Moments and interpretations of the Cohen–Lenstra–Martinet heuristics

Weitong Wang and Melanie Matchett Wood

Abstract. The goal of this paper 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.

1. Introduction

In this paper we prove several results to help elucidate the Cohen–Lenstra–Martinet conjectures [9,11] for the distributions of class groups of number fields, and to further the understanding of their implications. In Section 3, we explain the statement of the conjectures in the framework of probability theory. In Section 4, 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 3.5 and Theorem 4.1 for precise statements.)

Theorem 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

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

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 [9], 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 5, we slightly enlarge 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 $|H^{\Gamma_\infty}||\mathrm{Aut}_\Gamma(H)|$, explaining the probabilities above. Bartel and Lenstra [2] 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 [1]). Their predicted distribution on Arakelov class groups then pushes forward to the Cohen–Lenstra–Martinet distribution, over any base number field.

In Section 6, we determine the moments, which are important averages of the Cohen–Lenstra–Martinet distributions on finite abelian Γ-modules.

Theorem 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*

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

Here $\mathrm{Sur}_\Gamma(X, H)$ denotes the surjective Γ-module homomorphisms from X to H. See Theorem 4.1 and Theorem 6.2 for precise statements. These moments are the most important averages of the Cohen–Lenstra–Martinet distributions. (See [7, 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 [14] (and Datskovsky and Wright [13] 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 [3]. (There is also more known on the 2-Sylow subgroup of the class groups of quadratic fields; see [20, 44].) 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 [18] and the second author [50] for quadratic extensions, and of Liu, the second author,

and Zureick–Brown [34] for Γ-extensions, showing that as $q \to \infty$ the moments match those in Theorem 1.2. The paper [42] 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 1.2 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 1.3 (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*

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

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

See Theorems 6.12 and 6.13 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 1.3 is part of a long line of work showing results in the same spirit for other categories of groups, including work of Heath-Brown [27, Lemma 17] for elementary abelian p-groups, Ellenberg, Venkatesh, and Westerland [18, Section 8] for finite abelian p-groups, the second author for finite abelian groups [49, Section 8], and Boston and the second author [5, Theorem 1.4] for pro-p groups with a $\mathbb{Z}/2\mathbb{Z}$ action. See [16, 19, 24, 50] 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

$$\operatorname{Cl}_K \otimes_\mathbb{Z} \mathbb{Z}[|\Gamma|^{-1}] = (\operatorname{Cl}_L^{\Gamma'}) \otimes_\mathbb{Z} \mathbb{Z}[|\Gamma|^{-1}]$$

(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 1.4 (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 7.6 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 1.4 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 1.4, 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 [28] 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 [46] and Gruenberg and Weiss [26] 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 1.4 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 (7.1)). This prediction does not have the appearance of objects appearing with frequency inversely proportional to their number of automorphisms. However, in Section 8, 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 1.4) is naturally an $\mathfrak{o}$-module (see Lemma 8.4) and prove that our constructed $\mathfrak{o}$ is a maximal order (Corollary 8.10). 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 8.20 on degree 10 fields with Galois closure with group A_5 and Proposition 8.16 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 1.4 and the results in Section 8 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 $|\mathrm{Aut}_{\mathfrak{o}}(H)|^{-1}$ by way of the following result.

Theorem 1.5 (Cohen–Martinet predicts $|\mathrm{Aut}_{\mathfrak{o}}(H)|^{-1}$ for non-Galois fields). *Given a finite group Γ and subgroup Γ', for every prime p satisfying the condition of Theorem 1.4, 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*

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

See Theorem 8.14 for a related statement precisely on the implications of the Cohen–Martinet conjecture. The key result we prove that allows us to prove Theorem 1.5 is Theorem 8.9, 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 1.4 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 9, we prove that all of the predicted distributions agree, which is an important internal consistency check on the conjectures.

Theorems 1.1, 1.2, 1.3, and 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 1.2 and 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 [4, 15], and so in order to generalize the predictions of [41] 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 [24] and also [6–8,21–23,25,31,32,38,45,47]. 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 [30,37,49]. These theorems on the moments have also been used to show that certain random matrices have cokernels in the Cohen–Lenstra distribution [39,40,51], 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 [17,29]. The more general Cohen–Lenstra–Martinet distributions may be relevant in many of these contexts.

2. Notation

Throughout the whole paper, Γ is always a finite group and S is always a set of (possibly infinitely many) rational primes.

Definition 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 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 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 [11].) We will also use the usual notation $\mathbb{Z}_{(p)}$ for $\mathbb{Z}_S$ when $S = \{p\}$.

Definition 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 $R/(1 - e)R$.

3. 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.

3.1. 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 [43, §10] for basic results on semisimple $\mathbb{Q}$-algebras and maximal orders.)

3.2. 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 3.1. We define the rank of K/K_0 to be an $m - 1$-tuple in $\mathbb{Q}^{m-1}$ given by the formula

$$\underline{u} = (u_2, \ldots, u_m), \quad u_i = \frac{1}{h_i} \langle \chi_K, \varphi_i \rangle \qquad \forall i = 2, \ldots, m. \tag{3.1}$$

Remark 3.2. For the original definition of rank of K, see [11, Definition 6.4]. These two definitions are equivalent by [11, 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 [11], the distributions we will now define turn out to be equivalent to the ones considered in [11]. We think there are advantages of viewing the conjecture in multiple equivalent but differently presented forms.

Definition 3.3. 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

$$X = X\big((1 - e_1)\mathbb{Q}[\Gamma], \underline{u}, (1 - e_1)\mathbb{Z}_S[\Gamma]\big)$$

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

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

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

Remark 3.4. It follows from [11, 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

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

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.

3.3. Statement of the conjecture. The conjecture of Cohen–Martinet [11, Hypothesis 6.6] says the following.

Conjecture 3.5 (Cohen and Martinet [11]). *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*

$$X = X\big((1 - e_1)\mathbb{Q}[\Gamma], \underline{u}, (1 - e_1)\mathbb{Z}_S[\Gamma]\big)$$

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

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

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 [9, Fundamental Assumptions 8.1].

Remark 3.6. In [11], a quantity $M_{\underline{u}}^S(f)$ appears in place of $\mathbb{E}(f(X))$. The identity $M_{\underline{u}}^S(f) = \mathbb{E}(f(X))$ is proved in Proposition 6.6. Also the S-part of the relative class group Cl_{K/K_0}^S appears in place of $(1 - e_1)\mathrm{Cl}_K^S$. In Lemma 7.12, we show that these are actually the same. Note that $e_1 \mathrm{Cl}_K^S = \mathrm{Cl}_{K_0}^S$. 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 7.2.

Remark 3.7. In Conjecture 3.5, 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 Bartel and Lenstra [2, Theorem 1.1], 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 [2, Theorem 1.2] of Bartel and Lenstra, who suggest ordering fields by the radical of their discriminant based on work on the second author [48] that shows this ordering has nice statistical properties for abelian Galois groups. Third, Malle's work [35, 36] 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 [34] 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 [4, Section 5.6] and [2, 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 [50, Section 1] and [33, Section 3.5] for specific discussion of this aspect of the analogy.

4. 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 3.

Theorem 4.1. *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 [11, 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 3.1, and one can check $h = \dim \varphi$. We then know that

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

completing the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Remark 4.2. Actually the statement of Theorem 4.1 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 7). 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 [11] still holds in this case.

5. 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 [9, 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 [2] 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 $\overline{\mathbb{Q}} \subset \mathbb{C}$ so that $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has a canonical decomposition group $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ at ∞. We fix a map $s \colon \operatorname{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma$, let $K \subset \overline{\mathbb{Q}}$ be a Galois extension of $\mathbb{Q}$ with an isomorphism $\operatorname{Gal}(K/\mathbb{Q}) \simeq \Gamma$, and let the decomposition group at ∞ given by s (under the isomorphism). Let K' be the maximal unramified abelian extension of K in $\overline{\mathbb{Q}}$ of order prime to $|\Gamma|$. The structure we consider is the finite group $G := \operatorname{Gal}(K'/\mathbb{Q})$ with given maps

$$c \colon \operatorname{Gal}(\mathbb{C}/\mathbb{R}) \to G \quad \text{and} \quad \pi \colon G \to \operatorname{Gal}(K/\mathbb{Q}) = \Gamma,$$

where π is a surjection with abelian kernel. Of course, $\ker(\pi) = \operatorname{Cl}_K^S$ (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 5.1. For a given map $s\colon \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma$, we call (G, c, π) a *class triple* (for s) if G is a finite group satisfying the following conditions:

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

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

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

(iv) $\operatorname{im} c \cap \ker \pi = 1$.

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 5.2. *For a given map* $s\colon \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma$ *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

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

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 $K := \pi^{-1}(\operatorname{im} \pi \circ c)$. So we have

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

Since $\operatorname{im} c \cap \ker \pi = 1$, one splitting of the above is $\operatorname{im} \pi \circ c \to \operatorname{im} c$. Another splitting is $\operatorname{im} \pi \circ c \to 1 \times \operatorname{im} \pi \circ c \subset \ker \pi \rtimes \Gamma$ 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 $I = \operatorname{im} \pi \circ c$. Then the elements of $\operatorname{im} c$ are

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

for $\gamma \in I$. These elements are fixed by the element of $\operatorname{Aut}(G, \pi)$ that comes from $\psi \in \operatorname{Aut}_\Gamma(\ker \pi)$ and conjugation of Γ by $(m, 1)$ if and only if for all $\gamma \in I$,

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

i.e.

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

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 $|\operatorname{Aut}_\Gamma(\ker \pi)||(\ker \pi)^I|$ elements of $\operatorname{Aut}(H, \pi)$ 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. $\qquad\square$

Corollary 5.3. *Let $K \subset \bar{\mathbb{Q}}$ be a Galois extension of $\mathbb{Q}$ with Galois group Γ and decomposition group Γ_∞ at ∞ and map $s \colon \operatorname{Gal}(\mathbb{C}/\mathbb{R}) \to \Gamma_\infty \subset \Gamma$. Let $G := \operatorname{Gal}(K'/\mathbb{Q})$ with given maps*

$$c \colon \operatorname{Gal}(\mathbb{C}/\mathbb{R}) \to G \quad and \quad \pi \colon G \to \operatorname{Gal}(K/\mathbb{Q}) = \Gamma,$$

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

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

So, combining with Theorem 4.1, 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).

6. 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.

6.1. Moments for Galois extensions. We keep the notation from Section 3.1. 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 6.1 (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 3.4, 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 6.2. *Given a finite $\mathfrak{O}$-module H, we have*

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

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

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

where $G' \subset G$ denotes G' a sub-$\mathfrak{O}$-module of G. For G_1 and G_2 finite $\mathfrak{O}$-modules, [11, 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

$$Z(\underline{u}) = \sum_{G/\sim} \frac{1}{|G|^{\underline{u}} |\operatorname{Aut}_{\mathfrak{O}}(G)|}. \tag{6.1}$$

Then we deduce that

$$\mathbb{E}\big(|\operatorname{Sur}_{\mathfrak{O}}(X, H)|\big) = \sum_{G/\sim} \mathbb{P}(X \cong G)|\operatorname{Sur}_{\mathfrak{O}}(G, H)|$$

$$= \sum_{G/\sim} \frac{1}{|G|^{\underline{u}}|\operatorname{Aut}_{\mathfrak{O}}(G)|Z(\underline{u})}|\operatorname{Aut}_{\mathfrak{O}}(H)| \sum_{G_1/\sim} \#\{G' \subseteq G \mid G' \cong G_1, G/G' \cong H\}$$

$$= \frac{|\operatorname{Aut}_{\mathfrak{O}}(H)|}{Z(\underline{u})} \sum_{G_1/\sim} \frac{1}{|G_1|^{\underline{u}}|H|^{\underline{u}}} \sum_{G/\sim} \frac{1}{|\operatorname{Aut}_{\mathfrak{O}}(G)|}\#\{G' \subseteq G \mid G' \cong G_1, G/G' \cong H\}$$

$$= |\operatorname{Aut}_{\mathfrak{O}}(H)| \sum_{G_1/\sim} \frac{1}{|\operatorname{Aut}_{\mathfrak{O}}(G_1)| \cdot |G_1|^{\underline{u}}Z(\underline{u})} \frac{1}{|\operatorname{Aut}_{\mathfrak{O}}(H)| \cdot |H|^{\underline{u}}}$$

$$= \frac{1}{|H|^{\underline{u}}} \sum_{G_1/\sim} \mathbb{P}(X \cong G_1) = \frac{1}{|H|^{\underline{u}}}. \qquad \square$$

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 6.3. *Let $e = e_2 + \cdots + e_k$ be some central idempotent of A, and let*

$$X_1 = X\big(A, \underline{u} = (u_1, \ldots, u_m), \mathfrak{O}\big) \quad \text{and} \quad X_2 = X\big(eA, \underline{v} = (v_2, \ldots, v_k), e\mathfrak{O}\big)$$

be the random modules defined in Section 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. $\square$

Therefore, Theorem 6.2 can be applied to eX directly.

Corollary 6.4. *Let $e \in \mathfrak{O}$ be any central idempotent. Given a finite $\mathfrak{O}$-module H, we have*

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

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 6.3 and Theorem 6.2. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Now we will show that the expected values of functions of X agree with the averages that appear in the conjectures of [11].

Remark 6.5. The original definition of $M_{\underline{u}}^S(f)$, the average appearing the the conjectures in [11], 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 6.6. *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*

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

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 [11, 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 [11, Theorem 4.6 (ii)] with $\psi(G) = |\mathrm{Aut}_{\mathfrak{O}}(G)|^{-1}$ and $\underline{s} = \underline{u}$, if

$$g_{G_1}(G) = \#\{\varphi \in \mathrm{Hom}_{\mathfrak{O}}(P, G) : G/\mathrm{im}\,\varphi \cong G_1\}$$

and P is projective of rank $\underline{u}$, then

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

where Z is defined in (6.1) (and see Remark 3.4 for the convergence). Then we have

$$\sum_{G/\sim} |G|^{-\underline{u}} \sum_{\varphi \in \mathrm{Hom}_{\mathfrak{O}}(P,G)} |\mathrm{Aut}_{\mathfrak{O}}(G)|^{-1} f(G/\mathrm{im}\,\varphi)$$

$$= \sum_{G_1/\sim} f(G_1) \sum_{G/\sim} \frac{g_{G_1}(G)}{|\mathrm{Aut}_{\mathfrak{O}}(G)||G|^{\underline{u}}}$$

$$= \sum_{G_1/\sim} f(G_1) \frac{Z(\underline{0})}{|\mathrm{Aut}_{\mathfrak{O}}(G_1)||G_1|^{\underline{u}} Z(\underline{u})} = Z(\underline{0}) \mathbb{E}\big(f(X)\big).$$

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

6.2. Moments determine the distribution. So the random $\mathfrak{O}$-module X has H-moment $|H|^{-\underline{u}}$ for every finite $\mathfrak{O}$-module H. Now we ask: given a random finite $\mathfrak{O}$-module Y with H-moment $|H|^{-\underline{u}}$ 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 3.1: $A = \prod_{i=1}^{m} A_i$ 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

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

where $\mathfrak{o}_{i,\mathfrak{p}}$ 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

$$|\operatorname{Aut}_{\mathfrak{O}}(G_1)| = \prod_{(i,\mathfrak{p})} |\operatorname{Aut}_{\mathfrak{O}_{i,\mathfrak{p}}}(G_{1,\mathfrak{p}})|$$

and

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

Moreover, the category of $\mathfrak{O}_{i,\mathfrak{p}}$-modules is equivalent to the category of $\mathfrak{o}_{i,\mathfrak{p}}$-modules, because they are both matrix algebras over $\mathfrak{o}_{i,\mathfrak{p}}$. 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 $\mathfrak{o}$ and we consider the category of finite $\mathfrak{o}$-modules. Given any (finite) partition $\lambda: \lambda_1 \geq \lambda_2 \geq \ldots$, there exists a unique (up to isomorphism) finite $\mathfrak{o}$-module G such that

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

where $\mathfrak{p}$ is the unique maximal ideal of $\mathfrak{o}$, see, e.g. [11, Lemma 2.7]. Then we write $G = G_\lambda$ and call it the $\mathfrak{o}$-module of type λ. Also let $q = |\mathfrak{o}/\mathfrak{p}|$ be the cardinality of the simple $\mathfrak{o}$-module.

Definition 6.7. 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 6.8. *Let D be a division algebra over $\mathbb{Q}_p$ with maximal $\mathbb{Z}_p$-order $\mathfrak{O}$. Given two $\mathfrak{O}$-modules G_λ, G_μ of type λ and μ. Then*

$$|\operatorname{Hom}_{\mathfrak{O}}(G_\lambda, G_\mu)| = q^{\sum_{i=1}^{\infty} \lambda_i' \mu_i'}.$$

Proof. By Lemma 2.7 (and more generally §2) in [11], we only need to check the formula for the case when G_λ, G_μ are both cyclic, which is clear, i.e.

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

Lemma 6.9. *Let $G = G_\lambda$ be a $\mathfrak{O}$-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

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

i.e. if $f\colon G_\mu \to G_\lambda$ happens to be an injective map, then $f \circ g$ where $g \in \operatorname{Aut}_{\mathfrak{O}}(G_\mu)$ clearly gives us the same subgroup in G_λ. Then by Theorem 2.11 in [11], if $\pi_1, \ldots, \pi_t$ are the distinct (nonzero) values of $\{\mu_i\}$ with multiplicities $k_1, \ldots, k_t$, then

$$|\operatorname{Aut}_{\mathfrak{O}}(G_\mu)| = q^{\sum_i (\mu_i')^2} \prod_{i=1}^{t} (k_i)_q$$

$$\geq q^{\sum_i (\mu_i')^2} \prod_{i=1}^{t} (\infty)_q \geq q^{\sum (\mu_i')^2} \prod_{j=1}^{\infty} (1 - q^{-j})^{\mu_1},$$

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

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

$$\leq \prod_j \frac{1}{(1 - 2^{-j})^{\lambda_1}} \cdot q^{\sum \mu_i' \lambda_i' - (\mu_i')^2}. \qquad \square$$

Lemma 6.10. *For any given $\mathfrak{O}$-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 6.9 over all $\mu \leq \lambda$, and a bound for this sum is given in [49, Lemma 7.5]. $\qquad \square$

Now using the lemmas above and results from [49], 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 6.2 must converge to the Cohen–Lenstra–Martinet distribution.

Theorem 6.11. *Take $A, \mathfrak{O}, m$ as in Section 3.1 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 [43, 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 [49, 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 6.8 and the same argument as in [49, Theorem 8.3], for each $G \in \mathcal{S}$, there exists $G' \in \mathcal{S}$ such that

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

Then the same argument as in in [49, 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

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

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 $|\mathrm{Hom}_{\mathfrak{D}}(X, H)|$ and $|\mathrm{Sur}_{\mathfrak{D}}(X, H)|$ over all H, are determined from one another by finitely many steps of addition and subtraction. We will apply [49, 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 [49, 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 $i = 1, \dots, m$, 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 $\mathfrak{D}$-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 6.10, we know that C_λ satisfies

the condition in [49, Theorem 8.2]. Then [49, 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 [49, 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 6.12. *Keep the notations in Theorem 6.11. Assume that $|S| < \infty$. If $\{X_n\}$ is a sequence of random variables taking values in finite $\mathfrak{D}$-modules such that*

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

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

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

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

Proof. If $|S| < \infty$, we can take into account all the prime ideals of $\mathfrak{D}$ 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 6.11 we take $n_{i,\mathfrak{p}} = (\lambda^{i,\mathfrak{p}})'_1 + 1$. If H is any $\mathfrak{D}$-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 6.13. *Assume that $|S| = \infty$ and $u_i > 0$ for all $i = 1, \ldots, m$, and $X = X(A, \underline{u}, \mathfrak{D})$ is the random variable we've defined. If Y is a random variable taking values in finite $\mathfrak{D}$-modules such that*

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

Then,

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

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

Proof. We let $\mathfrak{p}_i$ be the primes of $\mathfrak{D}$. By Theorem 6.12, for every n we have

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

Then by basic properties of measures, we have

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

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

Example 6.14. 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

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

However, $\lim_{p \to \infty} \mathbb{P}(Y_p \cong H) = 0$. This shows there is no analog of Theorem 6.12 for infinite S.

7. Explanation of the Cohen–Martinet heuristics in the non-Galois case

Cohen and Martinet [11] 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 [11] that includes these primes.

In this section we continue the notations introduced in Section 3.1 and Section 3.2. In particular, Γ is a fixed finite group.

Definition 7.1. 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 [11, 6.1], but they are equivalent (see [43, 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, [11, Hypothesis 6.6] is a conjecture for the distribution of $e\, \mathrm{Cl}_K^S$. Proposition 6.6 and Lemma 7.12 show that this conjecture is equivalent to the following.

Conjecture 7.2 (Cohen and Martinet [11]). *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*

$$X = X\big(e(1 - e_1)\mathbb{Q}[\Gamma], \underline{u}, e\mathbb{Z}_S[\Gamma]\big).$$

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:

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

where L runs through all Γ-extensions of K_0 such that $|\mathrm{Disc}\, L| \le x$ 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 3.7 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 $i \colon I_K \to I_L$ defined on fractional ideals induce, by passing to the classes, the homomorphism:

$$i_* \colon \mathrm{Cl}_K \to \mathrm{Cl}_L \,.$$

For this homomorphism, we have the following.

Theorem 7.3 ([11, Theorem 7.6]). *Let L/K be a Γ'-extension of number fields. The kernel (resp. the cokernel) of*

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

The direct corollary is the following.

Corollary 7.4 ([11, 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*

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

When $p \nmid |\Gamma|$, the above results mean that Conjecture 7.2 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 7.14) that if p is a good prime for $e_{\Gamma/\Gamma'}$ which is defined below, then $p \mid |\Gamma'|$, which implies that Corollary 7.4 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 7.6 that allows us to deduce consequences Conjecture 7.2 for p-Sylow subgroups of class groups of non-Galois fields and $p \mid |\Gamma|$.

Definition 7.5. Let $1_{\Gamma'}$ be the unit character of Γ', and

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

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 7.6. *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 $i_*\colon \mathrm{Cl}_{K/K_0}^S \to \mathrm{Cl}_L^S$ is injective with image*

$$\left(e_{\Gamma/\Gamma'} \mathrm{Cl}_L^S \right)^{\Gamma'} \subseteq \mathrm{Cl}_L^S,$$

i.e.

$$i_*\colon \mathrm{Cl}_{K/K_0}^S \xrightarrow{\sim} \left(e_{\Gamma/\Gamma'} \mathrm{Cl}_L^S \right)^{\Gamma'}$$

is an isomorphism.

Remark 7.7. Cohen and Martinet give another result [11, Theorem 7.8] that could be used to relate the class groups of non-Galois fields to Galois fields, but [11, 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 [10]. However, our Theorem 7.6 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 7.8. *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 7.8 appears to be a new result on the capitulation kernel.

From Theorem 7.6, we see that Conjecture 7.2 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

$$\sum_{\substack{G/\sim \\ G^{\Gamma'} \cong H}} \frac{1}{|G|^{\underline{u}} |\mathrm{Aut}_\Gamma(G)|}, \tag{7.1}$$

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 7.6. In the next section we will give a simple expression for (7.1) and an interpretation of the values appearing in (7.1). We start with a useful statement that we will use repeatedly.

Lemma 7.9. *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*

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

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

Proof. Note that via the ring homomorphism $e\colon \mathbb{Z}_S[\Gamma] \to e\mathbb{Z}_S[\Gamma]$ 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 $\varphi\colon P \to G$. 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 [43, 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. $\qquad\square$

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

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

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 $(e_i \mathbb{Q}[\Gamma])^{\Gamma'} = e_1' e_i \mathbb{Q}[\Gamma]$. $\qquad\square$

Remark 7.11. 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 7.12. *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 7.13. 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 3.5 and 7.2) 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 $\mathrm{Nm}_{L/K_0}(I)$ is indeed a principal ideal of K_0 for all ideals $I \in I_L$ such that the ideal class $[I]$ is contained in $e\,\mathrm{Cl}_L[p^\infty]$.

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

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

Therefore,

$$\mathrm{Nm}_{L/K_0} : e\,\mathrm{Cl}_L[p^\infty] \to e\,\mathrm{Cl}_L[p^\infty]$$

is actually the zero map.

Claim. $(eP_{L,p})^\Gamma = P_{K_0,p} \cap eP_{L,p}$.

Proof of 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 7.9. In particular,

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

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. $\qquad\square$

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

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

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.

$$e\,\mathrm{Cl}_L[p^\infty] = e\,\mathrm{Cl}_{L/K_0}[p^\infty]. \qquad\qquad\square$$

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

Lemma 7.14. *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 $a x_0 = e_1$, i.e.

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

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

Finally let's prove Theorem 7.6.

Proof of Theorem 7.6. 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 7.14, we know that $p \nmid |\Gamma/\Gamma'| = [K : K_0]$. Then let us view $\mathrm{Cl}_{K_0}[p^\infty]$ as a subgroup of $\mathrm{Cl}_K[p^\infty]$ via the induced map $i_* \colon \mathrm{Cl}_{K_0} \to \mathrm{Cl}_K$. 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

$$n_*\big(\mathrm{Cl}_{K_0}[p^\infty]\big) = [K : K_0] \cdot \mathrm{Cl}_{K_0}[p^\infty] = \mathrm{Cl}_{K_0}[p^\infty].$$

Then, by $i_* \circ n_* = [K : K_0]$, we see that $\frac{1}{[K:K_0]} i_*$ is well-defined for $\mathrm{Cl}_{K_0}^S$ and splits n_*. This shows (i).

Next, let us 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 $i \colon I_K \to I_L$, we have an exact sequence

$$I_{K,p} \cap I_{L,p}^\Gamma \to \mathrm{Cl}_K[p^\infty] \to \mathrm{Cl}_{K/K_0}[p^\infty] \to 1, \tag{7.2}$$

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).

Proof of Claim 1. 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 $\mathrm{Cl}_K[p^\infty] \to \mathrm{Cl}_{K/K_0}[p^\infty]$. $\qquad\square$

Claim 2. We have a short exact sequence

$$1 \to P_{K,p} \cap e_{\Gamma/\Gamma'} P_{L,p} \to I_{K,p} \cap e_{\Gamma/\Gamma'} I_{L,p} \to \mathrm{Cl}_{K/K_0}[p^\infty] \to 1. \tag{7.3}$$

Proof of Claim 2. 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 $y \in (e_{\Gamma/\Gamma'} I_{L,p})^{\Gamma'}$ and $z \in I_{L,p}^{\Gamma}$. By Lemma 7.9, the $e_{\Gamma/\Gamma'} \mathbb{Z}_{(p)}[\Gamma]$-module $e_{\Gamma/\Gamma'} I_{L,p}$ is cohomologically trivial. Hence,

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

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.

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

where the direct product is the direct product as abelian groups. Then by (7.2), $[z] \in \mathrm{Cl}_{K_0}[p^{\infty}]$, and $[x] \equiv [y]$ in the relative class group

$$\mathrm{Cl}_{K/K_0}[p^{\infty}] = \mathrm{Cl}_K[p^{\infty}] / \mathrm{Cl}_{K_0}[p^{\infty}],$$

which proves Claim 2. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Moreover, the claim also tells us that

$$i_*\big(\mathrm{Cl}_{K/K_0}[p^{\infty}]\big) \subseteq e_{\Gamma/\Gamma'} \mathrm{Cl}_{L/K_0}[p^{\infty}].$$

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

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

where every object showing up is an $e_{\Gamma/\Gamma'} \mathbb{Z}_{(p)}[\Gamma]$-module. Then by Lemma 7.9, we know that $e_{\Gamma/\Gamma'} P_{L,p}$, $e_{\Gamma/\Gamma'} I_{L,p}$ and $e_{\Gamma/\Gamma'} \mathrm{Cl}_L[p^{\infty}]$ are all cohomologically trivial as Γ-modules. So the identity

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

holds. This immediately implies that if $[x] \in \big(e_{\Gamma/\Gamma'} \mathrm{Cl}_L[p^{\infty}]\big)^{\Gamma'}$, then $[x]$ is represented by an ideal coming from K, and

$$i_*: \mathrm{Cl}_{K/K_0}[p^{\infty}] \to \big(e_{\Gamma/\Gamma'} \mathrm{Cl}_L[p^{\infty}]\big)^{\Gamma'}$$

is surjective. Similarly, by

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

we know that

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

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

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

Then these identities together with the short exact sequence (7.3) gives the following commutative diagram which concludes the proof:

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

8. Reinterpretation of the Cohen–Martinet heuristics in the non-Galois case

In this section, we reinterpret the distribution on abelian groups from (7.1) 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 have defined the trivial idempotent e_1 in Section 3.2, the augmentation character $a_{\Gamma/\Gamma'}$ and the central idempotent $e_{\Gamma/\Gamma'}$ of $\mathbb{Q}[\Gamma]$ associated to it in Section 6. 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 7), 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 8.1. 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.

8.1. 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 8.10, we will see that $\mathfrak{o}$ is actually a maximal order.

Definition 8.2. 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

$$e_{\Gamma/\Gamma'}\mathfrak{O} = M_{n-1}(\mathbb{Z}_S) \quad \text{and} \quad \mathfrak{o} = \mathbb{Z}_S$$

(see Example 8.18). When $\Gamma = D_4$ and Γ' is a non-central order 2 subgroup, we have

$$e_{\Gamma/\Gamma'}\mathfrak{O} = \mathbb{Z}_S \times M_2(\mathbb{Z}_S) \quad \text{and} \quad \mathfrak{o} = \mathbb{Z}_S^2$$

(see Example 8.19). 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,

$$e_{\Gamma/\Gamma'}\mathfrak{O} = M_4(\mathbb{Z}_S) \quad \text{and} \quad \mathfrak{o} = \mathbb{Z}_S.$$

As suggested by these examples, we will show in general that $e_{\Gamma/\Gamma'}\mathfrak{O}$ and $\mathfrak{o}$ are Morita equivalent in Theorem 8.9, 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 8.3. *Let $e_1, \ldots, e_m$ be the distinct irreducible central idempotents of $\mathbb{Q}[\Gamma]$ and $e_{\Gamma/\Gamma'} = e_2 + \cdots + e_k$. 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

$$e_1' \mathbb{Q}[\Gamma] e_1 e_1' = e_1 A \quad \text{and} \quad {}^{\Gamma'}\big((1 - e_{\Gamma/\Gamma'})\mathfrak{O}e_1'\big) = {}^{\Gamma}\mathfrak{O},$$

c.f. Lemma 7.10. 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'

$$A' = e_2 e_1' A' \times \cdots \times e_m e_1' A',$$

with each component a $\mathbb{Q}$-algebra because $e_i e_1'$ 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 7.10. So we have

$$A' = e_2 e_1' A' \times \cdots \times e_k e_1' A'.$$

For any simple $\mathbb{Q}$-algebra $B \cong M_l(D)$ where D is a 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. [12, 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 $\sigma xe_1' = xe_1'$ for all $\sigma \in \Gamma'$, we know that $e_1' xe_1' = xe_1'$, 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 $xy \in e_{\Gamma/\Gamma'}\mathfrak{D}$ 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 $y \in |\Gamma'|^2 e_{\Gamma/\Gamma'}\mathfrak{D}$ because $\mathbb{Q} \otimes e_{\Gamma/\Gamma'}\mathfrak{D} = e_{\Gamma/\Gamma'}A$. Therefore,

$$e_1' xe_1' = \frac{1}{n} \otimes e_1' ye_1',$$

where $e_1' ye_1' \in {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{D})^{\Gamma'} \subseteq \mathfrak{o}$ 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 $e_{\Gamma/\Gamma'}\mathfrak{D}$ is finitely generated as a $\mathbb{Z}_S$-module, say $e_{\Gamma/\Gamma'}\mathfrak{D} = \mathbb{Z}_S \cdot x_1 + \cdots + \mathbb{Z}_S \cdot x_N$, then

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

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

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

Lemma 8.4. *For any finitely generated $e_{\Gamma/\Gamma'}\mathfrak{D}$-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 $e_{\Gamma/\Gamma'}\mathfrak{D}$ on G, for all $g \in {}^{\Gamma'}G$ and $\sigma e_1' \in \mathfrak{o}$ with $\sigma \in e_{\Gamma/\Gamma'}\mathfrak{D}$.

Remark 8.5. As the identity of $\mathfrak{o}$, the element $e_{\Gamma/\Gamma'}e_1'$ acts as identity on ${}^{\Gamma'}G$ for any $e_{\Gamma/\Gamma'}\mathfrak{D}$-module G despite the fact that $e_{\Gamma/\Gamma'}e_1'$ is not even contained $e_{\Gamma/\Gamma'}\mathfrak{D}$ in general.

Remark 8.6. We can immediately see from Theorem 7.6 that Cl_{K/K_0}^S is naturally an $\mathfrak{o}$-module. This will be the key to our interpretation of (7.1).

Proof. If $\sigma e_1' = \tau e_1'$ with $\sigma, \tau \in e_{\Gamma/\Gamma'}\mathfrak{D}$, 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 have 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. $\qquad\square$

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 8.7. *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

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

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 $f\colon H_1 \to H_2$ of abelian groups is surjective if and only if

$$f_p\colon H_{1,p} \to H_{2,p}$$

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

$$\hat{f}_p\colon \hat{H}_{1,p} \to \hat{H}_{2,p}$$

is surjective where $\hat{f}_p$ and $\hat{H}_{i,p}$ denote the completion at p.

Since $\hat{\mathfrak{D}} := \mathfrak{D} \otimes_{\mathbb{Z}_S} \mathbb{Z}_p$ is a maximal $\mathbb{Z}_p$-order in $\mathbb{Q}_p[\Gamma]$ (see [43, 11.6]) and $\hat{\mathfrak{o}} := \mathfrak{o} \otimes_{\mathbb{Z}_S} \mathbb{Z}_p$ is the same as $^{\Gamma'}(e_{\Gamma/\Gamma'}\hat{\mathfrak{D}}e_1')$, the results above go through similarly. In particular, the additive subgroup $^{\Gamma'}(e_{\Gamma/\Gamma'}\hat{\mathfrak{D}})$ of $e_{\Gamma/\Gamma'}\hat{\mathfrak{D}}$ is a left $\hat{\mathfrak{o}}$-module by the analogue of Lemma 8.4, hence an $(\hat{\mathfrak{o}}, e_{\Gamma/\Gamma'}\hat{\mathfrak{D}})$-bimodule. So we can reduce the problem to proving

$$\hat{\psi}_p\colon {}^{\Gamma'}(e\hat{\mathfrak{D}}) \otimes_{e\hat{\mathfrak{D}}} \hat{G} \to {}^{\Gamma'}\hat{G}$$

is surjective for all $p \in S$.

By abuse of notation, let $\mathfrak{D}$ be a maximal $\mathbb{Z}_p$-order in $\mathbb{Q}_p[\Gamma]$ with p a good prime for $e_{\Gamma/\Gamma'}$, and let $\mathfrak{o} := {}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{D}e_1')$ just like above. Let $e\mathbb{Q}_p[\Gamma] \cong M_l(D)$ be an isomorphism such that $e\mathfrak{D} \cong M_l(\mathfrak{o})$ where D is a division algebra over $\mathbb{Q}_p$ and $\mathfrak{o} \subseteq D$ is the unique maximal $\mathbb{Z}_p$-order in D with the unique two-sided maximal ideal $\mathfrak{p}$, c.f. [43, (12.8), (17.3)]. Then the finitely generated $e\mathfrak{D}$-module G admits the following matrix representation:

$$G \cong \begin{pmatrix} \mathfrak{o} & \cdots & \mathfrak{o} \\ \mathfrak{o} & \cdots & \mathfrak{o} \\ \vdots & \vdots & \vdots \\ \mathfrak{o} & \cdots & \mathfrak{o} \end{pmatrix}_{l\times m} \oplus \begin{pmatrix} \mathfrak{o}/\mathfrak{p}^{r_1} & \mathfrak{o}/\mathfrak{p}^{r_2} & \cdots & \mathfrak{o}/\mathfrak{p}^{r_n} \\ \mathfrak{o}/\mathfrak{p}^{r_1} & \mathfrak{o}/\mathfrak{p}^{r_2} & \cdots & \mathfrak{o}/\mathfrak{p}^{r_n} \\ \vdots & \vdots & \vdots & \vdots \\ \mathfrak{o}/\mathfrak{p}^{r_1} & \mathfrak{o}/\mathfrak{p}^{r_2} & \cdots & \mathfrak{o}/\mathfrak{p}^{r_n} \end{pmatrix}_{l\times n}$$

$$= \left(M_{l\times 1}(\mathfrak{o})\right)^m \oplus M_{l\times 1}(\mathfrak{o}/\mathfrak{p}^{r_1}) \oplus \cdots \oplus M_{l\times 1}(\mathfrak{o}/\mathfrak{p}^{r_n}),$$

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

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

via $e\mathbb{Q}_p[\Gamma] \cong M_l(D)$. There exists a surjective morphism $\pi\colon e\mathfrak{D} \to G$ given by the composition of $e\mathfrak{D} \to \mathfrak{D}f$ defined by $x \mapsto xf$ and the quotient map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p}^r$.

Since $e\mathfrak{O}$ is projective, by Lemma 7.9, 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

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

This proves the surjectivity of ψ, hence the lemma. $\qquad\square$

Lemma 8.8. *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 $exe_1' \otimes y \mapsto exe_1'y$, 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 8.7, 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 $e\mathfrak{O} \cong M_l(\mathfrak{o})$ under the isomorphism where $\mathfrak{o} \subseteq D$ 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 $\mathfrak{o}$ 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 $e\mathfrak{O} = M_l(\mathfrak{o})$ as a $(e\mathfrak{O}, e\mathfrak{O})$-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. $\qquad\square$

We finally have the following.

Theorem 8.9. *The category of $e_{\Gamma/\Gamma'}\mathfrak{O}$-modules and the category of $\mathfrak{o}$-modules are Morita equivalent via the functors:*

$$^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O}) \otimes_{e_{\Gamma/\Gamma'}\mathfrak{O}} -: e_{\Gamma/\Gamma'}\mathfrak{O}-\mathrm{Mod} \to \mathfrak{o}-\mathrm{Mod},$$

$$e_{\Gamma/\Gamma'}\mathfrak{O}e_1' \otimes_{\mathfrak{o}} -: \mathfrak{o}-\mathrm{Mod} \to e_{\Gamma/\Gamma'}\mathfrak{O}-\mathrm{Mod}.$$

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.

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

Then,

$$\left\{ e_{\Gamma/\Gamma'}\mathfrak{O}, \mathfrak{o}, {}_{\mathfrak{o}}\!\left({}^{\Gamma'}(e_{\Gamma/\Gamma'}\mathfrak{O})\right)_{e_{\Gamma/\Gamma'}\mathfrak{O}}, e_{\Gamma/\Gamma'}\mathfrak{O}\left(e_{\Gamma/\Gamma'}\mathfrak{O}e_1'\right)_{\mathfrak{o}}, (,), [,] \right\}$$

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 8.8. 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 8.7. Then the equivalence and the functors are given by Morita theorem (see [12, Theorem 3.54]) directly. $\qquad\square$

Corollary 8.10. *The $\mathbb{Z}_S$-order $\mathfrak{o}$ in $e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1'$ is a maximal order.*

Proof. By [43, 11.6], it suffices to show that $\hat{\mathfrak{o}}_p = \mathfrak{o} \otimes_{\mathbb{Z}_S} \mathbb{Z}_p$ 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 8.7 (i.e. $\mathfrak{O} := \hat{\mathfrak{O}}$ and $\mathfrak{o} := \hat{\mathfrak{o}}$).

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 8.3). By [43, 39.14], if $ee_1'\mathfrak{o}$ is a hereditary order in $ee_1'A'$, then it is of the form

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

where $\mathfrak{o} \subseteq D$ 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 [43, 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 $M_{l'}(\mathfrak{o})$, and it is a maximal order of ee'_1A' again by [43, 17.3]. The argument holds for all ee'_1, hence $\mathfrak{o}$ is a maximal order of A'. $\square$

8.2. Random $\mathfrak{o}$-module. From (7.1), 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

$$X = X\big(e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma], \underline{u}, e_{\Gamma/\Gamma'}\mathfrak{O}\big)$$

defined in Section 3.2 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 $e'_1 e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1$, we can also define a random $\mathfrak{o}$-module

$$Y = \big(e'_1 e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1, \underline{v}, \mathfrak{o}\big)$$

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 8.11. *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*

$$X = X\big(e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma], \underline{u}, e_{\Gamma/\Gamma'}\mathfrak{O}\big) \quad \text{and} \quad Y = Y\big(e'_1 e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e'_1, \underline{v}, \mathfrak{o}\big)$$

with $\underline{u}, \underline{v} \in \mathbb{Q}^{k-1}$ so that u_i corresponds to e_i and v_i corresponds to $e_i e'_1$ 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

$$X \cong e_{\Gamma/\Gamma'} \mathfrak{D} e_1' \otimes_\mathfrak{o} H,$$

by Theorem 8.9. Therefore, for any two finite $\mathfrak{o}$-modules H_1, H_2, let

$$G_i := e_{\Gamma/\Gamma'} \mathfrak{D} e_1' \otimes_\mathfrak{o} H_i$$

for $i = 1, 2$, and we have

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

Given any finite $\mathfrak{o}$-module H, let $G := e_{\Gamma/\Gamma'} \mathfrak{D} e_1' \otimes H$ be the finite $e_{\Gamma/\Gamma'} \mathfrak{D}$-module such that $^{\Gamma'} G \cong H$. By [11, Theorem 7.3], for each $i = 2, \ldots, k$, there exists some finite $\mathbb{Z}_S$-module G_i such that

$$e_i G \cong G_i^{\langle \chi_i, a_\Gamma \rangle} \quad \text{and} \quad e_i e_1' H = {}^{\Gamma'}(e_i G) \cong G_i^{\langle \chi_i, a_{\Gamma/\Gamma'} \rangle}, \tag{8.1}$$

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

$$|e_i G| = |e_i e_1' H|^{\langle \chi_i, a_\Gamma \rangle / \langle \chi_i, a_{\Gamma/\Gamma'} \rangle}. \tag{8.2}$$

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 $e_{\Gamma/\Gamma'} \mathfrak{D}$-modules G_1, G_2 such that $H_i := {}^{\Gamma'} G_i$ with $i = 1, 2$. Then the identities (8.1) 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 $i = 2, \ldots, k$. $\qquad \square$

Definition 8.12. 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 8.11 to be the rank of $L^{\Gamma'}/K_0$. (In Section 9 we show this does not depend on L, but only $L^{\Gamma'}$.)

Just like in Section 4, we can express $|H|^{\underline{v}}$ in terms of the decomposition groups Γ_v at infinite places $v|\infty$.

Corollary 8.13. *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*

$$|H|^{\underline{v}} = |e_{\Gamma/\Gamma'}\mathfrak{D}e_1' \otimes_{\mathfrak{o}} H|^{\underline{u}} = \prod_{v|\infty} |(e_{\Gamma/\Gamma'}\mathfrak{D}e_1' \otimes_{\mathfrak{o}} H)^{\Gamma_v}|,$$

where v runs over all infinite places of K_0.

Proof. This is the combination of Theorem 8.11 and Theorem 4.1. □

By Theorem 8.11, 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 8.14. *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*

$$Y = Y\left(e_1'e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1', \underline{v}, \mathfrak{o}\right)$$

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 7.2 for $f(^{\Gamma'}-)$ and $e = e_{\Gamma/\Gamma'}$) implies that

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

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

In particular, the results of Section 6 all apply here to give the moments of the predicted distributions and see that the distributions are determined by their moments.

Remark 8.15. The probabilities in Theorem 8.14 are

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

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 (7.1) 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 5 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 $e_{\Gamma/\Gamma'}\mathrm{Cl}_L^S$.

8.3. 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 8.11. 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 8.3 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 8.16. *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 8.17 ($a_{\Gamma/\Gamma'}$ 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 8.10, 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 8.11 that $v_i = r_K l_i$, where r_K is the number of infinite places of K.

Example 8.18 (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 4.1. Since $a_{\Gamma/\Gamma'}$ is absolutely irreducible with $a_{\Gamma/\Gamma'}(23\cdots(n-1)) = 1$, we have

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

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 8.11 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 $|H|^{-(n-1)}|\mathrm{Aut}(H)|^{-1}$ as Cl_K^S.

Example 8.19 (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 4.1).

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

$$X = \left(e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma], \underline{1}, e_{\Gamma/\Gamma'}\mathfrak{O}\right),$$

and let G be a finite $e_{\Gamma/\Gamma'}\mathfrak{O}$-module, and $H = {}^{\Gamma'}G$. Then,

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

Then using (8.2), we have

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

Example 8.20 (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 8.9, 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.

9. Independence of Galois fields

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 9.1. *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 $\overline{e}_1$ 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 $(1-\overline{e}_1)\mathbb{Q}[\Gamma/\Gamma']$.

Theorem 9.2. *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 $\widetilde{\underline{v}}$ 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

$$e'_1 := \frac{1}{|\Gamma'|} \sum_{\gamma \in \Gamma'} \gamma, \quad E'_1 := \frac{1}{|\Sigma'|} \sum_{\sigma \in \Sigma'} \sigma.$$

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 9.1, we have

$$E'_1 \mathbb{Q}[\Sigma] E'_1 = E'_1 F_1 \mathbb{Q}[\Sigma] E'_1 = \frac{1}{|\Sigma'|} \sum_{\sigma \in \Sigma'} \sigma \cdot \mathbb{Q}[\Sigma/\Delta] E'_1$$

$$= \frac{1}{|\Sigma'/\Delta|} \sum_{\sigma \Delta \in \Sigma'/\Delta} \sigma \Delta \cdot \mathbb{Q}[\Sigma/\Delta] E'_1 \cong e'_1 \mathbb{Q}[\Gamma] e'_1.$$

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 9.1,

$$\mathbb{Q}[\Gamma] \cong (E_1 + E_{\Sigma/\Delta})\mathbb{Q}[\Sigma],$$

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 9.1,

$$E_{\Sigma/\Delta}\mathbb{Q}[\Sigma] \cong (1 - e_1)\mathbb{Q}[\Gamma],$$

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 $E_i F_1 = e_i$ for all $i = 2, \ldots, m$.

Claim. $w_i = u_i$ for all $i = 2, \ldots, m$.

Proof of 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 4.1, we know that the claim is true. $\qquad\square$

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

$$Y = \left(e_1' e_{\Gamma/\Gamma'}\mathbb{Q}[\Gamma]e_1', \underline{v}, \mathfrak{o}\right)$$

does not depend on the choice of the Galois extension $M | K_0$ containing K. $\qquad\square$

References

[1] A. Bartel and H. W. Lenstra Jr., Commensurability of automorphism groups, *Compos. Math.*, **153** (2017), no. 2, 323–346. Zbl 1381.11105 MR 3705226

[2] A. Bartel and H. W. Lenstra Jr., On class groups of random number fields, *Proc. Lond. Math. Soc. (3)*, **121** (2020), no. 4, 927–953. Zbl 07242519 MR 4105790

[3] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math. (2)*, **162** (2005), no. 2, 1031–1063. Zbl 1159.11045 MR 2183288

[4] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains, Modeling the distribution of ranks, Selmer groups, and Shafarevich–Tate groups of elliptic curves, *Camb. J. Math.*, **3** (2015), no. 3, 275–321. Zbl 1329.14071 MR 3393023

[5] N. Boston and M. M. Wood, Non-abelian Cohen–Lenstra heuristics over function fields, *Compos. Math.*, **153** (2017), no. 7, 1372–1390. Zbl 1390.11093 MR 3705261

[6] G. Chinta, N. Kaplan, and S. Koplewitz, The cotype zeta function of $\mathbb{Z}^d$, 2017. arXiv:1708.08547

[7] J. Clancy, N. Kaplan, T. Leake, S. Payne, and M. M. Wood, On a Cohen–Lenstra heuristic for Jacobians of random graphs, *J. Algebraic Combin.*, **42** (2015), no. 3, 701–723. Zbl 1325.05146 MR 3403177

[8] J. Clancy, T. Leake, and S. Payne, A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs, *Exp. Math.*, **24** (2015), no. 1, 1–7. Zbl 1310.05121 MR 3305035

[9] H. Cohen and H. W. Lenstra Jr., Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, 33–62, Lecture Notes in Math., 1068, Springer, Berlin, 1984. Zbl 0558.12002 MR 756082

[10] H. Cohen and J. Martinet, Class groups of number fields: numerical heuristics, *Math. Comp.*, **48** (1987), no. 177, 123–137. Zbl 0627.12006 MR 866103

[11] H. Cohen and J. Martinet, Étude heuristique des groupes de classes des corps de nombres, *J. Reine Angew. Math.*, **404** (1990), 39–76. Zbl 0699.12016 MR 1037430

[12] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*. With applications to finite groups and orders. Reprint of the 1981 original. Wiley Classics Library, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1990. Zbl 0698.20001 MR 1038525

[13] B. Datskovsky and D. J. Wright, Density of discriminants of cubic extensions, *J. Reine Angew. Math.*, **386** (1988), 116–138. Zbl 0632.12007 MR 936994

[14] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields. II, *Proc. Roy. Soc. London Ser. A*, **322** (1971), no. 1551, 405–420. Zbl 0212.08101 MR 491593

[15] C. Delaunay, Heuristics on Tate–Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$, *Experiment. Math.*, **10** (2001), no. 2, 191–196. Zbl 1045.11038 MR 1837670

[16] C. Delaunay and F. Jouhet, The Cohen–Lenstra heuristics, moments and p^j-ranks of some groups, *Acta Arith.*, **164** (2014), no. 3, 245–263. Zbl 1306.11088 MR 3238116

[17] N. M. Dunfield and W. P. Thurston, Finite covers of random 3-manifolds, *Invent. Math.*, **166** (2006), no. 3, 457–521. Zbl 1111.57013 MR 2257389

[18] J. S. Ellenberg, A. Venkatesh, and C. Westerland, Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields, *Ann. of Math. (2)*, **183** (2016), no. 3, 729–786. Zbl 1342.14055 MR 3488737

[19] É. Fouvry and J. Klüners, Cohen–Lenstra heuristics of quadratic number fields, in *Algorithmic number theory*, 40–55, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006. Zbl 1143.11352 MR 2282914

[20] É. Fouvry and J. Klüners, On the 4-rank of class groups of quadratic number fields, *Invent. Math.*, **167** (2007), no. 3, 455–513. Zbl 1126.11062 MR 2276261

[21] J. Fulman, A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups, *J. Algebra*, **212** (1999), no. 2, 557–590. Zbl 0980.20036 MR 1676854

[22] J. Fulman, Cohen–Lenstra heuristics and random matrix theory over finite fields, *J. Group Theory*, **17** (2014), no. 4, 619–648. Zbl 1336.60013 MR 3228936

[23] J. Fulman, Hall–Littlewood polynomials and Cohen–Lenstra heuristics for Jacobians of random graphs, *Ann. Comb.*, **20** (2016), no. 1, 115–124. Zbl 1332.05127 MR 3461939

[24] J. Fulman and N. Kaplan, Random partitions and Cohen–Lenstra heuristics, *Ann. Comb.*, **23** (2019), no. 2, 295–315. Zbl 1415.15034 MR 3962859

[25] D. Garton, Some finite abelian group theory and some q-series identities, *Ann. Comb.*, **20** (2016), no. 2, 361–371. Zbl 1405.11020 MR 3505324

[26] K. W. Gruenberg and A. Weiss, Capitulation and transfer kernels, *J. Théor. Nombres Bordeaux*, **12** (2000), no. 1, 219–226. Zbl 1009.11061 MR 1827849

[27] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem. II. With an appendix by P. Monsky, *Invent. Math.*, **118** (1994), no. 2, 331–370. Zbl 0815.11032 MR 1292115

[28] D. Hilbert, *The theory of algebraic number fields*. Translated from the German and with a preface by Iain T. Adamson. With an introduction by Franz Lemmermeyer and Norbert Schappacher, Springer-Verlag, Berlin, 1998. Zbl 0984.11001 MR 1646901

[29] M. Kahle, F. Lutz, A. Newman, and K. Parsons, Cohen–Lenstra heuristics for torsion in homology of random complexes, *Exp. Math.*, **29** (2020), no. 3, 347–359. Zbl 07330691 MR 4134833

[30] S. Koplewitz, Sandpile groups and the coeulerian property for random directed graphs, *Adv. in Appl. Math.*, **90** (2017), 145–159. Zbl 1366.05048 MR 3666713

[31] J. Lengler, A combinatorial interpretation of the probabilities of p-groups in the Cohen–Lenstra measure, *J. Number Theory*, **128** (2008), no. 7, 2070–2084. Zbl 1180.05125 MR 2423750

[32] J. Lengler, The Cohen–Lenstra heuristic: methodology and results, *J. Algebra*, **323** (2010), no. 10, 2960–2976. Zbl 1213.11167 MR 2609186

[33] M. Lipnowski, W. Sawin, and J. Tsimerman, Cohen–Lenstra heuristics and bilinear pairings in the presence of roots of unity, 2020. arXiv:2007.12533

[34] Y. Liu, M. M. Wood, and D. Zureick–Brown, A predicted distribution for Galois groups of maximal unramified extensions, 2019. Available at: http://www.math.wisc.edu/~mmwood/Publications/

[35] G. Malle, Cohen–Lenstra heuristic and roots of unity, *J. Number Theory*, **128** (2008), no. 10, 2823–2835. Zbl 1225.11143 MR 2441080

[36] G. Malle, On the distribution of class groups of number fields, *Experiment. Math.*, **19** (2010), no. 4, 465–474. Zbl 1297.11139 MR 2778658

[37] A. Mészáros, The distribution of sandpile groups of random regular graphs, *Trans. Amer. Math. Soc.*, **373** (2020), no. 9, 6529–6594. Zbl 07255586 MR 4155185

[38] P. Nguyen and I. Shparlinski, Counting co-cyclic lattices, *SIAM J. Discrete Math.*, **30** (2016), no. 3, 1358–1370. Zbl 1348.11056 MR 3521539

[39] H. H. Nguyen and M. M. Wood, Cokernels of adjacency matrices of random r-regular graphs, 2018. arXiv:1806.10068

[40] H. H. Nguyen and M. M. Wood, Random integral matrices: Universality of surjectivity and the cokernel, 2018. arXiv:1806.00596

[41] J. Park, B. Poonen, J. Voight, and M. M. Wood, A heuristic for boundedness of ranks of elliptic curves, *J. Eur. Math. Soc. (JEMS)*, **21** (2019), no. 9, 2859–2903. Zbl 07117722 MR 3985613

[42] L. B. Pierce, C. L. Turnage–Butterbaugh, and M. M. Wood, An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups, *Invent. Math.*, **219** (2020), no. 2, 701–778. Zbl 1445.11129 MR 4054810

[43] I. Reiner, *Maximal orders*. Corrected reprint of the 1975 original. With a foreword by M. J. Taylor, London Mathematical Society Monographs. New Series, 28, The Clarendon Press, Oxford University Press, Oxford, 2003. Zbl 1024.16008 MR 1972204

[44] A. Smith, 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture, 2017. arXiv:1702.02325

[45] R. P. Stanley, Smith normal form in combinatorics, *J. Combin. Theory Ser. A*, **144** (2016), 476–495. Zbl 1343.05026 MR 3534076

[46] H. Suzuki, A generalization of Hilbert's theorem 94, *Nagoya Math. J.*, **121** (1991), 161–169. Zbl 0728.11061 MR 1096472

[47] Y. Wang and R. Stanley, The Smith normal form distribution of a random integer matrix, *SIAM J. Discrete Math.*, **31** (2017), no. 3, 2247–2268. Zbl 1372.05006 MR 3706911

[48] M. M. Wood, On the probabilities of local behaviors in abelian field extensions, *Compos. Math.*, **146** (2010), no. 1, 102–128. Zbl 1242.11081 MR 2581243

[49] M. M. Wood, The distribution of sandpile groups of random graphs, *J. Amer. Math. Soc.*, **30** (2017), no. 4, 915–958. Zbl 1366.05098 MR 3671933

[50] M. M. Wood, Cohen–Lenstra heuristics and local conditions, *Res. Number Theory*, **4** (2018), no. 4, Paper No. 41, 22pp. Zbl 1441.11291 MR 3858473

[51] M. M. Wood, Random integral matrices and the Cohen–Lenstra heuristics, *Amer. J. Math.*, **141** (2019), no. 2, 383–398. Zbl 1446.11170 MR 3928040

W. Wang, Department of Mathematics, Harvard University,
Science Center Room 325, 1 Oxford Street, Cambridge, MA 02138, USA
E-mail: weitongwang@math.harvard.edu

M. M. Wood, Department of Mathematics, Harvard University,
Science Center Room 325, 1 Oxford Street, Cambridge, MA 02138, USA
E-mail: mmwood@math.harvard.edu