)_{e_{\Gamma/\Gamma'}\mathfrak{O}}, {}_{e_{\Gamma/\Gamma'}\mathfrak{O}}\big(e_{\Gamma/\Gamma'}\mathfrak{O}e_1'\big)_{\mathfrak{o}}, (\ ,\ ), [\ ,\ ]\}$ forms a Morita context.

The map $e_{\Gamma/\Gamma'}\mathfrak{O}e_1' \otimes {}^{\Gamma'}\mathfrak{O} \to e_{\Gamma/\Gamma'}\mathfrak{O}$ is surjective by Lemma 2.6.6. The other map is also surjective because we have

$$
{}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \otimes_{e_{\Gamma/\Gamma'}\mathfrak{O}} e_{\Gamma/\Gamma'}\mathfrak{O}e_1' = {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}e_1') = \mathfrak{o}
$$

by Lemma 2.6.5. Then the equivalence and the functors are given by Morita theorem (see [53, Theorem 3.54]) directly. □

Corollary 2.6.8. *The $\mathbb{Z}_S$-order $\mathfrak{o}$ in $e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$ is a maximal order.*

Proof. By [52, p. 11.6], it suffices to show that $\widehat{\mathfrak{o}}_p = \mathfrak{o} \otimes_{\mathbb{Z}_S} \mathbb{Z}_p$ is a maximal $\mathbb{Z}_p$-order in $e_1'e_{\Gamma/\Gamma'}\mathbb{Q}_p[\Gamma]e_1'$ for each $p \in S$.

Let $A = \mathbb{Q}_p[\Gamma]$ and $A' = e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$. We use the same abuse of notation for $\mathfrak{O}$ and $\mathfrak{o}$ as in the proof of Lemma 2.6.5 (i.e., $\mathfrak{O} := \widehat{\mathfrak{O}}$ and $\mathfrak{o} := \widehat{\mathfrak{o}}$).

First of all $\mathfrak{o}$ is Morita equivalent to $e_{\Gamma/\Gamma'}\mathfrak{O}$. Since $e_{\Gamma/\Gamma'}\mathfrak{O}$ is hereditary and this property is preserved by Morita equivalence, we know that $\mathfrak{o}$ is also a hereditary ring. Let $e \neq e_1$ be an irreducible central idempotent in A such that $e \cdot e_1' \neq 0$, and $eA \cong M_l(D)$ where D is a division algebra over $\mathbb{Q}_p$ and $ee_1'A' \cong M_{l'}(D)$ for some $l' < l$ (see Proposition 2.6.3). By [52, p. 39.14], if $ee_1'\mathfrak{o}$ is a hereditary order in $ee_1'A'$, then it is of the form

$$
ee_1'\mathfrak{o} \cong \begin{pmatrix}
(\mathcal{O}) & (\mathfrak{p}) & (\mathfrak{p}) & \cdots & (\mathfrak{p}) \\
(\mathcal{O}) & (\mathcal{O}) & (\mathfrak{p}) & \cdots & (\mathfrak{p}) \\
(\mathcal{O}) & (\mathcal{O}) & (\mathcal{O}) & \cdots & (\mathfrak{p}) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(\mathcal{O}) & (\mathcal{O}) & (\mathcal{O}) & \cdots & (\mathcal{O})
\end{pmatrix}^{(n_1,\ldots,n_r)}
$$

where $\mathcal{O} \subseteq D$ is the maximal order in D and $\mathfrak{p}$ its unique maximal ideal and $n_1 + \cdots + n_r = l'$ gives the size of the block along the diagonal.

Assume for contradiction that $ee'_1\mathfrak{o}$ is not maximal. By [52, p. 17.3], we know that $r \geq 2$ and there exists at least two non-isomorphic indecomposable projective modules, because a column in the above matrix representation is exactly an indecomposable projective module. But this is already contradiction, for $e\mathfrak{O}$ only admits one indecomposable projective module up to isomorphism.

Therefore, $ee'_1\mathfrak{o}$ must be of the form $M_{l'}(\mathcal{O})$, and it is a maximal order of ee'_1A' again by [52, p. 17.3]. The argument holds for all ee'_1, hence $\mathfrak{o}$ is a maximal order of A'. □

Random $\mathfrak{o}$-Module

From (2.5.1), we were led to wanting to understand the distribution of the abelian groups ${}^{\Gamma'}X$ for our random $e_{\Gamma/\Gamma'}\mathfrak{O}$-modules X. Now, we realize that ${}^{\Gamma'}X$ is naturally an $\mathfrak{o}$-module, so we will instead consider the distribution of $\mathfrak{o}$-modules ${}^{\Gamma'}X$.

On one hand, the random $e_{\Gamma/\Gamma'}\mathfrak{O}$-module $X = X(e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma], \underline{u}, e_{\Gamma/\Gamma'}\mathfrak{O})$ defined in Section 2.1 with $\underline{u} = (u_2, \ldots, u_k) \in \mathbb{Q}^{k-1}$ gives us a random $\mathfrak{o}$-module ${}^{\Gamma'}X$. On the other hand, since $\mathfrak{o}$ is a maximal order in the semisimple $\mathbb{Q}$-algebra $e'_1e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1$, we can also define a random $\mathfrak{o}$-module $Y = (e'_1e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1, \underline{v}, \mathfrak{o})$ with $\underline{v} = (v_2, \ldots, v_k) \in \mathbb{Q}^{k-1}$. We are going to show that for suitably chosen $\underline{u} \in \mathbb{Q}^{k-1}$ and $\underline{v} \in \mathbb{Q}^{k-1}$, the random $\mathfrak{o}$-modules ${}^{\Gamma'}X$ and Y have the same distribution. For simplicity, let

$$X' = {}^{\Gamma'}X.$$

Theorem 2.6.9. *Let $e_1, \ldots, e_m$ be the distinct irreducible central idempotents of $\mathbb{Q}[\Gamma]$ and $e_{\Gamma/\Gamma'} = e_2 + \cdots + e_k$. Let χ_i be the $\mathbb{Q}$-irreducible character associated to e_i and φ_i be any fixed absolutely irreducible character contained in χ_i for all $i = 2, \ldots, k$. Let $X = X(e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma], \underline{u}, e_{\Gamma/\Gamma'}\mathfrak{O})$ and $Y = Y(e'_1e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1, \underline{v}, \mathfrak{o})$ with $\underline{u}, \underline{v} \in \mathbb{Q}^{k-1}$ so that u_i corresponds to e_i and v_i corresponds to $e_ie'_1$ for all $i = 2, \ldots, k$. The random $\mathfrak{o}$-modules $X' = {}^{\Gamma'}X$ and Y give the same probability distribution if and only if*

$$v_i = \frac{\langle \varphi_i, a_\Gamma \rangle}{\langle \varphi_i, a_{\Gamma/\Gamma'} \rangle} u_i$$

for all $i = 2, \ldots, k$, where $a_\Gamma = a_{\Gamma/1} := -1 + \mathrm{Ind}_1^\Gamma 1$ is the augmentation character of the trivial subgroup.

Proof. We will start by obtaining the formula for the probability distribution of X'. For any finite $\mathfrak{o}$-module H, we have $X' \cong H$ if and only if $X \cong e_{\Gamma/\Gamma'}\mathfrak{O}e'_1 \otimes_{\mathfrak{o}} H$ by Theorem 2.6.7. Therefore for any two finite $\mathfrak{o}$-modules H_1, H_2, let $G_i := e_{\Gamma/\Gamma'}\mathfrak{O}e'_1 \otimes_{\mathfrak{o}} H_i$ for $i = 1, 2$, and we have

$$\frac{\mathbb{P}(X' \cong H_1)}{\mathbb{P}(X' \cong H_2)} = \frac{|G_2|^{\underline{u}}|\mathrm{Aut}_{e_{\Gamma/\Gamma'}\mathfrak{O}}(G_2)|}{|G_1|^{\underline{u}}|\mathrm{Aut}_{e_{\Gamma/\Gamma'}\mathfrak{O}}(G_1)|} = \frac{|G_2|^{\underline{u}}|\mathrm{Aut}_{\mathfrak{o}}(H_2)|}{|G_1|^{\underline{u}}|\mathrm{Aut}_{\mathfrak{o}}(H_1)|}.$$

Given any finite $\mathfrak{o}$-module H, let $G := e_{\Gamma/\Gamma'}\mathfrak{O}e'_1 \otimes H$ be the finite $e_{\Gamma/\Gamma'}\mathfrak{O}$-module such that ${}^{\Gamma'}G \cong H$. By [14, Theorem 7.3], for each $i = 2, \ldots, k$, there exists some finite $\mathbb{Z}_S$-module G_i such that

$$e_i G \cong G_i^{\langle \chi_i, a_\Gamma \rangle} \quad \text{and} \quad e_i e'_1 H = {}^{\Gamma'}(e_i G) \cong G_i^{\langle \chi_i, a_{\Gamma/\Gamma'} \rangle}, \tag{2.6.1}$$

where the isomorphisms are isomorphisms as abelian groups. We then know that

$$|e_i G| = |e_i e'_1 H|^{\langle \chi_i, a_\Gamma \rangle / \langle \chi_i, a_{\Gamma/\Gamma'} \rangle}. \tag{2.6.2}$$

Therefore if

$$v_i = \frac{\langle \varphi_i, a_\Gamma \rangle}{\langle \varphi_i, a_{\Gamma/\Gamma'} \rangle} u_i$$

for all $i = 2, \ldots, k$, then $|G|^{\underline{u}} = |H|^{\underline{v}}$, hence X' is defined the same way as Y and they give the same probability distribution.

Conversely if X' and Y give the same distribution, then

$$\frac{|G_2|^{\underline{u}}}{|G_1|^{\underline{u}}} = \frac{|H_2|^{\underline{v}}}{|H_1|^{\underline{v}}}$$

for all finite $e_{\Gamma/\Gamma'}\mathfrak{O}$-modules G_1, G_2 such that $H_i := {}^{\Gamma'}G_i$ with $i = 1, 2$. Then the identities (2.6.1) tell us that this condition forces

$$v_i = \frac{\langle \varphi_i, a_\Gamma \rangle}{\langle \varphi_i, a_{\Gamma/\Gamma'} \rangle} u_i$$

for all $i = 2, \ldots, k$. □

Definition 2.6.10. Let L/K_0 be a Γ-extension and $\underline{u} \in \mathbb{Q}^m$ be the rank of L/K_0. Then define $\underline{v} \in \mathbb{Q}^{k-1}$ given by the formula in Theorem 2.6.9 to be the rank of $L^{\Gamma'}/K_0$. (In Section 2.7 we show this does not depend on L, but only $L^{\Gamma'}$.)

Just like in Section 2.2, we can express $|H|^{\underline{v}}$ in terms of the decomposition groups Γ_v at infinite places $v|\infty$.

Corollary 2.6.11. *If $\underline{u}$ is given by the rank of a Γ-extension L/K_0 and $\underline{v}$ the rank of $L^{\Gamma'}/K_0$ (as given in the definition just above), then for any finite $\mathfrak{o}$-module H, we have*

$$|H|^{\underline{v}} = |e_{\Gamma/\Gamma'}\mathfrak{O}e'_1 \otimes_{\mathfrak{o}} H|^{\underline{u}} = \prod_{v|\infty} |(e_{\Gamma/\Gamma'}\mathfrak{O}e'_1 \otimes_{\mathfrak{o}} H)^{\Gamma_v}|$$

where v runs over all infinite places of K_0.

Proof. This is the combination of Theorem 2.6.9 and Theorem 2.2.1. □

By Theorem 2.6.9, we can always identify the random $\mathfrak{o}$-module ${}^{\Gamma'}X$ with some random $\mathfrak{o}$-module $Y = Y(e'_1 e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1, \underline{v}, \mathfrak{o})$ and the Cohen-Martinet conjecture predicts Cl_K^S are distributed as random $\mathfrak{o}$-modules.

Theorem 2.6.12. *Let Γ be a finite group and $\Gamma' \subseteq \Gamma$ a subgroup. Assume that S only contains good primes for $e_{\Gamma/\Gamma'}$. If $\underline{u}$ is the rank of some Γ-extension L/K_0, then let $\underline{v}$ be the rank of $L^{\Gamma'}/K_0$ (as given in the definition just above) and $Y = Y(e_1' e_{\Gamma/\Gamma'} \mathbb{Q}[\Gamma] e_1', \underline{v}, \mathfrak{o})$ be the random finite $\mathfrak{o}$-module. For a non-negative function f defined on the class of isomorphism classes of finite $\mathfrak{o}$-modules, the Cohen-Martinet conjecture (Conjecture 2.5.2 for $f({}^{\Gamma'}-)$ and $e = e_{\Gamma/\Gamma'}$) implies that*

$$\lim_{x\to\infty} \frac{\sum_{|d_L|\le x} f(\mathrm{Cl}^S_{L^{\Gamma'}/K_0})}{\sum_{|d_L|\le x} 1} = \mathbb{E}\big(f(Y)\big),$$

where the sums are over Γ-extensions L/K_0 and the discriminant $|d_L| \le x$ and the rank of L/K_0 is $\underline{u}$.

In particular, the results of Section 2.4 all apply here to give the moments of the predicted distributions and see that the distributions are determined by their moments.

Remark. The probabilities in Theorem 2.6.12 are

$$\frac{c}{|H|^{\underline{v}}|\operatorname{Aut}_{\mathfrak{o}}(H)|}$$

for each finite $\mathfrak{o}$-module H. We also see that if we want the probability of obtaining some finite abelian group H, then the desired probability in (2.5.1) can be rewritten as a sum over $\mathfrak{o}$-module structures on the finite abelian group H of the above probabilities. One could also apply the class triples approach of Section 2.3 to obtain probabilities that are purely inversely proportional to automorphisms of some object. Perhaps the simplest way to do this to make a class triple from $e_{\Gamma/\Gamma'} \mathrm{Cl}^S_L$.

Examples

In this section, we give some examples of specific Γ and Γ' to see what $\mathfrak{o}$ is in that case. Given a finite group Γ and subgroup Γ', we define e_i, χ_i, φ_i as in Theorem 2.6.9. We have that $e_i\mathbb{Q}[\Gamma] \simeq M_{l_i}(D_i)$, where D_i is a division algebra with center K_i, and K_i is the field generated by the values of φ_i. We can decompose

$$a_{\Gamma/\Gamma'} = \sum_{i=2}^{k} a_i \chi_i.$$

for positive integers a_i. Then we can see from the proof of Proposition 2.6.3 and a dimension calculation using Frobenius reciprocity that

$$e_1' e_{\Gamma/\Gamma'} \mathbb{Q}[\Gamma] e_1' \simeq \bigoplus_{i=2}^{k} M_{a_i}(D_i).$$

From this we conclude the following about the cases in which there is really no additional structure by realizing the class group is an $\mathfrak{o}$-module.

Proposition 2.6.13. *The maximal $\mathbb{Z}_S$-order $\mathfrak{o}$ in $e_1' e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$ is isomorphic to $\mathbb{Z}_S$ if and only if $a_{\Gamma/\Gamma'}$ is absolutely irreducible.*

Example 2.6.14 ($a_{\Gamma/\Gamma'}$ multiplicity 1)**.** So if all the a_i are 1 and $D_i = K_i$ (i.e. all the Schur indices are 1), or equivalently, every absolutely irreducible character that appears in $a_{\Gamma/\Gamma'}$ appears with multiplicity 1, then by Corollary 2.6.8, we have that

$$\mathfrak{o} \simeq \bigoplus_{i=2}^{k} \mathbb{Z}_{K_i},$$

where $\mathbb{Z}_{K_i}$ is the localization of the ring of algebraic integers of K_i at by the non-zero rational integers not in S.

If in addition, all the decomposition groups Γ_v are trivial for a Galois Γ-extension L/K_0, then for the associated v_i for $L^{\Gamma'}$, we can compute using Theorem 2.6.9 that $v_i = r_K l_i$, where r_K is the number of infinite places of K.

Example 2.6.15 (An example on S_n)**.** Even more specifically, we consider the case where $K/\mathbb{Q}$ is a non-Galois extension whose Galois closure $L/\mathbb{Q}$ is a $\Gamma = S_n$-field such that K is the fixed field of $\Gamma' = S_{n-1}$ where $S_{n-1} \hookrightarrow S_n$ in the usual way. Moreover assume that $L/\mathbb{Q}$ is totally real, so $\underline{u} = \underline{1}$ by Theorem 2.2.1. Since $a_{\Gamma/\Gamma'}$ is absolutely irreducible with $a_{\Gamma/\Gamma'}\big(23\cdots(n-1)\big) = 1$, we have

$$a_{\Gamma/\Gamma'} = \frac{a_{\Gamma/\Gamma'}(1)}{|\Gamma|}\big((23\cdots(n-1))^{-1} + \cdots\big) = \frac{n-1}{n!}\big((23\cdots(n-1))^{-1} + \cdots\big).$$

Also, for $p \nmid n!/(n-1)$, one can explicitly compute $e_{\Gamma/\Gamma'}\mathbb{Z}_{(p)}[\Gamma] = M_{n-1}(\mathbb{Z}_{(p)})$. Therefore p is a good prime if and only if $p \nmid n!/(n-1)$. Let S be the set of good primes for $e_{\Gamma/\Gamma'}$.

By Theorem 2.6.9 we have

$$|H|^v = |H|^{n-1}$$

where $n = |\Gamma/\Gamma'|$, i.e., $v = n-1$. In this case, $\mathfrak{o}$ is just $\mathbb{Z}_S$. Hence we expect Cl_K^S to behave like a random abelian group without any additional structure coming from the $\mathfrak{o}$ action, and the predictions have each finite abelian $\mathbb{Z}_S$-module H appearing with probability $|H|^{-(n-1)}|\operatorname{Aut}(H)|^{-1}$ as Cl_K^S.

Example 2.6.16 (An example on D_4)**.** Let $\Gamma = D_4$, the dihedral group of order 8 and S only contain odd primes. Write $\Gamma = \langle \sigma, \tau\rangle$ with $\tau^2 = \sigma^4 = 1$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$. Let $K/\mathbb{Q}$ be a degree 4 extension with Galois closure $L|\mathbb{Q}$ a totally real Γ-field such that K is the fixed field of the subgroup $\Gamma' = \{1, \tau\}$ (so $\underline{u} = \underline{1}$ by Theorem 2.2.1).

The character $a_{\Gamma/\Gamma'}$ is of degree 3, the sum of two absolutely irreducible characters φ of degree 1, and χ of degree 2. Let e_φ, resp. e_χ, be the irreducible central idempotent in $\mathbb{Q}[\Gamma]$ associated to φ, resp. χ. The idempotents are given by

$$e_\chi = \frac{1}{8}(1 + \sigma^2 - \sigma - \sigma^3 + \tau + \sigma^2\tau - \sigma\tau - \sigma^3\tau) \quad \text{and} \quad e_\varphi = \frac{1}{2}(1 - \sigma^2)$$

and 2 is the only bad prime number for $e_{\Gamma/\Gamma'}$.

Since φ is an absolutely irreducible character of degree 1 and $e'_1 \cdot e_\varphi = e_\varphi$, we then know that $e_\varphi e'_1 \mathfrak{o} \cong \mathbb{Z}_S$. On the other hand, Frobenius reciprocity shows that $\dim_{\mathbb{Q}} e'_1 e_\chi \mathbb{Q}[\Gamma] e'_1 = 1$, hence $e_\chi e'_1 \mathfrak{o}$, as a maximal order in $e'_1 e_\chi \mathbb{Q}[\Gamma] e'_1$, is also isomorphic to $\mathbb{Z}_S$. So $\mathfrak{o} = \mathbb{Z}_S^2$ as an algebra.

On the other hand, the normalizer of Γ' is $\{1, \tau, \sigma^2, \sigma^2\tau\}$, i.e., there exists 2 automorphisms of $K/\mathbb{Q}$. In particular, the class group Cl_K^S is not only an abelian group but an abelian group with an order 2 automorphism, i.e., Cl_K^S is a $\mathbb{Z}_S[t]/(t^2-1)$-module with $t \cdot x = \sigma^2 \cdot x$. Moreover, one can check that the ring homomorphism $e_{\Gamma/\Gamma'} e'_1 \mathfrak{o} \to \mathbb{Z}_S[t]/(t^2-1)$ given by

$$e_\varphi e'_1 \mapsto \frac{1}{2}(1+t) \quad \text{and} \quad e_\chi e'_1 \mapsto \frac{1}{2}(1-t)$$

is an isomorphism which is compatible with the actions on class groups. So in this example, considering the $\mathfrak{o}$-module structure on Cl_K^S and the structure on Cl_K^S from the automorphisms of $K/\mathbb{Q}$ are equivalent.

We will also work out the predicted moments explicitly in this case. Let $X = (e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma], \underline{1}, e_{\Gamma/\Gamma'}\mathfrak{O})$, and let G be a finite $e_{\Gamma/\Gamma'}\mathfrak{O}$-module, and $H = {}^{\Gamma'}G$. Then

$$\mathbb{E}\left(|\mathrm{Sur}_{\mathfrak{o}}({}^{\Gamma'}X, H)|\right) = \mathbb{E}\left(|\mathrm{Sur}_{e_{\Gamma/\Gamma'}\mathfrak{O}}(X, G)|\right) = \frac{1}{|G|^{\underline{u}}} = \frac{1}{|e_\varphi G|}\frac{1}{|e_\chi G|}.$$

Then using (2.6.2), we have

$$\mathbb{E}\left(|\mathrm{Sur}_{\mathfrak{o}}({}^{\Gamma'}X, H)|\right) = \frac{1}{|\frac{1+t}{2}H||\frac{1-t}{2}H|^2}.$$

Example 2.6.17 (An Example on A_5)**.** This is an example where the non-Galois extension admits no "automorphism" but the ring $\mathfrak{o}$ is nontrivial.

Let $\Gamma = A_5$. The subgroup Γ' generated by (123) and (12)(45) is called the twisted S_3 in A_5 because this subgroup is isomorphic to S_3. It is a maximal proper subgroup of A_5. Since Γ is simple, this says that the normalizer of Γ' is itself.

Now assume that $K/\mathbb{Q}$ is a non-Galois extension with Galois closure a Γ-field $L|\mathbb{Q}$ such that $K = L^{\Gamma'}$. Since automorphisms of K over $\mathbb{Q}$ correspond to Γ' cosets of elements $\sigma \in \Gamma$ such that $\sigma\Gamma'\sigma^{-1} = \Gamma'$, then we can see that K admits no nontrivial automorphism.

The character $r_{\Gamma/\Gamma'}$ is given by a $\mathbb{Q}$-representation of dimension 10. By checking the character table, Γ has 4 characters over $\mathbb{Q}$. Note that there is a unit character contained in $r_{\Gamma/\Gamma'}$. The character $r_{\Gamma/\Gamma'}$ contains three different absolutely irreducible characters, say $r_{\Gamma/\Gamma'} = \chi_1 + \chi_2 + \chi_3$ where χ_1 is the unit character, χ_2 is the character of degree 4 and χ_3 is the character of degree 5. By Theorem 2.6.7, this implies that $\mathfrak{o}$ admits two orthogonal irreducible idempotents, hence cannot be isomorphic to $\mathbb{Z}_S$. By computations using Frobenius reciprocity, we can see that $e'_1 e_i \mathbb{Q}[\Gamma] e'_1$ is a one-dimensional $\mathbb{Q}$-vector space where e_i is the irreducible central idempotent associated to χ_i, for $i = 2, 3$. Therefore the ring $\mathfrak{o}$ is isomorphic to $\mathbb{Z}_S^2$. Moreover, we can check that a prime number p is good for $e_{\Gamma/\Gamma'}$ if and only if $p \neq 2, 3, 5$, i.e., $p \nmid |\Gamma|$. So for a set S of good primes, the class group Cl_K^S has a natural order 2 automorphism (from $(1, -1) \in \mathbb{Z}_S^2$) and the conjectures reflect this structure.

2.7 Independence of Galois field

Though we imagine the reader was thinking of L as the Galois closure of K in the last two sections, that was never strictly required. It could have also been a larger Galois extension. In fact, we could have even considered Γ' normal so that K/K_0 was Galois. With this realization, we see that the Cohen-Martinet heuristics make several (infinitely many) predictions for the averages of the the same class groups (though each prediction is with a different ordering of the fields, since the conjectures as worded are always ordered by the discriminants of the Galois fields). In this section, we show that all those predictions agree.

We start by showing that $\underline{v}$ does not depend on the choice of the Galois extension L/K_0 containing K/K_0 (see the explicit statement below). We start with a lemma, whose proof is straightforward.

Lemma 2.7.1. *If $\Gamma' \subseteq \Gamma$ is a normal subgroup, then e_1' is central in $\mathbb{Q}[\Gamma]$ and*

$$(e_1 + e_{\Gamma/\Gamma'})\mathbb{Q}[\Gamma] \cong e_1'\mathbb{Q}[\Gamma] \cong \mathbb{Q}[\Gamma/\Gamma'].$$

In particular, if we let $\bar{e}_1$ be the irreducible central idempotent in $\mathbb{Q}[\Gamma/\Gamma']$ associated to the unit character of Γ/Γ', then the maximal order $\mathfrak{o}$ of $e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]$ is isomorphic to a maximal order in $(1-\bar{e}_1)\mathbb{Q}[\Gamma/\Gamma']$.

Theorem 2.7.2. *Let K/K_0 be any finite extension with Galois closure a Γ-extension L/K_0 of rank $\underline{u} \in \mathbb{Q}^{m-1}$ such that $\mathrm{Gal}(L/K) \cong \Gamma$. Let $M|K_0$ be a Σ-extension of rank $\underline{w} \in \mathbb{Q}^{n-1}$ such that $L \subseteq M$ with $\mathrm{Gal}(M|L) \cong \Delta$, and $\mathrm{Gal}(M|K) \cong \Sigma'$. If S only contains good primes for $e_{\Gamma/\Gamma'} \in \mathbb{Q}[\Gamma]$ and $e_{\Sigma/\Sigma'} \in \mathbb{Q}[\Sigma]$, then the rank $\underline{v}$ of $L^{\Gamma'}/K_0$ and the rank $\underline{\tilde{v}}$ of $M^{\Sigma'}|K_0$ are the same. Moreover, ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O})$ is isomorphic to ${}^{\Sigma'}(e_{\Sigma/\Sigma'}\widetilde{\mathfrak{O}})$ where $\mathfrak{O}$, resp. $\widetilde{\mathfrak{O}}$, is a maximal $\mathbb{Z}_S$-order in $\mathbb{Q}[\Gamma]$, resp. in $\mathbb{Q}[\Sigma]$ provided that the embedding $\mathbb{Q}[\Gamma] \to \mathbb{Q}[\Sigma]$ defined by*

$$\gamma \mapsto \sigma \sum_{\delta \in \Delta} \delta$$

where γ is the image of δ under the surjective map $\Sigma \to \Gamma$, maps $\mathfrak{O}$ into $\widetilde{\mathfrak{O}}$.

Proof. We use E for central idempotents in $\mathbb{Q}[\Sigma]$ and e for the ones in $\mathbb{Q}[\Gamma]$. For example let $e_1' := \frac{1}{|\Gamma'|}\sum_{\gamma\in\Gamma'}\gamma$, $E_1' := \frac{1}{|\Sigma'|}\sum_{\sigma\in\Sigma'}\sigma$. Moreover let $F_1 := \frac{1}{|\Delta|}\sum_{\delta\in\Delta}\delta$. Note that $E_1' \cdot F_1 = F_1 \cdot E_1' = E_1'$. By Lemma 2.7.1, we have

$$\begin{aligned} E_1'\mathbb{Q}[\Sigma]E_1' = E_1'F_1\mathbb{Q}[\Sigma]E_1' &= \frac{1}{|\Sigma'|}\sum_{\sigma\in\Sigma'}\sigma\cdot\mathbb{Q}[\Sigma/\Delta]E_1' \\ &= \frac{1}{|\Sigma'/\Delta|}\sum_{\sigma\Delta\in\Sigma'/\Delta}\sigma\Delta\cdot\mathbb{Q}[\Sigma/\Delta]E_1' \cong e_1'\mathbb{Q}[\Gamma]e_1' \end{aligned}$$

This computation shows that ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O})$ is equivalent to ${}^{\Sigma'}(e_{\Sigma/\Sigma'}\widetilde{\mathfrak{O}})$, because they are both maximal orders in $e_1'\mathbb{Q}[\Gamma]e_1'$. Moreover, if the embedding $\mathbb{Q}[\Gamma] \hookrightarrow \mathbb{Q}[\Sigma]$ sends $\mathfrak{O}$ into $\widetilde{\mathfrak{O}}$,

then by the isomorphism in Lemma 2.7.1 $\mathbb{Q}[\Gamma] \cong (E_1 + E_{\Sigma/\Delta})\mathbb{Q}[\Sigma]$ which is induced by the embedding, we know that $\mathfrak{O} \cong (E_1 + E_{\Sigma/\Delta})\widetilde{\mathfrak{O}}$, hence the isomorphism ${}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \cong {}^{\Sigma'}(e_{\Sigma/\Sigma'}\widetilde{\mathfrak{O}})$.

Note that by Lemma 2.7.1, $E_{\Sigma/\Delta}\mathbb{Q}[\Sigma] \cong (1 - e_1)\mathbb{Q}[\Gamma]$, and they have same number of irreducible components whose correspondence is given by $E \mapsto EF_1$ for all irreducible central idempotents $E \in \mathbb{Q}[\Sigma]$. Assume without loss of generality that $E_{\Sigma/\Delta} = E_2 + \cdots + E_m$ in $\mathbb{Q}[\Sigma]$ and $E_iF_1 = e_i$ for all $i = 2, \ldots, m$.

Claim: $w_i = u_i$ for all $i = 2, \ldots, m$. Let's prove the claim. Let $\Sigma_v \subseteq \Sigma$ be any decomposition group of some infinite place $v|\infty$ of K_0 defined up to conjugacy. Note that the ranks $\underline{u}$ and $\underline{w}$ do not depend on the choice of the maximal orders. We may assume without loss of generality that $E_{\Sigma/\Delta}\widetilde{\mathfrak{O}} \cong (1 - e_1)\mathfrak{O}$. Let G be any finite $E_{\Sigma/\Delta}\widetilde{\mathfrak{O}}$-module and H the corresponding $(1 - e_1)\mathfrak{O}$-module under the isomorphism of maximal orders. Since G is fixed by Δ, hence a Σ/Δ-module, and we can take Γ_v to be the image of Σ_v under the surjective map $\Sigma \to \Gamma$, and obtain

$$|^{\Sigma_v}G| = |^{\Sigma_v\Delta}G| = |^{\Gamma_v}H|.$$

By Theorem 2.2.1, we know that the claim is true.

Then by the interpretation of $\underline{v}$ for non-Galois case and the fact that we can choose the maximal orders such that $E_{\Sigma/\Delta}\widetilde{\mathfrak{O}} \cong (1 - e_1)\mathfrak{O}$, we know that the computation of the rank $\underline{v}$ of K/K_0 can always be reduced to its Galois closure L/K_0, i.e., the rank $\underline{v}$ of K/K_0 is a property of K and the distribution of the random $\mathfrak{o}$-module $Y = (e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1', \underline{v}, \mathfrak{o})$ does not depend on the choice of the Galois extension $M|K_0$ containing K. □

Chapter 3

Distribution of the bad part of the class group

3.1 Non-randomness

The term non-randomness here refers to the case where we can obtain some nontrivial ideal classes in Cl_K associated to the ramified primes. There are two main reasons why we are interested in the relation between ideal classes and ramified primes. The first one is that we have the famous example of genus theory for quadratic number fields as in § 1.1, which means that from the definition of a quadratic number field alone we can tell the 2-rank of its class group. We of course want to see if this phenomena also happen when we look at higher degree fields. The second reason is that product of ramified primes is the main ordering we currently use for number fields. Even in the case people use some other orderings (discriminant, conductor etc.), they are still related to ramified primes. It then makes the results, providing nontrivial information about class groups asscociated to ramfied primes, more valuable. For the purpose of explaining the main results in this section, we first introduce a notion that will also be used in later sections.

Definition 3.1.1. Let $K/\mathbb{Q}$ be a number field, and let p, q be two rational primes. If $e_K(p) \equiv 0 \bmod q$, then we call p a *ramified prime of type* q. More generally, if $e_K(p) \equiv 0 \bmod q^l$ for some $l \geq 1$, then we call p a ramified prime of type q^l.

Because of the fundamental identity

$$[K : \mathbb{Q}] = \sum e_i f_i$$

where e_i is the ramification index and f_i is the inertia degree for a fixed prime, we only need to discuss ramified primes of type q for $q|[K : \mathbb{Q}]$.

Example 3.1.2. If $K/\mathbb{Q}$ is Galois itself, i.e., $\mathrm{Gal}(K/\mathbb{Q}) \cong \Gamma$, then for any rational prime p, one has $p\mathscr{O}_K = \prod_i \mathfrak{p}^e$. So it is just a question whether q divides the ramification index e

or not. An example would be a quadratic extension $K/\mathbb{Q}$ with $q = 2$. In this case, p is a ramified prime of type q if and only if p is ramified in $K/\mathbb{Q}$.

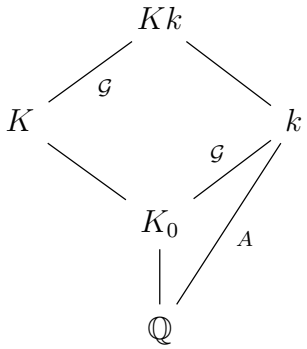
For non-Galois extensions, things become a little more complicated. Let $K/\mathbb{Q}$ be a non-Galois cubic extension with $q = 3$. Then p is a ramified prime of type 3 if and only if p is totally ramified in $K/\mathbb{Q}$. Note that there are partially ramified primes for non-Galois cubic extensions, i.e., $p\mathscr{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$, which are not ramified prime of type 3.

Genus theory

The goal of this section is to prove Theorem 1.1.6, by which we want to give a brief introduction on genus theory for number fields focused on the structure of the genus group. The basic question of genus theory is to find out the maximal unramified abelian extension of a number field K obtained by composing with an absolute abelian number field k. To be precise, we have the following definition.

Definition 3.1.3. let $K/\mathbb{Q}$ be a number field of degree n, and let $k/\mathbb{Q}$ be the maximal abelian extension such that Kk/K is an unramified extension. We call such a field the *genus field* Kk over K, and call the Galois group $\mathrm{Gal}(Kk/K)$ the *genus group* $\mathcal{G}$.

Since Kk/K is an unramified abelian extension, it is a subextension of the Hilbert extension of K whose Galois group is isomorphic to the class group Cl_K of K, hence the genus group is a quotient group of the class group Cl_K. According to Ishida [32, p.33-39], we make a summary of the results on the genus group. Fix a rational prime q such that $q^t \| n$ with $t \geq 1$. Let $A \cong \mathrm{Gal}(k/\mathbb{Q})$ be the Galois group of the abelian extension $k/\mathbb{Q}$, and let K_0 be the intersection of k and K which is also the maximal abelian subextension of $K/\mathbb{Q}$. See the diagram for summary below.



Definition 3.1.4. Let $K/\mathbb{Q}$ be a number field, and let p be a prime number. Let $k(p)$ be the unique subfield of $\mathbb{Q}(\zeta_p)$ with degree $\gcd(p-1, e_K(p))$ where ζ_p is a primitive pth root of unity.

Note that $k(p)$ is nontrivial if and only if $\gcd(p-1, e_K(p))$ is nontrivial. Moreover the Galois group of $k(p)/\mathbb{Q}$ is cyclic of order $\gcd(p-1, e_K(p))$. The first result is to describe the extension $k/\mathbb{Q}$ given the ramified primes of $K/\mathbb{Q}$.

Theorem 3.1.5. *[32, Chapter IV, Theorem 3] Let K be a number field, and let k be the abelian field such that Kk is the genus field. Let $k_1/\mathbb{Q}$ be the composite of $k(p)$ where p runs through all rational prime numbers such that $p \nmid e_K(p)$, and let $k_2/\mathbb{Q}$ be the intersection of all inertia subfields of k at p where p runs through all rational prime numbers such that $p \nmid e_K(p)$. Then $k = k_1k_2$ and $k_1 \cap k_2 = \mathbb{Q}$. In particular, A admits a subgroup*

$$\mathrm{Gal}(k/k_2) \cong \mathrm{Gal}(k_1/\mathbb{Q}) \cong \prod_{p \nmid e_K(p)} \mathbb{Z}/\gcd(p-1, e_K(p)).$$

Now that we have a result on the group A, the description of $\mathcal{G}$ follows from $A/\mathrm{Gal}(K_0/\mathbb{Q}) \cong \mathcal{G}$. In the sense of estimation for $\mathrm{rk}_q\, q^r\mathcal{G}$, we give the following statement.

Theorem 3.1.6. *Let $K/\mathbb{Q}$ be a number field with maximal abelian subextension $K_0/\mathbb{Q}$. Fix a rational prime q dividing $n := [K : \mathbb{Q}]$ and some integer $l \geq 1$, the q-rank of the group $q^{l-1}\mathcal{G}$ admits the following inequality*

$$\mathrm{rk}_q\, q^{l-1}\mathcal{G} \geq \#\{p \text{ is a ramified prime of type } q^l \text{ and } p \equiv 1 \bmod q\} - \mathrm{rk}_q\, \mathrm{Gal}(K_0/\mathbb{Q}).$$

Remark. Theorem 1.1.6 just follows from this result. Morever we can see that if $\mathcal{G}[q^\infty]$ admits higher torsion part, then $\mathrm{Cl}_K[q^\infty]$ must also have higher torsion part. Also, if there is no prime $p|e_K(p)$, then $k_2 = \mathbb{Q}$ and $A \cong \prod_{p \nmid e_K(p)} \mathbb{Z}/\gcd(p-1, e_K(p))$, hence $\mathcal{G} \cong \big(\prod_{p \nmid e_K(p)} \mathbb{Z}/\gcd(p-1, e_K(p))\big)/\mathrm{Gal}(K_0/\mathbb{Q})$.

Example 3.1.7. Let $K/\mathbb{Q}$ be a non-Galois cubic field, and q equal 3. Then the requirement $\gcd(p-1, e_K(p)) \equiv 0 \bmod 3$ is equivalent to p totally ramified in $K/\mathbb{Q}$ and $p \equiv 1 \bmod 3$. In other words, we have

$$\mathrm{rk}_3\, \mathrm{Cl}_K \geq \#\{p \text{ is a totally ramified prime and } p \equiv 1 \bmod 3\}.$$

This clearly generalizes genus theory for the quadratic case. See also [32, Chapter 5] for more discussions on the case of odd prime degree.

The class rank estimate on the invariant part of the class group

In the paper of Roquette and Zassenhaus [54], there is another result on the estimate of the q-rank of the class group with respect to ramified primes whose idea is totally different from genus theory. As seen in previous part, what genus theory really cares about is the genus group, which is the quotient of the class group. In this section the first goal is of course to give the proof Theorem 3.1.11. More importantly, we want to show the construction, which is more useful in this paper. We first need some notions to present their precise statement.

Definition 3.1.8. Let $K/\mathbb{Q}$ be a number field whose Galois closure is a Γ-extension $L/\mathbb{Q}$. By viewing the group of fractional ideals $\mathscr{I}_K$ of K as a subgroup of $\mathscr{I}_L$, we define the *invariant part of the class group*, denoted by C_K^Γ, of K under the action of Γ as the image of $\mathscr{I}_L^\Gamma \cap \mathscr{I}_K$ in Cl_K, i.e.,

$$C_K^\Gamma := \mathrm{im}(\mathscr{I}_L^\Gamma \cap \mathscr{I}_K \to \mathrm{Cl}_K).$$

To give a precise statement on the estimation for the invariant part C_K^Γ of the class group, we in addition need the following definition of q-radical subfields of K.

Definition 3.1.9 (q-radical subfields)**.** Let K_q be the subfield of K generated by all elements $\xi \in K$ which are q-radicals over $\mathbb{Q}$, i.e., $\xi^q \in \mathbb{Q}$. Let $n_q = [K_q : \mathbb{Q}]$ be its degree.

It is clear that $n_q \,|\, n$, hence one has

$$v_q(n_q) \leq v_q(n).$$

But if one wants to ask when $v_q(n_q)$ is strictly less than $v_q(n)$, then the following notation actually gives a condition for it.

Definition 3.1.10. Define the notion $\delta_K^{(q)}$ to be 1 or 0 according to whether or not the following conditions are *simultaneously* satisfied:

(i) $q > 2$;

(ii) K contains a primitive q-th root of unity ζ;

(iii) There exists some η in K^* such that $\zeta^{-1}\eta^q \in \mathbb{Q}$.

Remark. If all of the above three conditions hold, then one can show that $[K_q(\eta) : K_q] = q$ so that $n_q \cdot q \,|\, n$ and hence $v_q(n_q) + 1 \leq v_q(n)$. See [54, §6].

Using the notations introduced above, we can first state an estimation for C_K due to Roquette and Zassenhaus. Though in the paper [54], the main goal is to prove the result for the q-rank of the class group. We here instead describe the structure of the subgroup $C_K^\Gamma[q^\infty] \subseteq \mathrm{Cl}_K[q^\infty]$, which is also due to Roquette and Zassenhauss.

Theorem 3.1.11. *Let $K/\mathbb{Q}$ be a (not necessarily Galois) extension of degree n whose Galois group is Γ, and let q be a given prime number, and let $l \geq 1$ be an integer, then*

$$\begin{aligned}
&\#\{p \text{ is a ramified prime of type } q^l\} - \left(\mathrm{rk}_K + v_q(n_q) + \delta_K^{(q)}\right) \\
&\leq \mathrm{rk}_q\, q^{l-1} C_K^\Gamma \leq \\
&\#\{p \text{ is a ramified prime of type } q^l\}.
\end{aligned}$$

We prove the theorem by two lemmas. The first lemma gives a detailed description of the elements in C_K^Γ in the sense of fractional ideals.

Lemma 3.1.12. *[54, Equation (8)] Let $K/\mathbb{Q}$ be a number field whose Galois closure a Γ-extension $L/\mathbb{Q}$. For each prime p, define $\mathfrak{a}(p)$ to be the ideal such that $p\mathscr{O}_K = \mathfrak{a}(p)^{e_K(p)}$. Then $\mathscr{I}_K \cap \mathscr{I}_L^\Gamma$ is a free abelian group generated by $\{\mathfrak{a}(p)\}$. Let $\mathscr{P}_k$ be the group of principal ideals of a number field k. Then the group $\tilde{C}_K^\Gamma := \mathscr{I}_K \cap \mathscr{I}_L^\Gamma / \mathscr{P}_\mathbb{Q}$ is given by*

$$\tilde{C}_K^\Gamma \cong \prod_p \mathbb{Z}/e_K(p).$$

The second lemma is to estimate the difference between principal ideals of K and $\mathbb{Q}$.

Lemma 3.1.13. *[54, Equation(11)] Let $K/\mathbb{Q}$ be a number field whose Galois closure a Γ-extension $L/\mathbb{Q}$, and let $\mathcal{P}_k$ be the group of principal ideals of a number field k. Then*

$$rk_q \mathscr{P}_K^\Gamma / \mathscr{P}_\mathbb{Q} \leq \mathrm{rk}_K + v_q(n_q) + \delta_K^{(q)}, \tag{3.1.1}$$

where $\mathscr{P}_K^\Gamma := \mathscr{P}_K \cap \mathscr{I}_L^\Gamma$.

Now let's prove the theorem.

Proof of Theorem 3.1.11. It is clear that Lemma 3.1.12 gives the upper bound of $\mathrm{rk}_q\, q^{l-1} C_K^\Gamma$, because $\mathscr{P}_\mathbb{Q} \subseteq \mathscr{P}_K$. According to the short exact sequence

$$0 \to \mathscr{P}_K^\Gamma / \mathscr{P}_\mathbb{Q} \to \mathscr{I}_K^\Gamma / \mathscr{P}_\mathbb{Q} \to C_K^\Gamma \to 0,$$

the inequality (3.1.1) tells us the lower bound directly. □

An obvious application is to apply the theorem to the class group Cl_K, for $C_K^\Gamma \subseteq \mathrm{Cl}_K$.

Corollary 3.1.14. *Let K be a number field of degree n over $\mathbb{Q}$, and let q be a prime number, and let $l \geq 1$ be an integer, then*

$$\mathrm{rk}_q\, q^{l-1} \mathrm{Cl}_K \geq \#\{p \text{ is a ramified prime of type } q^l\} - \left(\mathrm{rk}_K + v_q(n_q) + \delta_K^{(q)}\right).$$

Remark. One can show that the number $\mathrm{rk}_K + v_q(n_q) + \delta_K^{(q)}$ is always smaller than $2(n-1)$, i.e., the above inequality has a weaker but shorter expression

$$\mathrm{rk}_q\, q^{l-1} \mathrm{Cl}_K \geq \#\{\text{ramified primes of type } q^l\} - 2(n-1),$$

which proves the statement of Theorem 1.1.7.

One of the advantages of this theory, as mentioned above, is that C_K^Γ is a subgroup of Cl_K. So, we can even try to discuss the relative class group here, i.e., for a subfield $K' \subseteq K$, we want to give a description for $C_K^\Gamma \cap \mathrm{Cl}(K/K')$.

Theorem 3.1.15. *Let $K/\mathbb{Q}$ be a number field of degree n whose Galois group is Γ. If $K' \subseteq K$ such that $q^l \| [K : K']$ where q is a rational prime, and $l \geq 1$, then*

$$\mathrm{rk}_q\, q^{l-1} \mathrm{Cl}(K/K') \geq \#\{p \text{ is a ramified prime of type } q^l\} - 2(n-1).$$

Proof. For each prime p, recall that $\mathfrak{a}(p)$ is the ideal of K such that $p\mathscr{O}_K = \mathfrak{a}(p)^{e_K(p)}$. We've shown in Lemma 3.1.12 that $\mathfrak{a}(p)$ is fixed by the action of Γ, viewed as an element of $\mathscr{I}_L$. So, we have the following computation

$$\mathrm{Nm}_{K/K'}(\mathfrak{a}(p)) = \mathfrak{a}(p)^{[K:K']},$$

where $\mathfrak{a}(p)^{[K:K']}$ is treated as an ideal of K'. If $q^l | e_K(p)$, and $\mathfrak{b}(p) := (\mathfrak{a}(p))^{e_K(p)/q^l}$, then $\mathrm{Nm}_{K/K'}(\mathfrak{b}(p))$ becomes a power of $p\mathscr{O}_{K'}$, hence a principal ideal of K'. So, $\mathfrak{b}(p)$ represents an ideal class of $\mathrm{Cl}(K/K')$. By Lemma 3.1.12, the group C_K^Γ is generated by ideals of the form $\mathfrak{a}(p)$, we therefore know that the subgroup $B_K^\Gamma := \langle \mathfrak{b}(p) | p \text{ is a ramified prime of type } q^l \rangle / \mathscr{P}_K \subseteq C_K^\Gamma[q]$ is contained in $\mathrm{Cl}(K/K')$. In particular, $\langle \mathfrak{b}(p) \rangle / \mathscr{P}_\mathbb{Q} \cong \prod_{i=1}^s \mathbb{Z}/q^l$, where $s = \#\{p \text{ is a ramified prime of type } q\}$. Then by Lemma 3.1.13, we know that $\mathrm{rk}_q \mathscr{P}_K^\Gamma / \mathscr{P}_\mathbb{Q}$ is bounded above by a constant $\mathrm{rk}_K + v_q(n_q) + \delta_K^{(q)} \leq 2(n-1)$, hence the result. □

3.2 Non-random primes

In Theorem 1.1.6 and Theorem 1.1.7, we see that $\mathrm{rk}_q \mathrm{Cl}_K$ is related to ramified primes of type q. If we fix the Galois group Γ, a question we can ask is for which primes q we can get ramified primes of type q? In a G-extension, let's first answer this question by the following lemma.

Lemma 3.2.1. *Let G be a finite transitive permutation group, and let q be a fixed prime. If $(K/\mathbb{Q}, \psi)$ is an extension of number fields such that its Galois closure $(\hat{K}, \psi)$ is a G-field and that $K = \hat{K}^{G_1}$, then a prime $p \nmid |G|$ is a ramified prime of type q if and only if $I(p) \cap \Omega(G, q^\infty) \neq \emptyset$ where $I(p)$ is the inertia subgroup of p.*

The proof comes from the relationship between the orbit sizes on an inertia generator and the ramification indices in the factorization $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$. See, for example, Neukirch [46, Definition 9.2 and Remark below] for details.

Example 3.2.2 (Counter-example)**.** We here show an example where the prime q divides the order of the extension $K/\mathbb{Q}$ but it is *not* a non-random prime. Consider the permutation group G defined as the image of the following morphism $A_4 \to S_6$, $(12)(34) \mapsto (1)(2)(34)(56)$, and $(123) \mapsto (134)(265)$. In the sense of number theory, $\mathcal{S}(G)$ contains number fields $K/\mathbb{Q}$ of degree 6, whose Galois closure $\hat{K}/\mathbb{Q}$ are A_4-extensions, so that the action of $\mathrm{Gal}(\hat{K}/\mathbb{Q})$ on $K/\mathbb{Q}$ induces a map $A_4 \to S_6$. The stabilizer of 1 is the image of $\{1, (12)(34)\}$ in this case. One can check that the group G has no element required in Definition 1.1.8 to turn the prime 2 into a non-random prime, despite the fact that 2 divides the order of $[K : \mathbb{Q}]$. Note that according to Cohen and Martinet [14], the prime 2 is not "good", i.e., 2 is not good but not non-random. See also [59, §7] for details on the concept "good primes".

Our most important goal in this section is to prove Theorem 1.1.12, which can justify the notion non-random prime from the view of statistics. We reach the theorem in several steps. Recall that we have the Conjectures 1.1.11 in § 1.1. Step zero is to prove the relation between these two conjectures, i.e., Conjecture 1.1.11(1) implies Conjecture 1.1.11(2).

Lemma 3.2.3. *Let G be a transitive permutation group and k be a fixed number field, and let $\mathcal{S} := \mathcal{S}(G, k)$. Let d be an invariant of number fields in $\mathcal{S}$. Suppose that Ω is a (nonempty)*

subset of G that is closed under invertible powering. If for all $r = 0, 1, 2, \ldots,$ there exists some r' such that

$$N(\mathcal{S}, d; (\Omega, r); x) = o\left(N(\mathcal{S}, d; (\Omega, r'); x)\right)$$

then for all $r = 0, 1, 2, \ldots,$ we have

$$N(\mathcal{S}, d, (\Omega, r); x) = o\left(N(\mathcal{S}, d; x)\right).$$

Proof. Since all fields counted by $N(\mathcal{S}, d; (\Omega, r); x)$ and $N(\mathcal{S}, d; (\Omega, r;); x)$ are also counted by $N(\mathcal{S}, d; x)$, we have $N(\mathcal{S}, d; (\Omega, r'); x) \leq N(S, d; x)$. The lemma then follows. □

The first step is to show that Conjecture 1.1.11(2) implies zero-probability.

Theorem 3.2.4. *Let $1 \leq G \leq S_n$ be a transitive permutation group, and let $\mathcal{S} := \mathcal{S}(G)$. Let $G_1 \subseteq H \subseteq G$, where G_1 is the stabilizer of 1 that fixes $K \in \mathcal{S}$. Let q be a non-random prime for G such that $q^l \| [H : G_1]$, where $l \geq 1$, and let $\Omega := \bigcup_{j=l}^{\infty} \Omega(G, q^j)$. Let d be an invariant of the number fields in $\mathcal{S}$. If for all $r = 0, 1, 2, \ldots,$ we have*

$$N(\mathcal{S}, d, (\Omega, r); x) = o(N(\mathcal{S}, d; x)),$$

then for all $r = 0, 1, 2, \ldots,$ we have

$$\mathbb{P}(\mathrm{rk}_q\, q^{l-1}\, \mathrm{Cl}(K/\hat{K}^H) \leq r) = 0,$$

where K runs over fields in $\mathcal{S}$ for the invariant d, and $\hat{K}$ is the Galois closure of K.

Proof. First of all, recall that we have for all finite abelian group A and for all $r = 0, 1, 2, \ldots,$

$$\mathbf{1}_{\mathrm{rk}_q \leq r}(A) = \begin{cases} 1 & \text{if } \mathrm{rk}_q\, A \leq r \\ 0 & \text{otherwise.} \end{cases}$$

According to Thereom 3.1.15, if there are at least $r+2n$ ramified primes p for $K/\mathbb{Q}$ contained in the set $\{p \nmid |G| : I(p) \cap \Omega \neq \emptyset\}$, then

$$\mathrm{rk}_q\, q^{l-1}\, \mathrm{Cl}(K/\hat{K}^H) > r.$$

If $N(\mathcal{S}, d, (\Omega, r); x) = o(N(\mathcal{S}, d; x))$ for all r, then this implies that

$$\begin{aligned} \mathbb{P}(\mathrm{rk}_q\, q^{l-1}\, \mathrm{Cl}(K/\hat{K}^H) \leq r) &= \lim_{x \to \infty} \frac{N(\mathcal{S}, d; \mathbf{1}_{\mathrm{rk}_q \leq r} \circ (q^{l-1}\, \mathrm{Cl}(K/\hat{K}^H)); x)}{N(\mathcal{S}, d; x)} \\ &\leq \lim_{x \to \infty} \frac{N(\mathcal{S}, d; \sum_{i=0}^{r+2n} \mathbf{1}_{(\Omega, i)}; x)}{N(\mathcal{S}, d; x)} = 0. \end{aligned}$$

□

Then let's prove that bounded probability, hence also zero-probability, implies infinite moment.

Theorem 3.2.5. *Let $1 \leq G \leq S_n$ be a transitive permutation group, and let $\mathcal{S} := \mathcal{S}(G)$. Let $G_1 \subseteq H \subseteq G$, where G_1 is the stabilizer of 1 that fixes $K \in \mathcal{S}$. Let d be an invariant of the number fields in $\mathcal{S}$. Let q be a rational prime and $l \geq 1$ be an integer. If there exists some constant $0 \leq c < 1$ such that for all $r = 0, 1, 2, \ldots$, we have*

$$\mathbb{P}(\mathrm{rk}_q\, q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H) \leq r) \leq c, \quad \textit{then} \quad \mathbb{E}(|\operatorname{Hom}(q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H), C_q)|) = +\infty,$$

where K runs over fields in $\mathcal{S}$ for the invariant d, and $\hat{K}$ is the Galois closure of K, and C_q is the cyclic group of order q.

Proof. According to similar idea, $\mathbf{1}_{\mathrm{rk}_q=r}(A)$ to be the indicator that tells us if $\mathrm{rk}_q\, A = r$. By definition of the C_q-moment and the probability of the q-rank, for all $r \geq 0$, we have

$$\begin{aligned}
\mathbb{E}(|\operatorname{Hom}(q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H), C_q)|) &= \lim_{x\to\infty} \frac{N(\mathcal{S}, d; |\operatorname{Hom}(q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H), C_q)|; x)}{N(\mathcal{S}, d; x)} \\
&= \lim_{x\to\infty} \sum_{n=0}^{\infty} q^n \frac{N(\mathcal{S}, d; \mathbf{1}_{\mathrm{rk}_q=n} \circ (q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H)); x)}{N(\mathcal{S}, d; x)} \\
&\geq q^r \lim_{x\to\infty} \left(1 - \frac{N\left(\mathcal{S}, d; \mathbf{1}_{\mathrm{rk}_q\leq r-1} \circ (q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H))\right); x)}{N(\mathcal{S}, d; x)}\right) \\
&= q^r \cdot (1 - \mathbb{P}(\mathrm{rk}_q\, q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H) < r)) \geq q^r(1-c).
\end{aligned}$$

For any number $N > 0$, by taking a large enough $r > 0$, we have

$$\mathbb{E}(|\operatorname{Hom}(q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H), C_q)|) > N,$$

hence $\mathbb{E}(|\operatorname{Hom}(q^{l-1}\,\mathrm{Cl}(K/\hat{K}^H), C_q)|) = +\infty$. □

In short, we can just say that whenever the Conjecture 1.1.11 holds, then we have zero-probability and infinite moment, i.e., Theorem 1.1.12 is true. We will show in later sections that for abelian extensions, the Conjecture 1.1.11(1) holds. Here we discuss an example where the fields are not ordered by product of ramified primes.

Example 3.2.6 (Ordering by discriminant)**.** Let's consider non-Galois cubic extensions the set $\mathcal{S} := \mathcal{S}(S_3, \{1, (23)\})$ of $K/\mathbb{Q}$. In this case we want to show that the analogous statement of Conjecture 1.1.11(1) is *false* for $(\mathcal{S}; \{(123), (132)\})$ when the fields ordered by *discriminant*, despite the fact that 3 is non-random for S_3.

According to the work of Bhargava, Shankar, and Tsimerman [6, Theorem 8], we know that counting nowhere totally ramified degree 3 cubic fields will give the main term cx where c is a nonzero constant, which is the same main term as counting all cubic fields by discriminant. This already contradicts the analagous statement of Conjecture 1.1.11(2) when ordering fields by discriminant, the weaker one. So we can conclude that when cubic fields ordered by discriminant with non-random prime 3 is a counter-example for the analogous result of the conjecture. On the other hand, Proposition 3.4.8 shows that, under some hypothesis, Conjecture 1.1.11(2) holds for $(\mathcal{S}; \{(123), (132)\})$. This shows that the conjecture, and possibly the statistical behaviours of non-random primes that show qualitatively difference from good primes, are dependent on the choice of the ordering of the number fields.

3.3 Dirichlet series and Tauberian Theorem

For the purpose of proving results on counting fields in different situations, we discuss the analytic properties of some Dirichlet series. Let's first present a Tauberian Theorem that is used in the paper repeatedly.

Theorem 3.3.1 (Delange-Ikehara)**.** *[45, Appendix II Theorem I] Assume that the coefficients of the Dirichlet series are real and non-negative, and that it converges in the half-plane $\sigma > 1$, defining a regular function $f(s)$. Assume, moreover, that in the same half-plane one can write*

$$f(s) = \sum_{j=0}^{q} g_j(s) \log^{b_j}\left(\frac{1}{s-1}\right)(s-1)^{-\alpha_j} + g(s),$$

where functions $g, g_0, \ldots, g_q$ are regular in the closed half plane $\sigma \geq 1$, the b_j-s are non-negative rational integers, α_0 is a positive real number, $\alpha_1, \ldots, \alpha_q$ are complex numbers with $\Re\alpha_j < \alpha_0$, and $g_0(1) \neq 0$.

Then for the summatory function $S(x) = \sum_{n<x} a_n$ we have, for x tending infinity,

$$S(x) = \left(\frac{g_0(1)}{\Gamma(\alpha_0)} + o(1)\right) x \log^{\alpha_0 - 1} x (\log\log x)^{b_0}.$$

If f satisfies the same assumptions, except that $\alpha_0 = 0$ and $b_0 \geq 1$, then

$$S(x) = (b_0 g_0(1) + o(1)) x \frac{(\log\log x)^{b_0 - 1}}{\log x}.$$

Remark. According to the statement of Conjecture 1.1.11 and our discussion in § 3.2, for results on asymptotics, we are focused on the comparison of the main terms. The complex analysis metheds in number theory (like Tauberian Theorms) can give us the information of the error term. See, for example, [58, Part II] for more details.

Let's introduce a notion that will be used later. It is inspired by counting fields problems.

Definition 3.3.2. For a pair (q, a) of relatively prime numbers, let

$$\mathcal{P}(q, a; x) := \{p \text{ is a prime natural number} | \, p \leq x \text{ and } p \equiv a \bmod q\}.$$

In particular, let $\mathcal{P}(q, a)$ be the set of all prime natural numbers such that $p \equiv a \bmod q$. Then define

$$\zeta\big(q, a; s\big) = \prod_{p \in \mathcal{P}(q,a)} (1 - p^{-s})^{-1}$$

when $\Re(s) > 1$.

A suitable power of the function $\zeta(q, a; s)$ admits a meromorphic extension to the closed half plane $\sigma \geq 1$. To prove this, we need a lemma.

Lemma 3.3.3. *There exists a holomorphic function $g_1(s)$ in the closed half plane such that*

$$\sum_p p^{-s} = \log\left(\frac{1}{s-1}\right) + g_1(s).$$

Proof. Let $\zeta(s)$ be the Riemann zeta function. Since it admits a meromorphic extension to the whole of the complex plane with a simple pole at $s = 1$, we can write it as

$$\zeta(s) = \frac{f_0(s)}{s-1},$$

with $f_0(s)$ holomorphic function on the complex plane with $f_0(1) = 1$. By taking the logarithm of the Euler product $\prod_p (1-p^{-s})^{-1}$ in $\sigma > 1$, we see that

$$\log \zeta(s) = \sum_p p^{-s} + \sum_{n\geq 2} \frac{1}{n} \sum_p p^{-ns}.$$

This shows that $\sum_p p^{-s}$ is a holomorphic function in $\sigma > 1$, hence in the open half plane $\sigma > 1$ there exists $g_1(s)$ such that

$$\sum_p p^{-s} = \log\left(\frac{1}{s-1}\right) + g_1(s),$$

where

$$e^{g_1(s)} = f_0(s) \cdot \exp\left(\sum_n \frac{1}{n} \sum_p p^{-ns}\right) =: f(s)$$

for all $\sigma > 1$. Since $\zeta(s) \neq 0$ for all $\sigma \geq 1$. We then see that $f_0(s) \neq 0$ for all $\sigma \geq 1$. Therefore we can extend $g_1(s)$ to the closed half plane $\sigma \geq 1$. To be precise, for each point s on the line $\sigma = 1$, since $f(s) \neq 0$, there exists some open neighbourhood U of s, such that $f_0(U)$ is away from 0 so that $\log \circ f$ is well-defined and equal to g_1 on $U \cap \{\sigma > 1\}$. Since the presheaf of holomorphic functions on $\mathbb{C}$ forms a sheaf, we can glue the local analytic continuations together and obtain an analytic continuation for $g_1(s)$ on the closed half plane $\sigma \geq 1$. □

Lemma 3.3.4. *Let (q, a) be a pair of relatively prime numbers. The function $\zeta(q, a; s)^{\phi(q)}$ admits a meromorphic continuation to the half plane $\sigma > 1/2$ with a simple pole at $s = 1$. To be precise, there exists some holomorphic function $f_0(s)$ in the closed half plane $\sigma \geq 1$ such that*

$$\zeta(q, a; s)^{\phi(q)} = f_0(s) \frac{1}{s-1}.$$

In addition, $f_0(s)$ and $L(\chi, s)$ has no zero along the line $\sigma = 1$ for all Dirichlet characters χ.

Proof. Let $\mathcal{P} := \mathcal{P}(q,a)$ and $\langle \mathcal{P} \rangle$ denote the semi-subgroup of $\langle \mathbb{Z}_{>0}, \cdot \rangle$ generated by $\mathcal{P}$. Since

$$\sum_{\substack{n \le x \\ n \in \langle \mathcal{P} \rangle}} \frac{1}{|n^s|} \le \sum_{n \le x} \frac{1}{|n^s|},$$

we know that $\zeta(q,a;s)$ converges absolutely and uniformly in $\sigma > 1+\delta$ for any $\delta > 0$. Then for any $\sigma > 1$, we have

$$\log \zeta(q,a;s) = \sum_{p \in \mathcal{P}} p^{-s} + \frac{1}{2} \sum_{p \in \mathcal{P}} p^{-2s} + \cdots .$$

Similarly for any Dirichet character $\chi \bmod q$, we have

$$\log L(s,\chi) = \sum \frac{\chi(p)}{p^s} + \frac{1}{2} \sum \frac{\chi(p^2)}{p^{2s}} + \cdots .$$

Therefore

$$\log \zeta(q,a;s) = \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \log L(s,\chi) + g(s)$$

for all $\sigma > 1$, where $g(s)$ is given by

$$g(s) = \sum_{n=2}^{\infty} \frac{1}{n} \sum_{p \in \mathcal{P}} \left(p^{-ns} - \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \chi(p^n) p^{-ns} \right) = \sum_{n=2}^{\infty} \frac{1}{n} \sum_{p^n \not\equiv a \bmod q} p^{-ns}$$

Note that $g(s)$ is absolutely convergent in $\sigma > 1/2$. By taking the exponent, we have

$$\zeta(q,a;s)^{\phi(q)} = \prod_{\chi} L(s,\chi)^{\overline{\chi}(a)} \cdot h(s)$$

where $h(s)$ is an analytic non-vanishing function in $\sigma > 1/2$. Therefore the pole behaviour of $\zeta(q,a;s)$ is the same as $\prod_{\chi} L(s,\chi)^{\overline{\chi}(a)}$, hence the same as $L(s,\chi_0)$ where χ_0 is the principal Dirichlet character modulo q (see for example [44, pp. 4.8, 4.9]), which concludes the proof for the formula. For all $a \in (\mathbb{Z}/q)^*$, write

$$\zeta(q,a;s)^{\phi(q)} = \frac{f_a(s)}{s-1}$$

for some holomorphic function $f_a(s)$ in the closed half plane $\sigma \ge 1$, we then see that

$$\begin{aligned} \prod_{p \mid q} (1-p^{-s})^{\phi(q)} \zeta(s)^{\phi(q)} &= \prod_{a \in (\mathbb{Z}/q)^*} \zeta(q,a;s)^{\phi(q)} \\ &= \prod_{a \in (\mathbb{Z}/q)^*} \frac{f_a(s)}{s-1} \end{aligned}$$

This shows that each $f_a(s)$ has no zero along the line $\sigma = 1$. Then by

$$\frac{f_a(s)}{s-1} = \zeta(q,a;s)^{\phi(q)} = \prod_{\chi} L(\chi,s)^{\bar{\chi}(a)} \cdot h(s),$$

we see that each $L(\chi, s)$ has no zero along the line $\sigma = 1$. □

Based on the above lemma, we can study the asymptotics of counting primes that are a mod q. This result is given by the following.

Proposition 3.3.5. *For a given pair of coprime numbers (q, a), one has*

$$\sum_{p \in \mathcal{P}(q,a)} \phi(q) p^{-s} = \log\left(\frac{1}{s-1}\right) + g(s)$$

where $g_0(s)$ is a holomorphic function in the closed half plane $\sigma \geq 1$. Moreover, there exists holomorphic functions $f_1, \ldots, f_r$ in the closed half plane $\sigma \geq 1$ such that

$$\sum_{\substack{p_1 < \cdots < p_r \\ \in \mathcal{P}(q,a)}} \phi(q)^r (p_1 p_2 \cdots p_r)^{-s} = \log^r\left(\frac{1}{s-1}\right) + \sum_{i=1}^{r} f_i(s) \log^{r-i}\left(\frac{1}{s-1}\right).$$

Proof. According to Lemma 3.3.4, $L(\chi, s)$ has no zero along the line $\sigma = 1$. If $\chi \neq \chi_0$ is not the principal character, then one see that the formula

$$\log L(s,\chi) = \sum_{p} \frac{\chi(p)}{p^s} + \sum_{n \geq 2} \frac{1}{n} \sum_{p} \frac{\chi(p^n)}{p^{ns}}$$

first defines a holomorphic function in the open half plane $\sigma > 1$ and then extends to the closed half plane $\sigma \geq 1$, which serves as $\log L(\chi, s)$. Therefore by summing over all the Dirichlet characters modulo q, we obtain

$$\sum_{p \in \mathcal{P}(q,a)} \phi(q) p^{-s} = \sum_{p} p^{-s} + g_0(s)$$

where $g_0(s)$ is a holomorphic function in the closed half plane $\sigma \geq 1$. According to Lemma 3.3.3, we see that

$$\sum_{p \in \mathcal{P}(q,a)} \phi(q) p^{-s} = \log\left(\frac{1}{s-1}\right) + g_1(s) + g_0(s)$$

where $g_1(s)$ is a holomorphic function in the closed half plane $\sigma \geq 1$. By taking $g(s) := g_0(s) + g_1(s)$, we then obtain the required formula.

The formula for $\sum_{p_1\neq\cdots\neq p_r\in\mathcal{P}(q,a)}\phi(q)^r(p_1\cdots p_r)^{-s}$ can be obtained by induction on r. It is clear that the statement is true for $r=1$. Provided that the claim is true for $1,\dots,r$. Then by induction, one has

$$\begin{aligned}
&\sum_{\substack{p_1<\cdots<p_{r+1}\\ \in\mathcal{P}(q,a)}}\phi(q)^{r+1}(p_1\cdots p_{r+1})^{-s}\\
&=\sum_{l=1}^{r+1}(-1)^{l-1}\sum_{p\in\mathcal{P}(q,a)}\phi(q)^l p^{-ls}\sum_{\substack{p_1<\cdots<p_r\\ \in\mathcal{P}(q,a)}}\phi(q)^{r+1-l}(p_1\cdots p_{r+1-l})^{-s}\\
&=\log^{r+1}\left(\frac{1}{s-1}\right)+\cdots.
\end{aligned}$$

The coefficients of $\log^i(1/(s-1))$ are all holomorphic functions in the closed half plane $\sigma\geq 1$ by induction, for all $i=0,1,2,\dots,r+1$. And the proof is done by induction on r. □

A result that will be used in this paper, inspired by Hardy-Littlewood Tauberian Theorem (see for example [44, Theorem 5.7]), relates $\sum_{n<x}a_n$ and $\sum_{n<x}a_n/n$. Using the identity

$$\sum_{n=1}^{\infty}a_n n^{-s}=s\int_1^{\infty}A(x)x^{-s-1}\,\mathrm{d}\,x$$

for a Dirichlet series and summation by parts (see in particular [58, Theorem 0.3]), we can prove the following statement.

Lemma 3.3.6. *Let $\{a_n\}$ be a non-negative sequence.*

(i) If there exists a constant $\alpha>0$ and an integer $\beta\geq 0$ such that

$$\sum_{n<x}a_n=(\alpha+o(1))x\log^{\beta}x,$$

Then we have

$$\sum_{n<x}\frac{a_n}{n}=\left(\frac{\alpha}{\Gamma(\beta+2)+o(1)}\right)(\log x)^{\beta+1}.$$

(ii) If there exists some integers $\beta_1\geq -1,\beta_2>0$ such that

$$\sum_{n<x}a_n\ll x(\log x)^{\beta_1}(\log\log x)^{\beta_2},$$

then

$$\sum_{n<x}\frac{a_n}{n}\ll(\log x)^{\beta_1+1}(\log\log x)^{\beta_2'},$$

where $\beta_2'=\beta_2$ if $\beta_1>-1$, and $\beta_2'=\beta_2+1$ if $\beta_1=-1$.

The proof itself is left to the reader.

3.4 Semidirect product of abelian groups

In this section we consider the following set-up. Let $G := H \rtimes F$ where H, F are both finite abelian groups such that for each $h \in H$ and $g \in F$ we have

$$ghg^{-1} = h^{a(g,h)}.$$

For example, an abelian group $G = H \oplus F$. For another example, dihedral group $G = D_q$ where q is an odd prime. Our first goal in this section is focused counting fields with local specifications, i.e., give an estimate for $N(\mathcal{S}(G), P; (\Omega, r); x)$ where Ω is closed under invertible powering and conjugation. Then we can try to apply the counting fields results to different situations including abelian extensions ($G = H$). We make a notion at the beginning of this section for the convenience of our discussion.

Definition 3.4.1. If $g \in G$, then define γ_g to be its order.

Galois theory

First of all, we take a look at Class Field Theory. Let $K/\mathbb{Q}$ be an abelian F-extension. Let $\mathscr{J}_K$ be the idèle class group of K. Let $\mathscr{O}_v^*$ be the units of the complete local field K_v with v some place of K, and let $\mathscr{O}_K^*$ be the group of global units. For any F-module A, B, let $\mathrm{Hom}_F(A, B)$ be the group of F-morphisms from A to B. The following short exact sequences

$$\begin{aligned} 1 \to \mathscr{O}_K^* \to \prod_v \mathscr{O}_v^* \to \Big(\prod_v \mathscr{O}_v^*\Big)/\mathscr{O}_K^* \to 1 \\ 1 \to \Big(\prod_v \mathscr{O}_v^*\Big)/\mathscr{O}_K^* \xrightarrow{i} \mathscr{J}_K \to \mathrm{Cl}_K \to 1 \end{aligned}$$

where we denote the embedding $(\prod_v \mathscr{O}_v^*)/\mathscr{O}_K^* \to \mathscr{J}_K$ by i, induce long exact sequences respectively, i.e., for any F-module A, we have

$$\begin{aligned} &0 \to \mathrm{Hom}_F\Big((\prod_v \mathscr{O}_v^*)/\mathscr{O}_K^*, A\Big) \to \mathrm{Hom}_K(\prod_v \mathscr{O}_v^*, A) \to \mathrm{Hom}_F(\mathscr{O}_K^*, A) \\ &\to \mathrm{Ext}_F^1\Big((\prod_v \mathscr{O}_v^*)/\mathscr{O}_K^*, A\Big) \to \cdots \\ &0 \to \mathrm{Hom}_F(\mathrm{Cl}_K, A) \to \mathrm{Hom}_F(\mathscr{J}_K, A) \xrightarrow{i^*} \mathrm{Hom}_H\Big((\prod_v \mathscr{O}_v^*)/\mathscr{O}_K^*, A\Big) \\ &\to \mathrm{Ext}_F^1(\mathrm{Cl}_K, A) \to \cdots \end{aligned} \tag{3.4.1}$$

Remark. The first observation is that given a set of local morphisms $\{\rho_v \in \mathrm{Hom}_F(\mathscr{O}_v^*, A)\}_v$ that are trivial almost everywhere, their product $\rho := \prod_v \rho_v$ may not be extended to $\mathscr{J}_K$ because of global units $\mathscr{O}_K^*$ and $\mathrm{Ext}_F^1(\mathrm{Cl}_K, A)$. Second, if there is $\tilde{\rho} \in \mathrm{Hom}_F(\mathrm{Cl}_K, A) \to \mathrm{Hom}_F(\mathscr{J}_K, A)$ such that $\tilde{\rho}$ coincide with ρ_v on $\mathscr{O}_v^*$ for each v, then the number of the preimages of ρ in $\mathrm{Hom}_F(\mathscr{J}_K, A)$ is exactly $|\mathrm{Hom}_F(\mathrm{Cl}_K, A)|$.

Next, we give a description for the Galois action of F on the H-extensions. For a rational prime $p \nmid |G|$, let $s_p \in G$ be the image of Frobenius (up to conjugation) and let $t_p \in G$ be the generator of inertia (up to conjugation). Since $s_p t_p s_p^{-1} = t_p^p$, we have the following result.

Lemma 3.4.2. *Let $L/\mathbb{Q}$ be a Galois G-extension, and let p be a rational prime such that $p \nmid |G|$. Recall that for an element $g \in G$, its order is denoted by γ_g.*

(a) If s_p is not conjugate to any $g \in F$, then $\gamma_{t_p} | (p-1)$;

(b) else if s_p is conjugate to some $g \in F$, and $g t_p g^{-1} = t_p^{a(g,t_p)}$, then $\gamma_{t_p} | (p^{\gamma_g} - 1)$ and $p \equiv a(g, t_p) \bmod \gamma_{t_p}$.

Inspired by the Galois action, or the twisting of F on H, we make the following notion.

Definition 3.4.3. Fix a rational prime p. Let Ω be a subset of G closed under invertible powering and conjugation, and let $H_p(\Omega)$ be a subset of Ω constructed as follows.

(i) If $h \in \Omega \backslash F$, and $\gamma_h | (p-1)$, then $h \in H_p(\Omega)$.

(ii) If $h \in \Omega \backslash F$, and $p \equiv a(g,h) \bmod \gamma_h$ for some $g \in F$, then $h \in H_p(\Omega)$.

Let $h_p(\Omega) := |H_p(\Omega)|$ denote its order.

Counting fields

We first make a notion inspired by Wood [64, Theorem 3.1]. Recall that for $g \in G$, we denote its order by γ_g.

Definition 3.4.4. Let Ω be a subset of $G = H \rtimes F$ closed under invertible powering and conjugation. Define

$$\beta(F, \Omega) := \sum_{\mathrm{id} \neq g \in \Omega} c(g) [\mathbb{Q}(\zeta_{\gamma_g}) : \mathbb{Q}]^{-1}$$

where $c(g)$ is the number of elements conjugate to g.

Note that the notion $\beta(F, \Omega)$ is always an integer. In this section, we show the following two theorems on counting fields.

Theorem 3.4.5. *Recall that $G = H \rtimes F$ such that $ghg^{-1} = h^{a(g,h)}$ for all $g \in F$ and $h \in H$.*

(i) Let $\Omega_1 \subseteq H \backslash \{\mathrm{id}\}$ be a subset that is closed under invertible powering and conjugation. If there exists some integer β_1 such that

$$N(\mathcal{S}(F), P; |\operatorname{Hom}(\mathrm{Cl}(K), H)|^2; x) \ll x (\log x)^{\beta_1}$$

then

$$N(\mathcal{S}(G), P; (\Omega_1, r); x) \ll \begin{cases} x (\log x)^{\beta(F, H \backslash \Omega_1) + \frac{1}{2}\beta_1} (\log \log x)^{\frac{1}{2}(r+1)} & \text{if } \Omega_1 \neq \emptyset \\ x (\log x)^{\beta(F,H) + \frac{1}{2}\beta_1} & \text{Otherwise.} \end{cases}$$

(ii) Let $\Omega_2 \subseteq G\backslash\{\mathrm{id}\}$ be a subset that is closed under invertible powering and conjugation such that $\Omega_2 \cap F \neq \emptyset$. Let $r = 0, 1, 2, \ldots$ be an integer. If there exists some constant β_2, β_3 such that

$$N(\mathcal{S}(F), P; |\operatorname{Hom}(\mathrm{Cl}(K), H)|^2 \cdot \mathbf{1}_{(F\cap\Omega_2, r)}; x) \ll x(\log x)^{\beta_2}(\log\log x)^{\beta_3},$$

then

$$N(\mathcal{S}(G), P; (\Omega_2, r); x) \ll \begin{cases} x(\log x)^{\beta(F,H\backslash\Omega_2)+\frac{1}{2}\beta_2}(\log\log x)^{\frac{1}{2}(r+\beta_3)+1} & \text{if } \Omega_2 \cap H = \emptyset; \\ x(\log x)^{\beta(F,H\backslash\Omega_2)+\frac{1}{2}\beta_2}(\log\log x)^{\frac{1}{2}\beta_3+1} & \text{otherwise.} \end{cases}$$

Theorem 3.4.6. *Assume that G is an abelian group. If $\mathrm{id} \notin \Omega \subseteq G$ is closed under invertible powering, then for large enough r, we have*

$$\begin{aligned} N(\mathcal{S}(G), P; (\Omega, r); x) &\asymp x(\log x)^{\beta(G\backslash\Omega)-1}(\log\log x)^r && \text{if } \Omega \neq G\backslash\,\mathrm{id} \\ N(\mathcal{S}(G), P; (\Omega, r); x) &\asymp \frac{x}{\log x}(\log\log x)^{r+1} && \text{if } \Omega = G\backslash\,\mathrm{id} \end{aligned}$$

where $f(x) \asymp g(x)$ means that $g(x) \ll f(x) \ll g(x)$ as $x \to \infty$, and

$$\beta(G\backslash\Omega) := \sum_{g\in G\backslash\Omega} [\mathbb{Q}(\zeta_{\gamma_g}) : \mathbb{Q}]^{-1}.$$

Let's first present a lemma, which is the key of the above results.

Lemma 3.4.7. *Let K be a fixed F-field. Recall that $G = H \rtimes F$ and that $ghg^{-1} = h^{a(g,h)}$ for all $g \in F$ and $h \in H$. Let $1 \notin \Omega$ be a subset of H closed under invertible powering and conjugation.*

(i) Let

$$\sum_n b_n(\Omega, r)n^{-s} := \prod_{p\nmid|G|}(1 + h_p(H\backslash\Omega)p^{-s})\left(1 + \sum_{p_1<p_2<\cdots<p_r}\prod_{i=1}^{r} h_{p_i}(\Omega)p_i^{-s}\right).$$

There exists some analytic functions $g_0(s), \ldots, g_r(s), g(s)$ in the closed half plane $\Re(s) \geq 1$ such that

$$\sum_n b_n(\Omega, r)n^{-s} = \sum_{i=0}^{r} g_i(s)(s-1)^{\beta(F,H\backslash\Omega)}\log^{r-i}\left(\frac{1}{s-1}\right) + g(s).$$

(ii) Let $h(p) := |\operatorname{Hom}(\mathbb{Z}^*_{p^{|F|}}, G)|$, and let

$$\begin{aligned} \sum_n b_n(K, (\Omega, r))n^{-s} :&= |\operatorname{Hom}(\mathrm{Cl}(K), H)| \prod_{p|\gcd(P(K),|G|)} h(p)p^{-s} \prod_{p:v_p(P(K)/|G|)>0} p^{-s} \\ &\prod_{p:v_p(|G|/P(K))>0} (1 + h(p)p^{-s}) \sum_n b_n(\Omega, r)n^{-s}. \end{aligned}$$

Then, we have

$$\sum_n \sum_{\substack{L\in\mathcal{S}(G)\\ K\subseteq L,\, P(L)=n}} \mathbf{1}_{(\Omega,r)}(L)n^{-s} \le \sum_n b_n(K,(\Omega,r))n^{-s}.$$

Proof. First we note that Ω is not required to be a proper subset of H, i.e., Ω may be empty, hence the result can be applied to the case when we want to estimate the counting of all extensions L/K such that $L \in \mathcal{S}(G)$. And $\Omega = \emptyset$ simply says that $\mathbf{1}_{(\Omega,r)}(L) = 1$ for all L/k and $L \in \mathcal{S}(G)$, and that $b_p(\Omega) = 0$ for all p, and that $\beta(F,\Omega) = 0$.

Second, we give the definition of product of ramified primes for a homomorphism $\rho \in \mathrm{Hom}_F(\prod_v \mathscr{O}_v^*, H)$ where v runs over all places of K. For each p, let $\rho_p \in \mathrm{Hom}(\prod_{v|p} \mathscr{O}_v^*, H)$ be the corresponding local morphism. We define $P(\rho_p) = p$ if ρ_p is nontrivial, and $P(\rho_p) = 1$ otherwise. Then define $P(\rho) := \prod_p P(\rho_p)$. Let L/K be an H-extension such that $L \in \mathcal{S}$. There exists an Artin reciprocity map $\tilde{\rho} \in \mathrm{Hom}(\mathcal{J}_K, H)$ corresponding to L, i.e., L is the class field of $\tilde{\rho}$. If $\tilde{\rho}$ agrees with ρ on $\prod_v \mathscr{O}_v^*$, then we have

$$P(\tilde{\rho}) = P(\rho),$$

i.e., we can treat in this case $P(L/K) := P(\tilde{\rho})$.

Third, according to Class Field Theory (3.4.1), we have

$$N(\mathrm{Hom}_F(\mathcal{J}_K, H), P; \mathbf{1}_{(\Omega_1,r)}; x) \le |\mathrm{Hom}(\mathrm{Cl}_K, H)| \cdot N(\mathrm{Hom}_F(\prod_v \mathscr{O}_v^*, H), P; \mathbf{1}_{(\Omega,r)}; x).$$

Hence it suffices to estimate the number of the morphisms $\rho \in \mathrm{Hom}_F(\prod_v \mathscr{O}_v^*, H)$. Note that a morphism ρ can be decomposed into local morphisms $\rho = \prod_p \rho_p$, where

$$\rho_p \in \mathrm{Hom}_F(\prod_{v|p} \mathscr{O}_v^*, H),$$

and ρ_p is trivial for all but finitely many prime p. For each ρ_p, the Galois action of F says that it is enough to consider $\rho_v : \mathscr{O}_v^* \to H$ for some $v|p$. If $p \nmid |G|$, then the local morphism ρ_v always factors through the group of roots of unity $\mu = \langle\zeta\rangle$ of $\mathscr{O}_v^*$, hence is totally determined by the image of the generator ζ. According to Lemma 3.4.2, for $h \in H$, if $\rho_v(\zeta) = h$, then $h \in H_p(H)$. Similar results hold when we replace H by $\Omega \cap H$ and $H\backslash\Omega$. So, for each square-free n, we know that

$$b_n(K,(\Omega,r)) \ge |\{\rho : P(\rho) = n \text{ and for } i = 1,2,\ldots,r, \exists p_i (p_i | n \text{ and } \rho_{p_i}(\zeta_i) \in \Omega)\}|,$$

where $\zeta_i \in \mathscr{O}_{v_i}^*$ is a generator of the group of roots of unity and $v_i|p_i$ is a place of K lying above p_i. This prove that

$$\sum_n \sum_{\substack{L\in\mathcal{S}(G)\\ k\subseteq L,\, P(L)=n}} \mathbf{1}_{(\Omega,r)}(L)n^{-s} \le \sum_n b_n(K,(\Omega,r))n^{-s}.$$

And we are done for the proof of (ii).

Fourth, we want to give the correct analytic description and continuation of the Dirichlet series of $\sum_n b_n(\Omega, r)n^{-s}$. The definition of $H_p(H\backslash\Omega)$ means that we can classify $H_p(H\backslash\Omega)$ based on $p \equiv a \bmod |F|$. Recall that for an element $h \in H$ we denote its order by γ_h. Let f be the annihilator of F. We consider the following Euler product

$$\sum_n b'_n(\Omega, r)n^{-s} := \prod_{\mathrm{id}\neq h\notin\Omega} \prod_{a(g,h):g\in F} \zeta(\gamma_h, a(g,h); s) \prod_{\substack{p_1<\cdots<p_r \\ \in\bigcup_{h\in\Omega}\mathcal{P}(\gamma_h,1)}} \phi(f)^r p_1^{-s}\cdots p_r^{-s},$$

where $\zeta(m, n; s) = \prod_{p\in\mathcal{P}(m,n)}(1 - p^{-s})^{-s}$, and $\mathcal{P}(m, n)$ is the set of all primes $p \equiv n \bmod m$ for a pair of coprime number (m, n) (see also Definition 3.3.2). We can compute the order of the pole by the following expression:

$$\sum_{\mathrm{id}\neq h\in H\backslash\Omega} c(h)[\mathbb{Q}(\zeta_{\gamma_h}) : \mathbb{Q}]^{-1} = \beta(F, H\backslash\Omega),$$

where $c(h)$ denote the number of elements conjugate to h. So, this shows that

$$\sum_n b'_n(\Omega, r)n^{-s} = g_0(s)(s-1)^{\beta(F,H\backslash\Omega)} \log^r\left(\frac{1}{s-1}\right) + \cdots,$$

whose analytic continuation is given by Lemma 3.3.4 and Proposition 3.3.5. Then the comparison between $\sum_n b_n(\Omega, r)n^{-s}$ and $\sum_n b'_n(\Omega, r)n^{-s}$ finishes the proof. □

Finally let's give the proof of the theorems.

Proof of Theorem 3.4.5. Let

$$\sum_n A_n(\Omega_i, r)n^{-s} := \sum_n \sum_{\substack{L\in\mathcal{S} \\ P(L)=n}} \mathbf{1}_{(\Omega_i,r)}(L)n^{-s}$$

where $i = 1, 2$, and q is a rational prime. Since the proof of each case is similar, we present only one of them, and the rest is left to the reader.

Let $\Omega_1 \subseteq H\backslash\{1\}$ be a non-empty subset closed under invertible powering and conjugation. Consider first the Dirichlet series

$$\sum_n a_n(K; (\Omega_1, r)) := \sum_n \sum_{\substack{L\in\mathcal{S}_1 \\ P(L)=n}} \mathbf{1}_{(\Omega_1,r)}(L)n^{-s}.$$

According to Lemma 3.4.7, we know that

$$\sum_n a_n(K; (\Omega_1, r)) \leq \sum_n b_n(K; (\Omega_1, r))n^{-s},$$

i.e., $a_n(K;(\Omega_1,r)) \le b_n(K;(\Omega_1,r))$ for each n. Then by taking into account all quadratic number fields, we have

$$\begin{aligned}\sum_n A_n(\Omega_1,r)n^{-s} &= \sum_{K\in\mathcal{S}(F)}\sum_n a_n(K;(\Omega_1,r))n^{-s}\\ &\le \sum_{K\in\mathcal{S}(F)}\sum_n b_n(K;(\Omega_1,r))n^{-s} =: \sum_n B_n(\Omega_1,r)n^{-s}\end{aligned}$$

Then, by Cauchy-Schwartz Inequality, we have

$$\begin{aligned}&\sum_{n<x} A_n(\Omega_1,r) \le \sum_{n<x} B_n(\Omega_1,r)\\ &\le h^{\omega(|G|)}\left(\sum_{P(K)<n} |\operatorname{Hom}(\mathrm{Cl}_K,H)|^2\frac{x}{P(K)}\right)^{1/2}\left(\sum_{n<x}(b_n(\Omega_1,r))^2\right)^{1/2}\end{aligned}$$

where $h := \max_p |\operatorname{Hom}(\mathbb{Z}^*_{p^{|F|}},G)|$. By our assumption we know that

$$\sum_{P(K)<n} |\operatorname{Hom}(\mathrm{Cl}_K,H)|^2\frac{x}{P(K)} \ll x(\log x)^{\beta_1+1}.$$

Since $\sum_{n<x} b_n(\Omega_1,r))^2$ is the coefficient of the Euler product

$$\prod_p(1+h_p(H\backslash\Omega_1)^2p^{-s})\sum_{d=p_1\cdots p_r}\prod_{i=1}^r h_{p_i}(\Omega_1)^2p_i^{-s},$$

we can apply Lemma 3.4.7 and Theorem 3.3.1 here, and get

$$\sum_{n<x}(b_n(\Omega_1,r))^2 \ll x(\log x)^{2\beta(F,H\backslash\Omega_1)-1}(\log\log x)^{r+1}.$$

Combining all components of the inequality, and we are done for (i). □

Then let's prove Theorem 3.4.6, the Conjecture 1.1.11(1) for abelian extensions.

Proof of Theorem 3.4.6. Let $\beta := \beta(G\backslash\Omega)$, and δ be the indicator of -1, i.e., $\delta(-1)=1$ and $\delta(x)=0$ otherwise. Let

$$\sum_n a_n(\Omega,r)n^{-s} := \sum_n \sum_{\substack{K\in\mathcal{S}(G)\\P(K)=n}} \mathbf{1}_{(\Omega,r)}(K)n^{-s}.$$

By setting $F=\{\mathrm{id}\}$ and $G=H$, we see that Lemma 3.4.7 already gives an upper bound for counting fields with local specifications (Ω,r). To be precise, we have

$$\sum_n a_n(\Omega,r)n^{-s} \le \sum_n b_n(\mathbb{Q};\Omega,r)n^{-s},$$

where the Dirichlet series $\sum_n b_n(\mathbb{Q};\Omega,r)n^{-s}$ is given in the statement of Lemma 3.4.7. Then the analytic continuation of $\sum_n b_n(\mathbb{Q};\Omega,r)n^{-s}$, shown as in Lemma 3.4.7, together with Tauberian Theorem 3.3.1 gives the asymptotics

$$N(\mathcal{S}(G),P;(\Omega,r);x) \ll x(\log x)^{\beta-1}(\log\log x)^{r+\delta(\beta)}.$$

On the other hand, since $G=H$ is abelian, we apply Class Field Theory here, and consider the Dirichlet series

$$\sum_n c_n(\Omega,r)n^{-s} := \prod_{p\nmid|G|}(1+h_p(G\backslash\Omega)p^{-s}) \sum_{p_1<p_2<\cdots<p_r} \prod_{i=1}^{r} h_{p_i}(\Omega)p_i^{-s}.$$

Since $F=\{\mathrm{id}\}$ in this case, the computation of $h_p(\Omega)$ gives

$$h_p(\Omega)=\{h\in\Omega | h\neq \mathrm{id} \text{ and } p\equiv 1 \bmod \gamma_y\}.$$

Therefore, $\sum_n c_n(\Omega,r)n^{-s} \leq \sum_n a_n(\Omega,r)n^{-s}$, and the analytic continuation of $\sum_n c_n(\Omega,r)n^{-s}$ can be obtained by comparing with

$$\sum_n c_n'(\Omega,r)n^{-s} := \prod_{g\in G\backslash\{\mathrm{id}\}\cup\Omega} \zeta(\gamma_g,1;s) \sum_{\substack{p_1<\cdots<p_r\\ p_i\in\bigcup_g \mathcal{P}(\gamma_g,1)}} p_1^{-s}\cdots p_r^{-s},$$

which is also of the form $f(s)(s-1)^{\beta}(\log\frac{1}{s-1})^r+\cdots$. So, by Tauberian Theorem 3.3.1, we know that

$$N(\mathcal{S}(G),P;(\Omega,r);x) \gg x(\log x)^{\beta-1}(\log\log x)^{r+\delta(\beta)}.$$

And we are done for the proof. □

Applications

Let's first use the following result to explain why the above discussions are useful for dihedral extensions.

Proposition 3.4.8. *Let q be an odd prime, and let $\Omega := \Omega(D_q,q)$. If the Cohen-Lenstra Heuristics hold for quadratic number fields, and*

$$N(\mathcal{S}(D_q),P;x) \gg x\log x,$$

then, we have

$$N(\mathcal{S}(D_q),P;(\Omega,r);x) = o(N(\mathcal{S}(D_q),P;x))$$

for all $r=1,2,\ldots$. Also, for all $r=0,1,2,\ldots$, we have

$$\mathbb{P}(\mathrm{rk}_q\,\mathrm{Cl}_K\leq r)=0 \quad \textit{and} \quad \mathbb{E}(|\,\mathrm{Hom}(\mathrm{Cl}_K,C_q)|)=+\infty,$$

where K runs over all fields in $\mathcal{S}$ for the product of ramified primes in $K/\mathbb{Q}$.

Proof. In this case, if we write $D_q = C_q \rtimes C_2$, then $\Omega = C_q \backslash \{\mathrm{id}\}$. Therefore, $\beta(C_2, C_q\backslash\Omega) = 0$, and the rest follows from Theorem 3.4.5, Theorem 3.2.4 and Theorem 3.2.5. □

Remark. The statement itself is exactly Conjecture 1.1.11(2) for D_q-extensions. But we need two hypothesis: the Cohen-Lenstra Heuristics for quadratic number fields and an estimate for counting D_q-fields.

Then let's show Theorem 1.1.13, the result of relative class groups for abelian extensions, as promised in § 1.1.

Theorem 3.4.9. *Let G be a finite abelian group with a subgroup H, and let $\mathcal{S} := \mathcal{S}(G)$. If q is a prime number such that $q^l \| |G/H|$ where $l \geq 1$, then q is a non-random prime for the quotient G/H. In addition, for all $r = 0, 1, 2, \ldots$, we have*

$$\mathbb{P}(\mathrm{rk}_q\, q^{l-1}\,\mathrm{Cl}(K/K^H) \leq r) = 0 \quad \textit{and} \quad \mathbb{E}(|\,\mathrm{Hom}(q^{l-1}\,\mathrm{Cl}(K/K^H), C_q)|) = +\infty,$$

where K runs over all fields in $\mathcal{S}$ for the product of ramified primes in $K/\mathbb{Q}$.

Proof. Since $q^l || |G|$, the set $\Omega := \bigcup_{i=l}^{\infty} \Omega(G, q^i)$ is nontrivial, where we view the abelian group G as a transitive permutation group. This shows that q is a non-random prime for G. In particular, Theorem 3.1.15 shows that

$$\mathrm{rk}_q\, q^{l-1}\,\mathrm{Cl}(K/K^H) \geq \#\{p \nmid |G| : I(p) \cap \Omega \neq \emptyset\} - 2(|G| - 1),$$

where $I(p)$ means the inertia subgroup of p. The set Ω is closed under invertible powering (and conjugation), hence Theorem 3.4.6, Theorem 3.2.4 and Theorem 3.2.5 show that the statements of zero-probability and infinite moment are true. □

3.5 D_4 extensions

In this section, let $D_4 = \langle \sigma, \tau | \sigma^4 = 1 = \tau^2, \tau^{-1}\sigma\tau = \sigma^3 \rangle$ be the dihedral group of order 8. Define $\mathcal{S} := \mathcal{S}(D_4, \langle\tau\rangle)$, i.e., we are mainly focused on the quartic extensions whose Galois closure are D_4-fields, According to the Definition 1.1.8 of non-random primes, we also view the group D_4 as a permutation group $D_4 \hookrightarrow S_4$ via the Galois action of D_4 on the embeddings $K \to \mathbb{C}$ where $L \in \mathcal{S}$. The prime 2 is the only non-random prime for the permutation group D_4 by checking all elements in the form of cycles.

The distribution of $\mathrm{Cl}_L[2^\infty]$ when ordered by conductor

We first introduce the definition of the *conductor* for a quadratic extension of a quadratic number field, which will be used here as the invariant of the number fields.

Definition 3.5.1 (Conductor)**.** If K is a quadratic field and L is a quadratic extension of K, define the *conductor* of the pair (L, K) as

$$C(L, K) := \frac{\mathrm{disc}(L)}{\mathrm{disc}(K)}.$$

If L is a D_4-field and K denotes its (unique) quadratic subfield, then $C(L,K) = C(L)$ (the conductor of L).

Note that this conductor given by the above formula agrees with the Artin conductor for the irreducible 2-dimensional representation of D_4, if the quartic field has D_4-Galois closure. See [1, §2.3] for details. We here follow this definition for the convenience of both computation and generalization to other quartic fields. Recall that $\mathcal{S} = \mathcal{S}(D_4, \langle\tau\rangle) = \{(L,\psi)\}$. Note that L admits a unique quadratic subfield K. Let $q = 2$, which is the only non-random prime for $(D_4, \langle\tau\rangle)$. We want to study the statistical behaviour of $\mathrm{Cl}_L[2^\infty]$ where $L \in \mathcal{S}$ for the conductor. Let's first prove a lemma similar to [1, Lemma 5.1].

Lemma 3.5.2. *For any $0 < \epsilon < \frac{1}{2}$, we have*

$$\sum_{\substack{0<D<X\\ D \text{ squarefree}}} \frac{2^{\omega(D)}}{D} \cdot \left(\sum_{m=1}^{\infty} \sum_{\substack{n=1\\ mn\neq\square}}^{D^{\frac{1}{2}+\epsilon}} \frac{\mu(m)}{m^2 n} \left(\frac{D}{mn}\right) \right) = O_\epsilon(X),$$

where $\left(\frac{\cdot}{\cdot}\right)$ means Legendre symbol here.

Proof. We follow the idea of [1, Lemma 5.1] to prove it. First of all, interchanging the order of the sum gives

$$\sum_{\substack{0<D<X\\ D \text{ squarefree}}} \frac{2^{\omega(D)}}{D} \left(\sum_{m=1}^{\infty} \sum_{\substack{n=1\\ mn\neq\square}}^{D^{\frac{1}{2}+\epsilon}} \frac{\mu(m)}{m^2 n} \left(\frac{D}{mn}\right) \right) = \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{\substack{n<X^{\frac{1}{2}+\epsilon}\\ mn\neq\square}} \frac{1}{n} \sum_{\substack{n^{\frac{2}{1+2\epsilon}}<D<X\\ D \text{ squarefree}}} \frac{2^{\omega(D)}}{D} \left(\frac{D}{mn}\right). \tag{3.5.1}$$

Let's focus on the n-sum and D-sum. We apply a squarefree seive to complete the D-sum. In particular, we can rewrite (3.5.1) as

$$\sum_{\substack{n<X^{\frac{1}{2}+\epsilon}\\ mn\neq\square}} \frac{1}{n} \Bigg(\sum_{\alpha<n^{\frac{1}{1+2\epsilon}}} \frac{\mu(\alpha)}{\alpha^2} \sum_{n^{\frac{2}{1+2\epsilon}}\leq\alpha^2 d<X} \frac{\tau(d)}{d} \left(\frac{\alpha^2 d}{mn}\right) + \sum_{n^{\frac{1}{1+2\epsilon}}<\alpha<X^{\frac{1}{2}}} \frac{\mu(\alpha)}{\alpha^2} \sum_{n^{\frac{2}{1+2\epsilon}}\leq\alpha^2 d<X} \frac{\tau(d)}{d} \left(\frac{\alpha^2 d}{mn}\right) \Bigg),$$

where $\tau(d)$ is the number of positive divisors of d. For squarefree D, the notion $\tau(D) = 2^{\omega(D)}$. Note that for any nontrivial Dirichlet character χ and its associated series $L(s,\chi) = \sum_n \chi(n) n^{-s}$, we know that $L(s,\chi)$ is a holomorphic function in the closed half plane $\Re(s) \geq 1$. In particular $L(1,\chi)$ is a constant that is bounded by $\max_N |\sum_{n=1}^{N} \chi(n)|$. We may therefore estimate the sum by Pólya-Vinogradov inequality. In particular, (3.5.1) is bounded

by

$$\begin{aligned}
&\ll \sum_{\substack{n<X^{\frac{1}{2}+\epsilon}\\ mn\neq\square}} \frac{1}{n}\Bigg(\sum_{\alpha<n^{\frac{1}{1+2\epsilon}}} \frac{1}{\alpha^2} \left| \sum_{\alpha^{-2}n^{\frac{2}{1+2\epsilon}}\leq d<\alpha^{-2}X} \frac{\tau(d)}{d}\left(\frac{\alpha^2 d}{mn}\right)\right| \\
&+ \sum_{n^{\frac{1}{1+2\epsilon}}<\alpha<X^{\frac{1}{2}}} \frac{1}{\alpha^2}\left|\sum_{d<\alpha^{-2}X}\frac{\tau(d)}{d}\left(\frac{\alpha^2 d}{mn}\right)\right|\Bigg) \\
&\ll \sum_{\substack{n<X^{\frac{1}{2}+\epsilon}\\ mn\neq\square}} \frac{m(\log n)^2}{n^{\frac{1}{1+2\epsilon}}} \\
&\ll mX^{\frac{1}{2}+\epsilon}(\log X)^2
\end{aligned}$$

The lemma then follows from the m-sum, i.e.,

$$X^{\frac{1}{2}+\epsilon}(\log X)^2\sum_{m=1}^{\infty} m^{-1} = o(X).$$

□

We define

$$N(\mathcal{S}, C; f; x, y) := \sum_{n<x} \sum_{\substack{L\in\mathcal{S}\\ C(L)=n, \mathrm{Disc}(K)<y}} f(L),$$

where f is some function defined on $\mathcal{S}$. In other words we put some restrictions on the discriminant of $K \subseteq L$ by this notion.

Theorem 3.5.3. *Recall that $\mathcal{S} = \mathcal{S}(D_4, \{1, \tau\})$, and for each $L \in \mathcal{S}$, let K be its unique quadratic subfield. We have*

$$\mathbb{E}_C(|\operatorname{Hom}(\mathrm{Cl}_L, C_2)|) = +\infty$$

where L runs over all fields in $\mathcal{S}$ for the conductor C.

Proof. First of all, by Theorem 3.1.11, it suffices to prove that

$$\mathbb{E}_C(f) = +\infty$$

where $f(L) = 2^{\omega(\mathrm{Disc}(K))}$ for each $L \in \mathcal{S}$, because $|\operatorname{Hom}(\mathrm{Cl}_L, C_2)| \geq 2^{-6}\cdot f(L)$. Second, [1, Lemma 4.5] gives the smooth count result, hence we are reduced to prove that

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ \mathrm{Disc}(K)<y}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})}\frac{2^{\omega(\mathrm{Disc}(K))}}{|\operatorname{Disc}(K)|} \sim c(\log y)^2,$$

where $L(s, K/\mathbb{Q}) = \sum_n \frac{\chi_K(n)}{n^s}$ and χ_K is the quadratic character associated to K. According to Lemma 3.5.2, we know that

$$\sum_{\substack{0<D<y \\ D \text{ squarefree}}} \frac{2^{\omega(D)}}{D} \cdot \left(\sum_{m=1}^{\infty} \sum_{\substack{n=1 \\ mn \neq \square}}^{D^{\frac{1}{2}+\epsilon}} \frac{\mu(m)}{m^2 n} \left(\frac{D}{mn} \right) \right) = o(y),$$

for any $0 < \epsilon < \frac{1}{2}$. Then by [1, (21)], we know that

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ \mathrm{Disc}(K)>0}} \frac{2^{\omega(\mathrm{Disc}(K))}}{|\mathrm{Disc}(K)|^{-s}} \cdot \sum_{\substack{0<a,b<\infty \\ (\mathrm{Disc}(K),ab)=1}} \frac{\mu(a)}{a^3 b^2} = \zeta(2) \cdot \prod_p (1 + 2p^{-s} - \frac{2}{p^2} p^{-s} - \frac{1}{p^3}).$$

This implies that

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0<\mathrm{Disc}(K)<y}} \frac{2^{\omega(\mathrm{Disc}(K))}}{|\mathrm{Disc}(K)|} \cdot \sum_{\substack{0<a,b<\infty \\ (\mathrm{Disc}(K),ab)}} \frac{\mu(a)}{a^3 b^2} \sim c_1 (\log y)^2,$$

where $c_1 > 0$ is a constant. Similar result holds when $\mathrm{Disc}(K) < 0$. According to [1, (19) and (20)], we finally obtain that

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ |\mathrm{Disc}(K)|<y}} \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \frac{2^{\omega(\mathrm{Disc}(K))}}{|\mathrm{Disc}(K)|} \sim c_2 (\log y)^2$$

where $c_2 > 0$ is a constant. By [1, Lemma 4.5], we know that

$$N(\mathcal{S}, C; f; x, x^\beta) \sim cx(\log x)^2,$$

where $0 < \beta < \frac{2}{3}$. Hence we have

$$\mathbb{E}_C(|\operatorname{Hom}(\mathrm{Cl}_L, C_2)|) \geq 2^{-6} \mathbb{E}_C(f) \geq 2^{-6} \lim_{x \to \infty} \frac{N(\mathcal{S}, C; f; x, x^\beta)}{N(\mathcal{S}, C; x)} = +\infty.$$

□

Further discussion with Malle-Bhargava Heuristics

The main topic in this section is slightly different from the previouos one. When ordered by product of ramified primes, the Malle-Bhargava Heuristics ([41, 4, 62]) predict that

$$N(\mathcal{S}, P; x) \gg x \log^3 x. \tag{3.5.2}$$

For a quartic number field $L \in \mathcal{S}$, it admits a unique quadratic number field K. We can first try to describe the image of $\mathrm{Cl}_K[2]$ in Cl_L and then prove the related statistical results. Consider the group homomorphism

$$i : \mathscr{I}_K \to \mathscr{I}_L$$

between fractional ideals. It induces a group homomorphism on the class groups $\mathrm{Cl}_K \to \mathrm{Cl}_L$, which we denote by i_*. Recall that if M is the Galois closure,

$$C_K^{D_4} = (\mathscr{I}_K \cap \mathscr{I}_M^{D_4}) \cdot \mathcal{P}_K/\mathcal{P}_K,$$

where $\mathcal{P}_K$ is the group of principal ideals. We already know by genus theory for quadratic number fields that $\mathrm{Cl}_K[2]$ admits a good estimate with an algebraic expression and this result can give an infinite moment. So, it would not be surprising that $\mathrm{Cl}_L[2]$ has similar algebraic structure or statistical behaviour. We first give a statement explaining the relation between $\mathrm{Cl}_K[2^\infty]$ and $\mathrm{Cl}_L[2^\infty]$.

Lemma 3.5.4. *Let $L/\mathbb{Q}$ be a quartic number field with Galois D_4-closure $M/\mathbb{Q}$, let K be the quadratic subfield of L, and let $I(p)$ be the inertia subgroup of p.*

(i) Let Ω_1 be the set $\{\sigma, \sigma^3, \sigma\tau, \sigma^3\tau\}$. Then we have

$$|\{p \neq 2 : I(p) \cap \Omega_1 \neq \emptyset\}| \geq \mathrm{rk}_2\, i_* C_K^{D_4} \geq |\{p \neq 2 : I(p) \cap \Omega_1 \neq \emptyset\}| - 6.$$

(ii) Let Ω_2 be the set $\{\sigma^2\}$. Then we have

$$\mathrm{rk}_2\, C_L^{D_4}/i_*(C_K^{D_4}) \geq |\{p \neq 2 : I(p) \cap \Omega_2 \neq \emptyset\}| - 6.$$

(iii) Let Ω_3 be the set $\{\sigma, \sigma^3\}$. Then we have

$$|\{p \neq 2 : I(p) \cap \Omega_3 \neq \emptyset\}| \geq \mathrm{rk}_2\, 2C_L^{D_4} \geq |\{p \neq 2 : I(p) \cap \Omega_3 \neq \emptyset\}| - 6.$$

(iv) Let $\Omega_4 := \Omega(D_4, 2^\infty) = \{\sigma, \sigma^3, \sigma^2, \sigma\tau, \sigma^3\tau\}$. Then we have

$$\mathrm{rk}_2\, \mathrm{Cl}(L/K) \geq |\{p \neq 2 : I(p) \cap \Omega_4 \neq \emptyset\}| - 6.$$

Proof. We view the group of fractional ideals $\mathscr{I}_K, \mathscr{I}_L$ as subgroups of $\mathscr{I}_M$. *(i)*: First of all, an odd prime p is ramified in the quadratic extension $K/\mathbb{Q}$ if and only if $I(p) \cap \Omega_1 \neq \emptyset$. In other words,

$$C_K^{D_4} = \langle \mathfrak{p} | p \neq 2,\, I(p) \cap \Omega_1 \neq \emptyset \rangle / \mathscr{P}_K^{D_4},$$

where $\mathfrak{p} = (p\mathscr{O}_K)^2$ and $\mathscr{P}_K$ is the group of principal ideal of K. This already gives the upper bound of the 2-rank. It is clear that $\Omega_1 \subseteq \Omega(D_4, 2^\infty)$, i.e., $i_* C_K^{D_4}$ is a subgroup of $C_L^{D_4}$. So the lower bound of $\mathrm{rk}_2\, i_* C_K^{D_4}$ comes from

$$\mathrm{rk}_2\, \mathscr{P}_L/\mathscr{P}_K \leq \mathrm{rk}_2\, \mathscr{P}_L/\mathscr{P}_\mathbb{Q} \leq 6$$

by Lemma 3.1.13.

(ii): By comparing with the choice of Ω_1, it is not hard to see that if an odd prime p has inertia in Ω_2, then this means that p is unramified in $K/\mathbb{Q}$, and then prime(s) lying above p are ramified in L/K. Whatever the specific splitting type of p is, we see that $e_L(p) \equiv 0 \bmod 2$, hence p is a ramified prime of type 2. This shows that $\Omega_2 \subseteq \Omega(D_4, 2^\infty)$, i.e.,

$$\langle \mathfrak{a}(p) | p \neq 2 \text{ and } I(p) \cap \Omega_2 \neq \emptyset \rangle / \mathscr{P}_L^{D_4},$$

where $\mathfrak{a}(p) = (p\mathscr{O}_L)^{e_L(p)}$, is a subgroup of $C_L^{D_4}$. So, by Lemma 3.1.13 again, we obtain the result directly.

(iii): An odd prime p has inertia in Ω_3 means that it is totally ramified in $L/\mathbb{Q}$. The conclusion itself follows from Theorem 3.1.11 directly. Note that this also explains that if we want an upper bound for $\mathrm{rk}_2\, C_L^{D_4}/i_*(C_K^{D_4})$, then we can write it as

$$\mathrm{rk}_2\, C_L^{D_4}/i_*(C_K^{D_4}) \leq |\{p \neq 2 : I(p) \cap (\Omega_2 \cup \Omega_3) \neq \emptyset\}|.$$

(iv): This is just the application of Theorem 3.1.15 with $\Gamma = D_4$ and $[L : K] = 2 = q$. □

This lemma shows the relation between Ω_i, defined in the lemma, and the different subgroups of $C_L^{D_4}$. Now let's see what happens for counting fields.

Theorem 3.5.5. *Recall the definition of Ω_i in the above Lemma 3.5.4, where $i = 1, 2, 3, 4$. We show that*

$$N(\mathcal{S}, P; (\Omega_1, r); x) \ll x(\log x)^2 x(\log\log x)^{r+1}$$
$$N(\mathcal{S}, P; (\Omega_2, r); x) \ll x(\log x)^{7/2}(\log\log x)^{\frac{1}{2}(r+1)}$$
$$N(\mathcal{S}, P; (\Omega_3, r); x) \ll x(\log x)^{5/2}(\log\log x)^{\frac{1}{2}(r+1)}$$
$$N(\mathcal{S}, P; (\Omega_4, r); x) \ll x(\log x)^2(\log\log x)^{\frac{1}{2}(r+1)}.$$

Proof. The proof for Ω_1 and Ω_4 are similar to each other. The choice of Ω_1 means that if p has inertia in Ω_1 then p is ramified in the quadratic subextension $K/\mathbb{Q}$ of $L/\mathbb{Q}$. First we define the Dirichlet series

$$\sum_n a_n n^{-s} := \sum_n \left(\sum_{L \in \mathcal{S}, P(L)=n} \mathbf{1}_{(\Omega,r)}(L) \right) n^{-s}.$$

Given a quadratic number field $K/\mathbb{Q}$ of product of ramified primes $P(K)$, we can consider all quadratic extensions L/K to get an upper bound, that is, let

$$\sum_n b_n(K) n^{-s} := \sum_n \sum_{P(\rho)=n} 1 \cdot n^{-s}.$$

By considering the local morphisms $\mathrm{Hom}(\prod_{v|p} \mathscr{O}_v^*, C_2)$ together with their ramified primes, we have

$$\sum_n b_n(K) n^{-s} \leq |\,\mathrm{Hom}(\mathrm{Cl}_K, C_2)| 2^{\omega(P(K))+4} P(K)^{-s}(1 + 16 \cdot 2^{-s}) \prod_{p \nmid d} (1 + 3p^{-s}).$$

Finally we let K runs over all quadratic number fields and define the following Dirichlet series

$$\sum_n c_n n^{-s} := \sum_{d=p_1\cdots p_r} \sum_{P(K)=d} \sum_n b_n(K) n^{-s}.$$

By considering the upper bound of $\sum_n c_n n^{-s}$, we have

$$\begin{aligned}\sum_{n<x} c_n n^{-s} &\le \sum_{d=p_1\cdots p_r} 2^{2r+5} d^{-s}(1+16\cdot 2^{-s}) \prod_p (1+3p^{-s}) \\ &= g(s) + g_0(s)\log^r\left(\frac{1}{s-1}\right)(s-1)^{-3} + \cdots\end{aligned}$$

where $g(s), g_0(s), \ldots$ are holomorphic functions in the closed half plane $\Re(s) \ge 1$ whose existence follows from Proposition 3.3.5. Clearly, $\sum_n a_n n^{-s} \le \sum_n c_n n^{-s}$, hence by Theorem 3.3.1, we have

$$N(\mathcal{S}, P; (\Omega, r); x) \ll x \log^2 x (\log\log x)^r,$$

which is $o(x\log^3 x)$.

The proof for Ω_2, Ω_3 are based on Theorem 3.4.5 and similar to each other, so we only show one of them here. Recall that $\Omega_3 = \{\sigma, \sigma^3\}$. If an odd prime p has inertia in Ω_3, then this means that p is totally ramified in $L/\mathbb{Q}$ where $L \in \mathcal{S}$ is the quartic number field. Let $M/\mathbb{Q}$ be the Galois closure of $L/\mathbb{Q}$. Instead of considering the quartic number fields $L \in \mathcal{S}$, we consider another quadratic subfield $K_1 := M^{\langle\sigma\rangle}$. Note that K_1 is *not* a subfield of L. In other words, we view $D_4 = C_4 \rtimes C_2$. By Alex Smith [55], we know that Gerth's conjecture holds for Cl_{K_1} where K_1 runs over quadratic number fields. This shows the following:

$$\begin{aligned}N(\mathcal{S}(C_2), P; |\operatorname{Hom}(\mathrm{Cl}_{K_1}, C_4)|^2; x) &= \sum_{P(K_1)<x} |\operatorname{Sur}(\mathrm{Cl}_{K_1}, C_4)|^2 + \sum_{P(K_1)<x} |\operatorname{Hom}(\mathrm{Cl}_{K_1}, 2C_4)|^2 \\ &\ll N(\mathcal{S}(C_2), P; 4^{\omega(P(K_1))}; x) \\ &\ll x\log^3 x,\end{aligned}$$

where Sur means surjective group homomorphism. In addition, $C_4\backslash\Omega_3 = \{1, \sigma^2\}$. By Theorem 3.4.5 with $\mathcal{S}(D_4)$ and the given Ω_3, we have $\beta_1 = 3$ and $\beta(C_2, C_4\backslash\Omega_3) = 1$. Therefore, we have

$$N(\mathcal{S}, P; (\Omega_3, r); x) \ll x\log^{5/2} x (\log\log x)^{\frac{1}{2}(r+1)}.$$

□

Consequently we have the following statistical results, whose proof are just a direct application of Theorem 3.2.4 and Theorem 3.2.5.

Corollary 3.5.6. *Assume that the Malle-Bhargava Heuristics hold for $N(\mathcal{S}, P; x)$, or (3.5.2) holds, then for all $r = 1, 2, 3, \ldots$, we have*

$$\begin{aligned}&\mathbb{P}(\mathrm{rk}_2\, i_*(\mathrm{Cl}_K) \le r) = 0 \quad \textit{and} \quad \mathbb{E}(|\operatorname{Hom}(i_*(\mathrm{Cl}_K), C_2)|) = +\infty \\ &\mathbb{P}(\mathrm{rk}_2\, 2\,\mathrm{Cl}_L \le r = 0) \quad \textit{and} \quad \mathbb{E}(|\operatorname{Hom}(2\,\mathrm{Cl}_L, C_2)|) = +\infty \\ &\mathbb{P}(\mathrm{rk}_2\, \mathrm{Cl}(L/K) \le r = 0) \quad \textit{and} \quad \mathbb{E}(|\operatorname{Hom}(\mathrm{Cl}(L/K), C_2)|) = +\infty\end{aligned}$$

where $L \in \mathcal{S}$ for the product of ramified primes in $L/\mathbb{Q}$ and K is the quadratic subfield of L.

Bibliography

[1] Salim Ali Altug et al. *The number of quartic D_4-fields ordered by conductor*. 2017. arXiv: 1704.01729 [math.NT].

[2] Alex Bartel and Hendrik W Lenstra. "Commensurability of automorphism groups". In: *Compositio Mathematica* 153.2 (2017), pp. 323–346.

[3] Alex Bartel and Hendrik W Lenstra Jr. "On class groups of random number fields". In: *Proceedings of the London Mathematical Society* 121.4 (2020), pp. 927–953.

[4] Manjul Bhargava. "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants". English (US). In: *International Mathematics Research Notices* 2007 (2007). ISSN: 1073-7928. DOI: https://doi.org/10.1093/imrn/rnm052.

[5] Manjul Bhargava. "The density of discriminants of quartic rings and fields". In: *Annals of mathematics, ISSN 0003-486X, Vol. 162, Nº 2, 2005, pags. 1031-1062* 162 (Sept. 2005). DOI: 10.4007/annals.2005.162.1031.

[6] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. "On the Davenport–Heilbronn theorems and second order terms". In: *Inventiones mathematicae* 193.2 (2013), pp. 439–499.

[7] Manjul Bhargava et al. "Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves". In: *Cambridge Journal of Mathematics* 3.3 (2015), pp. 275–321. DOI: 10.4310/cjm.2015.v3.n3.a1. URL: https://doi.org/10.4310%2Fcjm.2015.v3.n3.a1.

[8] Nigel Boston and Melanie Matchett Wood. "Non-abelian Cohen–Lenstra heuristics over function fields". In: *Compositio Mathematica* 153.7 (2017), pp. 1372–1390.

[9] Gautam Chinta, Nathan Kaplan, and Shaked Koplewitz. "The cotype zeta function of $\mathbb{Z}^d$". In: *arXiv: Number Theory* (2017).

[10] Julien Clancy, Timothy Leake, and Sam Payne. "A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs". In: *Experimental Mathematics* 24.1 (2015), pp. 1–7.

[11] Julien Clancy et al. "On a Cohen–Lenstra heuristic for Jacobians of random graphs". In: *Journal of Algebraic Combinatorics* 42.3 (2015), pp. 701–723.

[12] H. Cohen and H. W. Lenstra. "Heuristics on class groups of number fields". In: (1984). Ed. by Hendrik Jager, pp. 33–62.

[13] Henri Cohen and Jacques Martinet. "Class groups of number fields: numerical heuristics". In: *Mathematics of Computation* 48.177 (1987), pp. 123–137.

[14] Henri Cohen and Jacques Martinet. "Étude heuristique des groupes de classes des corps de nombres." fre. In: *Journal für die reine und angewandte Mathematik* 404 (1990), pp. 39–76. URL: http://eudml.org/doc/153196.

[15] Boris Datskovsky and David J Wright. "Density of discriminants of cubic extensions." In: (1988).

[16] Harold Davenport and Hans Arnold Heilbronn. "On the density of discriminants of cubic fields. II". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 322 (1971), pp. 405–420.

[17] Christophe Delaunay. "Heuristics on Tate-Shafarevitch groups of elliptic curves defined over Q". In: *Experimental Mathematics* 10.2 (2001), pp. 191–196.

[18] Christophe Delaunay and Frédéric Jouhet. "The Cohen-Lenstra heuristics, moments and p^j-ranks of some groups". In: *arXiv preprint arXiv:1303.7337* (2013).

[19] Nathan M Dunfield and William P Thurston. "Finite covers of random 3-manifolds". In: *Inventiones mathematicae* 166.3 (2006), pp. 457–521.

[20] Jordan S Ellenberg, Akshay Venkatesh, and Craig Westerland. "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields". In: *annals of Mathematics* (2016), pp. 729–786.

[21] Étienne Fouvry and Jürgen Klüners. "Cohen–Lenstra heuristics of quadratic number fields". In: *International Algorithmic Number Theory Symposium*. Springer. 2006, pp. 40–55.

[22] Étienne Fouvry and Jürgen Klüners. "On the 4-rank of class groups of quadratic number fields." In: *Inventiones mathematicae* 167.3 (2007).

[23] III Frank Gerth. "Extension of conjectures of Cohen and Lenstra". In: *Expositiones Mathematicae* 5.2 (1987), pp. 181–184.

[24] Jason Fulman. "A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups". In: *Journal of Algebra* 212.2 (1999), pp. 557–590.

[25] Jason Fulman. "Cohen–Lenstra heuristics and random matrix theory over finite fields". In: *Journal of Group Theory* 17.4 (2014), pp. 619–648.

[26] Jason Fulman. "Hall-Littlewood polynomials and Cohen-Lenstra heuristics for Jacobians of random graphs". In: *Annals of Combinatorics* 20.1 (2016), pp. 115–124.

[27] Jason Fulman and Nathan Kaplan. "Random partitions and Cohen–Lenstra heuristics". In: *Annals of Combinatorics* 23.2 (2019), pp. 295–315.

[28] Derek Garton. "Some Finite Abelian Group Theory and Some q-Series Identities". In: *Annals of Combinatorics* 20.2 (2016), pp. 361–371.

[29] KW Gruenberg and A Weiss. "Capitulation and transfer kernels". In: *Journal de théorie des nombres de Bordeaux* 12.1 (2000), pp. 219–226.

[30] David R Heath-Brown. "The size of Selmer groups for the congruent number problem, II". In: *Inventiones Mathematicae* 118.2 (1994), pp. 331–370.

[31] David Hilbert. *The theory of algebraic number fields*. Springer Science & Business Media, 1998.

[32] M. Ishida. *The genus fields of algebraic number fields*. Lecture notes in mathematics. Springer-Verlag, 1976. URL: https://books.google.com/books?id=v6oZAQAAIAAJ.

[33] Matthew Kahle et al. "Cohen–Lenstra heuristics for torsion in homology of random complexes". In: *Experimental Mathematics* 29.3 (2020), pp. 347–359.

[34] Shaked Koplewitz. "Sandpile groups and the coeulerian property for random directed graphs". In: *Advances in Applied Mathematics* 90 (2017), pp. 145–159.

[35] Johannes Lengler. "A combinatorial interpretation of the probabilities of p-groups in the Cohen–Lenstra measure". In: *Journal of Number Theory* 128.7 (2008), pp. 2070–2084.

[36] Johannes Lengler. "The Cohen–Lenstra heuristic: methodology and results". In: *Journal of Algebra* 323.10 (2010), pp. 2960–2976.

[37] Michael Lipnowski, Will Sawin, and Jacob Tsimerman. "Cohen-Lenstra heuristics and bilinear pairings in the presence of roots of unity". In: *arXiv preprint arXiv:2007.12533* (2020).

[38] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown. "A predicted distribution for Galois groups of maximal unramified extensions". In: *arXiv preprint arXiv:1907.05002* (2019).

[39] Gunter Malle. "Cohen–Lenstra heuristic and roots of unity". In: *Journal of Number Theory* 128.10 (2008), pp. 2823–2835.

[40] Gunter Malle. "On the Distribution of Class Groups of Number Fields". In: *Experimental Mathematics* 19 (2010), pp. 465–474.

[41] Gunter Malle. "On the distribution of Galois groups, II". In: *Experimental Mathematics* 13.2 (2004), pp. 129–135.

[42] Melanie Matchett Wood. "The distribution of sandpile groups of random graphs". In: *arXiv e-prints*, arXiv:1402.5149 (Feb. 2014), arXiv:1402.5149. arXiv: 1402.5149 [math.PR].

[43] András Mészáros. "The distribution of sandpile groups of random regular graphs". In: *Transactions of the American Mathematical Society* 373.9 (2020), pp. 6529–6594.

[44] H.L. Montgomery and R.C. Vaughan. *Multiplicative Number Theory I: Classical Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006. ISBN: 9781139459938. URL: https://books.google.com/books?id=nGb1NADRWgcC.

[45] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer, 2014. ISBN: 9783662070024. URL: https://books.google.com/books?id=5KQGswEACAAJ.

[46] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013. ISBN: 9783662039830. URL: https://books.google.com/books?id=hS3qCAAAQBAJ.

[47] Hoi H Nguyen and Melanie Matchett Wood. "Cokernels of adjacency matrices of random r-regular graphs". In: *arXiv preprint arXiv:1806.10068* (2018).

[48] Hoi H Nguyen and Melanie Matchett Wood. "Random integral matrices: universality of surjectivity and the cokernel". In: *Inventiones mathematicae* (2021), pp. 1–76.

[49] Phong Q Nguyen and Igor E Shparlinski. "Counting co-cyclic lattices". In: *SIAM Journal on Discrete Mathematics* 30.3 (2016), pp. 1358–1370.

[50] Jennifer Park et al. "A heuristic for boundedness of ranks of elliptic curves". In: *Journal of the European Mathematical Society* 21.9 (2019), pp. 2859–2903.

[51] Lillian B Pierce, Caroline L Turnage-Butterbaugh, and Melanie Matchett Wood. "On a conjecture for l-torsion in class groups of number fields: from the perspective of moments". In: *arXiv preprint arXiv:1902.02008* (2019).

[52] I. Reiner. *Maximal Orders*. London Mathematical Society monographs series: London Mathematical Society. Clarendon Press, 2003. ISBN: 9780198526735. URL: https://books.google.com/books?id=0liBQgAACAAJ.

[53] Irving Reiner and Charles Whittlesey Curtis. *Methods of representation theory with applications to finite groups and orders*. Wiley, 1990.

[54] P. Roquette and H. Zassenhaus. "A Class Rank Estimate for Algebraic Number Fields". In: *Journal of the London Mathematical Society* s1-44.1 (1969), pp. 31–38. DOI: 10.1112/jlms/s1-44.1.31. eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms/s1-44.1.31. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-44.1.31.

[55] Alexander Smith. "2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture". In: *arXiv preprint arXiv:1702.02325* (2017).

[56] Richard P Stanley. "Smith normal form in combinatorics". In: *Journal of Combinatorial Theory, Series A* 144 (2016), pp. 476–495.

[57] Hiroshi Suzuki. "A generalization of Hubert's theorem 94". In: *Nagoya Mathematical Journal* 121 (1991), pp. 161–169.

[58] G. Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory*. Graduate Studies in Mathematics. American Mathematical Society, 2015. ISBN: 9780821898543. URL: https://books.google.com/books?id=UEk-CgAAQBAJ.

[59] Weitong Wang and Melanie Matchett Wood. "Moments and interpretations of the Cohen–Lenstra–Martinet heuristics". In: *Commentarii Mathematici Helvetici* 96.2 (2021), pp. 339–387.

[60] Yinghui Wang and Richard P Stanley. "The Smith normal form distribution of a random integer matrix". In: *SIAM Journal on Discrete Mathematics* 31.3 (2017), pp. 2247–2268.

[61] Melanie Wood. "The distribution of sandpile groups of random graphs". In: *Journal of the American Mathematical Society* 30.4 (2017), pp. 915–958.

[62] Melanie Matchett Wood. "ARIZONA WINTER SCHOOL 2014 COURSE NOTES: ASYMPTOTICS FOR NUMBER FIELDS AND CLASS GROUPS". In: 2014.

[63] Melanie Matchett Wood. "Cohen-Lenstra heuristics and local conditions". In: *Research in Number Theory* 4.4 (2018), pp. 1–22.

[64] Melanie Matchett Wood. "On the probabilities of local behaviors in abelian field extensions". In: *Compositio Mathematica* 146.1 (2010), pp. 102–128.

[65] Melanie Matchett Wood. "Random integral matrices and the Cohen-Lenstra heuristics". In: *American Journal of Mathematics* 141.2 (2019), pp. 383–398.