On class groups of random number fields

Alex Bartel and Hendrik W. Lenstra Jr.

Abstract

The main aim of this paper is to disprove the Cohen–Lenstra–Martinet heuristics in two different ways and to offer possible corrections. We also recast the heuristics in terms of Arakelov class groups, giving an explanation for the probability weights appearing in the general form of the heuristics. We conclude by proposing a rigorously formulated Cohen–Lenstra–Martinet conjecture.

Contents

1. Introduction

The Cohen–Lenstra–Martinet heuristics [5, 7] make predictions on the distribution of class groups of 'random' algebraic number fields. In this paper, we disprove the predictions in two different ways, and propose possible adjustments. In addition, we show that the heuristics can be equivalently formulated in terms of Arakelov class groups of number fields. This formulation has the merit of conforming to the general expectation that a random mathematical object is isomorphic to a given object A with a probability that is inversely proportional to $\#\mathrm{Aut}A$. We end by offering two rigorously formulated Cohen–Lenstra–Martinet conjectures. In particular, we give two possible precise definitions of the notion of a 'reasonable function' occurring in [5, 7]. The conjectures can likely be further sharpened and strengthened. We will be pointing out concrete avenues for further research throughout the paper.

The class group Cl_F of a number field F is in a natural way a module over $\mathrm{Aut}F$. Our first disproof of the heuristics proceeds by pointing out restrictions on the possible module structure that had not been taken into account. To explain this, recall that for a ring R, the Grothendieck group $\mathrm{G}(R)$ of the category of finitely generated R-modules has one generator

---

$[L]$ for every finitely generated R-module L, and one defining relation $[L] + [N] = [M]$ for every short exact sequence $0 \to L \to M \to N \to 0$ of finitely generated R-modules.

The rings R that we will mainly be interested in are certain group rings. For a set S of prime numbers, we write $\mathbb{Z}_{(S)} = \{a/b : a, b \in \mathbb{Z}, b \notin \bigcup_{p \in S \cup \{0\}} p\mathbb{Z}\}$, which is a subring of $\mathbb{Q}$. Let now G be a finite abelian group, and let S be a set of prime numbers not dividing $\#G$. Then if R is a quotient of the group ring $\mathbb{Z}_{(S)}[G]$, the torsion subgroup $\mathrm{G}(R)_{\mathrm{tors}}$ of $\mathrm{G}(R)$ may be identified with a product of class groups of certain cyclotomic rings. For example, if G is cyclic of prime order p, then $\mathrm{G}(\mathbb{Z}_{(S)}[G])_{\mathrm{tors}}$ is naturally isomorphic to the class group of $\mathbb{Z}_{(S)}[\zeta_p]$, where ζ_p denotes a primitive pth root of unity. For more details the reader may consult Section 4. Assume now that G has even order, and fix an element $c \in G$ of order 2. The ring that occurs in our first disproof of the heuristics is the ring $T^- = \mathbb{Z}_{(S)}[G]/(1 + c)$. Every finite T^--module represents a class in $\mathrm{G}(T^-)_{\mathrm{tors}}$. This applies, in particular, to the module $T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ if F is a number field whose Galois group is identified with G such that c acts as complex conjugation. As we will explain in Section 4, the Cohen–Lenstra–Martinet heuristics predict that if F runs through all such fields, the class of $T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ is equidistributed in $\mathrm{G}(T^-)_{\mathrm{tors}}$. We will argue that this stands in contradiction to the following theorem, which we will prove in Section 4 as a consequence of the Iwasawa Main Conjecture for abelian fields, as proven by Mazur–Wiles in [16].

If F is a number field, let μ_F denote the group of roots of unity in F.

THEOREM 1.1. *Let $F/\mathbb{Q}$ be a finite imaginary abelian extension, let G be its Galois group, let $c \in G$ denote complex conjugation, let S be a set of prime numbers not dividing $\#G$, and let $T^- = \mathbb{Z}_{(S)}[G]/(1 + c)$. Then we have $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F] = [T^- \otimes_{\mathbb{Z}[G]} \mu_F]$ in $\mathrm{G}(T^-)$.*

Theorem 1.1 is a variant of a result of Greither [11, Theorem 5.5], who obtained a stronger conclusion under some additional hypotheses.

One way of obtaining a contradiction between Theorem 1.1 and the Cohen–Lenstra–Martinet heuristics is as follows. Suppose that G is cyclic of order 58, and S consists of all prime numbers not dividing 58. Then $\mathrm{G}(T^-)_{\mathrm{tors}}$ is the class group of $\mathbb{Z}_{(S)}[\zeta_{29}]$, which is elementary abelian of order 8, and in Section 4 we will deduce from Theorem 1.1 that $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F]$ is trivial for all but one F, contradicting the equidistribution prediction of the heuristics. In the Cohen–Lenstra–Martinet conjecture that we propose below, we will remove this obstruction by requiring the set S to be finite, in which case one has $\mathrm{G}(T^-)_{\mathrm{tors}} = 0$. To formulate correct heuristics, or even conjectures, when S is not assumed to be finite remains an important problem, which we will turn to in a future paper.

Our second disproof indicates that enumerating fields by discriminant is fundamentally flawed in the context of Cohen–Lenstra–Martinet heuristics. The heuristics were initially formulated for number fields of degree 2. Degree 1 was skipped, since there is only one number field of degree 1; its class group is trivial, and does not obey a Cohen–Lenstra–Martinet law. For a similar reason we shall, in our reformulated conjecture, require that the class $\mathcal{F}$ of fields be infinite (see the introduction to Conjecture 1.5). If $\mathcal{F}$ were finite but non-empty, it would form a discrete probability space. In that case the distribution of the class groups of the fields in $\mathcal{F}$ would be influenced by the class group of each individual field in $\mathcal{F}$, and when that is the case one would generally not expect a Cohen–Lenstra–Martinet distribution. Also, the fact that $\mathbb{Q}$ has class number 1 affects other number fields, simply because they have $\mathbb{Q}$ as a subfield. Indeed, if F is a Galois number field, G is the Galois group, and S is a set of prime numbers not dividing $\#G$, then the subgroup of G-invariants of the group $\mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} \mathrm{Cl}_F$ equals $\mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} \mathrm{Cl}_{\mathbb{Q}}$ and is therefore trivial, not obeying a Cohen–Lenstra–Martinet law. Enumerating fields by discriminant may lead to a difficulty that, imprecisely speaking, is a combination of the two issues just outlined, namely it may induce a discrete probability distribution on subfields. We will now give a

concrete example of this situation, which suffices to disprove the Cohen–Lenstra–Martinet heuristics.

For a real number x, let $\mathcal{C}(x)$ be the set of cyclic quartic fields with discriminant at most x inside a fixed algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, and for a quadratic number field $k \subset \bar{\mathbb{Q}}$ let $\mathcal{C}_k(x) = \{F \in \mathcal{C}(x) : k \subset F\}$. A more precise version of the following result will be proven in Section 6 as Theorem 6.1.

THEOREM 1.2.   *For every quadratic field k, there exists a real number p_k satisfying $0 \leqslant p_k < 1$, computable to arbitrary precision, and such that:*

(i) *if the discriminant of k is either negative or has at least one prime divisor that is congruent to 3 (mod 4), then $p_k = 0$ and $\mathcal{C}_k(x)$ is empty for all real numbers x;*

(ii) *otherwise one has*

$$\lim_{x \to \infty} \frac{\#\mathcal{C}_k(x)}{\#\mathcal{C}(x)} = p_k > 0;$$

(iii) *one has $\sum_{k \subset \bar{\mathbb{Q}}} p_k = 1$, with the sum running over all quadratic number fields k.*

Thus, enumerating cyclic quartic fields by discriminant defines a discrete probability distribution on the quadratic subfields. A concrete counterexample to the Cohen–Lenstra–Martinet heuristics is obtained from this as follows. Let $\mathcal{C}'(x) \subset \mathcal{C}(x)$ be the subset of those $F \in \mathcal{C}(x)$ for which the class number of the quadratic subfield is not divisible by 3. Then, as we will explain in Section 6, the Cohen–Lenstra–Martinet heuristics predict that the limit $\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x)$ exists and that $\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x) \approx 0.8402$, where the notation $a \approx b$ means that a rounds to b with the given precision. However, in Theorem 6.2 we will deduce from Theorem 1.2 that the limit $\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x)$ does indeed exist, and one has

$$\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x) \approx 0.9914,$$

contradicting the heuristics.

We propose to use an order of enumeration that, by work of Wood [21], does not induce a discrete probability distribution on subfields when the Galois group is abelian, and is not expected to do so in the generality of our conjecture. Enumerating number fields by discriminant has also been observed to pose problems in the context of other questions in arithmetic statistics, which are not obviously related to the Cohen–Lenstra–Martinet heuristics (see, for example, [1, 21]). It would be interesting to classify all finite groups G such that enumerating G-extensions by discriminant exhibits the same bad behaviour as described above. More broadly, a type of question that we first heard from Wood is: which invariants of number fields with a given Galois structure are 'admissible' for the purposes of ordering number fields in the Cohen–Lenstra–Martinet heuristics?

Let us now discuss the shift of perspective towards Arakelov class groups. Let F be a number field. For the definition of the Arakelov class group Pic_F^0 of F, we refer to [20]. It may be compactly described as the cokernel of the natural map $\mathrm{c}(\mathrm{J}_F) \to \mathrm{c}(\mathrm{J}_F/F^{\times})$, where J_F denotes the idèle group of F (see [4]) and $\mathrm{c}(X)$ denotes the maximal compact subgroup of X; in particular, Pic_F^0 is a compact abelian group. We denote the Pontryagin dual of Pic_F^0 by Ar_F. It is an immediate consequence of [20, Proposition 2.2] that Ar_F is a finitely generated discrete abelian group that fits in a short exact sequence of $\mathrm{Aut}F$-modules

$$0 \to \mathrm{Hom}(\mathrm{Cl}_F, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Ar}_F \to \mathrm{Hom}(\mathcal{O}_F^{\times}, \mathbb{Z}) \to 0, \qquad (1.3)$$

where $\mathcal{O}_F$ denotes the ring of integers of F. Thus, knowing the torsion subgroup of Ar_F is equivalent to knowing Cl_F, and knowing its torsion-free quotient amounts to knowing $\mathcal{O}_F^{\times}$ modulo roots of unity.

The Arakelov class group of a number field is often better behaved than either the class group or the integral unit group. As an example of this phenomenon, we mention the following analogue of Theorem 1.1 for real abelian fields, which we will prove in Section 5, also relying on the results of Mazur–Wiles [**16**].

THEOREM 1.4. *Let $F/\mathbb{Q}$ be a finite real abelian extension, let G be its Galois group, let S be a set of prime numbers not dividing $2 \cdot \#G$, and let $T = \mathbb{Z}_{(S)}[G]$. Then we have the equality $[T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F] = [T] - [\mathbb{Z}_{(S)}]$ in $\mathrm{G}(T)$, where $[\mathbb{Z}_{(S)}]$ denotes the class of $\mathbb{Z}_{(S)}$ with the trivial G-action.*

As we will explain in Section 5, this theorem expresses that the class of $T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$ in $\mathrm{G}(T)$ is 'as trivial as it can be', given the $\mathbb{Q}[G]$-module structure of $\mathbb{Q}[G] \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$. There is no reason to believe that an analogous result holds for either of the other two terms in the exact sequence (1.3).

We also reinterpret Theorems 1.1 and 1.4 in terms of the so-called oriented Arakelov class group, a notion that was introduced by Schoof in [**20**] and of which we recall the definition in Section 5. That reinterpretation results in a uniform statement for both theorems — see Theorem 5.4 — and moreover in a statement that might conceivably hold for arbitrary finite Galois extensions and that should point the way towards relaxing the assumption in Conjecture 1.5 that S be finite. We intend to take up this theme in a forthcoming paper.

Above we mentioned the principle that, if a mathematical object is 'randomly' drawn, a given object appears with a probability that is inversely proportional to the order of its automorphism group. In the context of Arakelov class groups, however, the relevant automorphism groups are typically of infinite order. In [**2**], we overcame this obstacle to applying the principle by means of an algebraic theory, the consequences of which we now explain.

Let G be a finite group, and let A be a quotient of the group ring $\mathbb{Q}[G]$ by some two-sided ideal. If p is a prime number and $S = \{p\}$, then we write $\mathbb{Z}_{(p)}$ for $\mathbb{Z}_{(S)}$. We say that a prime number p is *good for A* if there is a direct product decomposition $\mathbb{Z}_{(p)}[G] = J \times J'$, where J is a maximal $\mathbb{Z}_{(p)}$-order in A, and the quotient map $\mathbb{Z}_{(p)}[G] \to A$ equals the projection $\mathbb{Z}_{(p)}[G] \to J$ composed with the inclusion $J \to A$. For example, all prime numbers p not dividing $\#G$ are good for all quotients of $\mathbb{Q}[G]$. Let S be a set of prime numbers that are good for A, and let R denote the image of $\mathbb{Z}_{(S)}[G]$ in A. Let $\mathcal{M}$ be a set of finite R-modules with the property that for every finite R-module M' there is a unique $M \in \mathcal{M}$ such that $M \cong M'$, and let $\mathcal{P}$ be a set of finitely generated projective R-modules such that for every finitely generated projective R-module P' there is a unique $P \in \mathcal{P}$ such that $P \cong P'$. Note that $\mathcal{M}$ and $\mathcal{P}$ are countable sets.

Assume for the rest of the introduction that S is finite. As we will show in Section 3, it follows from our hypotheses that for every finitely generated A-module V, there is a unique $P_V \in \mathcal{P}$ such that $A \otimes_R P_V \cong_A V$; and that moreover for every finitely generated R-module M satisfying $A \otimes_R M \cong_A V$, there exists a unique module $M_0 \in \mathcal{M}$ such that $M \cong P_V \oplus M_0$. For a finitely generated A-module V, we define $\mathcal{M}_V = \{P_V \oplus M_0 : M_0 \in \mathcal{M}\}$.

Let V be a finitely generated A-module. In Section 3, we will deduce from [**2**] that there is a unique discrete probability measure $\mathbb{P}$ on $\mathcal{M}_V$ with the property that for any isomorphism $L \oplus E \cong M$ of R-modules, where L and M are in $\mathcal{M}_V$, and E is finite, we have

$$\mathbb{P}(L) = (\mathrm{Aut}\, M : \mathrm{Aut}\, L) \cdot \mathbb{P}(M),$$

where the inclusion $\mathrm{Aut}\, L \subset \mathrm{Aut}\, M$ is the obvious one. This condition expresses that one can think of $\mathbb{P}(M)$ as being proportional to $1/\#\mathrm{Aut}\, M$.

We will now formulate an incomplete version of our conjecture on distributions of Arakelov class groups, leaving the discussion of the crucial missing detail, the notion of a 'reasonable' function, to Section 7. If f is a complex valued function on $\mathcal{M}_V$, then we define the expected value of f to be the sum $\mathbb{E}(f) = \sum_{M \in \mathcal{M}_V} (f(M) \cdot \mathbb{P}(M))$ if the sum converges absolutely.

Let G, A, S, R, and V be as above, and assume that $\sum_{g \in G} g = 0$ in A. Let K be a number field, let $\bar{K}$ be an algebraic closure of K, and let $\mathcal{F}$ be the set of all pairs (F, ι), where $F \subset \bar{K}$ is a Galois extension of K that contains no primitive pth root of unity for any prime $p \in S$, and ι is an isomorphism between the Galois group of F/K and G that induces an isomorphism $A \otimes_{\mathbb{Z}[G]} \mathcal{O}_F^{\times} \cong V$ of A-modules. Assume that $\mathcal{F}$ is infinite. For all $(F, \iota) \in \mathcal{F}$, we will view Ar_F as a G-module via the isomorphism ι. Let $(F, \iota) \in \mathcal{F}$ be arbitrary. It follows from the exact sequence (1.3) that we have an isomorphism $A \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F \cong \mathrm{Hom}(V, \mathbb{Q})$ of A-modules. Moreover, every finitely generated $\mathbb{Q}[G]$-module is isomorphic to its $\mathbb{Q}$-linear dual (see, for example, [8, §10D]), so we have an isomorphism $\mathrm{Hom}(V, \mathbb{Q}) \cong V$ of A-modules. Thus, $R \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$ is isomorphic to a unique element of $\mathcal{M}_V$.

If F/K is a finite extension, let $c_{F/K}$ be the ideal norm of the product of the prime ideals of $\mathcal{O}_K$ that ramify in F/K. For a positive real number B, let $\mathcal{F}_{c \leqslant B} = \{(F, \iota) \in \mathcal{F} : c_{F/K} \leqslant B\}$. If M is a finitely generated R-module satisfying $A \otimes_R M \cong_A V$, and f is a function defined on $\mathcal{M}_V$, then we write $f(M)$ for the value of f on the unique element of $\mathcal{M}_V$ that is isomorphic to M.

CONJECTURE 1.5. Let f be a 'reasonable' complex valued function on $\mathcal{M}_V$. Then the limit

$$\lim_{B \to \infty} \frac{\sum_{(F, \iota) \in \mathcal{F}_{c \leqslant B}} f(R \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F)}{\#\mathcal{F}_{c \leqslant B}}$$

exists, and is equal to $\mathbb{E}(f)$.

For any $(F, \iota) \in \mathcal{F}$, the assumption that S only contain prime numbers that are good for A implies that the short exact sequence of R-modules that one obtains by applying the functor $R \otimes_{\mathbb{Z}[G]} \bullet$ to the exact sequence (1.3) splits, so that the isomorphism class of the R-module $R \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$ is determined by those of $R \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ and of $R \otimes_{\mathbb{Z}[G]} \mathcal{O}_F^{\times}$. Moreover, the additional assumption that S be finite implies that the isomorphism class of $R \otimes_{\mathbb{Z}[G]} \mathcal{O}_F^{\times}$ is determined by the isomorphism class of the A-module $A \otimes_{\mathbb{Z}[G]} \mathcal{O}_F^{\times}$, and in particular is constant as $(F, \iota) \in \mathcal{F}$ varies. Thus, for all $(F, \iota) \in \mathcal{F}$ the isomorphism class of $R \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$ carries precisely the same information as the isomorphism class of $R \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$.

In order to allow the reader to compare our conjecture with the Cohen–Lenstra–Martinet heuristics, we will prove in Section 3 that the probability distribution $\mathbb{P}_V$ on $\mathcal{M}$ that $\mathbb{P}$ induces on the set of $\mathbb{Z}_{(S)}$-torsion submodules of $M \in \mathcal{M}_V$ satisfies, for all L_0, $M_0 \in \mathcal{M}$,

$$\frac{\mathbb{P}_V(L_0)}{\mathbb{P}_V(M_0)} = \frac{\#\mathrm{Hom}(P_V, M_0) \cdot \#\mathrm{Aut}(M_0)}{\#\mathrm{Hom}(P_V, L_0) \cdot \#\mathrm{Aut}(L_0)}.$$

The distribution $\mathbb{P}_V$ is, in fact, the probability distribution that is used in the original Cohen–Lenstra–Martinet heuristics, a version of which we will give in Section 2. In other words, the probability distribution that we postulate on Ar_F recovers, and explains, the probability distribution of Cohen–Lenstra–Martinet on Cl_F. The main differences between our conjecture and the original heuristic are: the hypothesis that S be finite; and the changed ordering on $\mathcal{F}$.

In substance, there is only one piece of theoretical evidence for Conjecture 1.5 that we are aware of, which also appears to be the only piece of evidence for the original conjecture. It is the work of Davenport–Heilbronn [10], as generalised by Datskovsky–Wright [9], which implies that Conjecture 1.5 holds if G has order 2, and f is the function $f(M) = \#(M/3M)$. The theorem actually addresses the average of the function f when the quadratic extensions are enumerated by ideal norm of the relative discriminant rather than of the product of ramified primes, but also shows that the average is unchanged if one restricts to quadratic extensions with prescribed local behaviour at the primes above 2 — see also [3, Corollary 4] for the special case $K = \mathbb{Q}$. It is not hard to deduce from this refined statement that Conjecture 1.5 itself also holds for this choice of G and f.

As for computational evidence, in almost all large scale computational data for Cohen–Lenstra–Martinet related questions assembled to date that we are aware of fields are enumerated by the absolute value of their discriminant, as in the original heuristics. It would be desirable to have a large body of computational data, not only for Conjecture 1.5, but also for variants with other orders of enumeration that do not suffer from the problem pointed out in this paper.

We conclude the introduction by discussing the notion of a 'reasonable function'. It already appears in the original heuristics of Cohen–Lenstra [5] and Cohen–Martinet [7], but has never been made precise. In order to turn the heuristics into actual conjectures, with a truth value, we will offer two possible definitions of this notion in Section 7.

Of course, the minimal requirement that a function f has to fulfil in order to satisfy the conclusion of Conjecture 1.5 is that the expected value $\mathbb{E}(f)$ should exist. It may be tempting to conjecture that, at least for $\mathbb{R}_{\geqslant 0}$-valued functions f, this minimal condition is in fact sufficient. However, the following result, which we will prove as Theorem 7.1, using a construction communicated to us by Bjorn Poonen, shows that the conjecture is likely false in that generality.

THEOREM 1.6.   *Let X be a countably infinite set, and let p be a discrete probability measure on X. For all $x \in X$, abbreviate $p(\{x\})$ to $p(x)$ and assume that $p(x) > 0$. Let B be the subset of $X^{\mathbb{Z}_{\geqslant 1}}$ consisting of those sequences $(y_i)_{i \in \mathbb{Z}_{\geqslant 1}} \in X^{\mathbb{Z}_{\geqslant 1}}$ for which there exists a function $f \colon X \to \mathbb{R}_{\geqslant 0}$ such that:*

(i) the expected value $\sum_{x \in X} f(x)p(x)$ is finite, but
(ii) the limit $\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} f(y_i)$ does not exist in $\mathbb{R}$.

Then the measure of B with respect to the product measure induced by p on $X^{\mathbb{Z}_{\geqslant 1}}$ is equal to 1.

Theorem 1.6 suggests that if the sequence of dual Arakelov class groups really were a random sequence with probability measure $\mathbb{P}$, then with probability 1 there would be a function f for which $\mathbb{E}(f)$ exists but the conclusion of Conjecture 1.5 is violated, and such functions f should therefore not be considered 'reasonable'.

One of our two ways of narrowing down the class of reasonable functions is to require, in Conjecture 7.3, that for all $j \in \mathbb{Z}_{\geqslant 1}$ the jth moment of $|f|$ be finite. In Question 7.4, we raise the probability-theoretic problem of showing that this additional requirement suffices to eliminate the difficulty mentioned. In our second proposal, in Conjecture 7.6, we take a completely different, computer science perspective.

2.   *The Cohen–Lenstra–Martinet heuristics*

In this section, we give a version of the heuristics of Cohen–Lenstra and Cohen–Martinet. Our formulation differs from the original one in several ways, as we will point out, but does not yet incorporate the corrections that will be necessary in light of the results of Sections 4 and 6.

Let G be a finite group, let A be a quotient of the group ring $\mathbb{Q}[G]$ by some two-sided ideal that contains $\sum_{g \in G} g$, let S be a set of prime numbers that are good for A, let R be the image of $\mathbb{Z}_{(S)}[G]$ in A under the quotient map, let P be a finitely generated projective R-module, and let V denote the A-module $A \otimes_R P$. Let $\mathcal{M}$ be as in the introduction. If $\mathbf{B} = (B_{A'})_{A'}$ is a sequence of real numbers indexed by the simple quotients A' of A, then let $\mathcal{M}_{\leqslant \mathbf{B}}$ be the set of all $M \in \mathcal{M}$ such that for every simple quotient A' of A we have $\#(R' \otimes_R M) \leqslant B_{A'}$, where R' denotes the image of R in A'. We will write $\mathbf{B} \to \infty$ to mean $\min_{A'} B_{A'} \to \infty$.

If f is a function on $\mathcal{M}$, and M is a finite R-module, then we will write $f(M)$ for the value of f on the unique element of $\mathcal{M}$ that is isomorphic to M. For a finite module M, define $w_P(M) = \frac{1}{\#\mathrm{Hom}(P,M)\cdot\#\mathrm{Aut}\,M}$.

Let K be a number field, let $\bar{K}$ be an algebraic closure of K, and let $\mathcal{F}$ be the set of all pairs (F,ι), where $F \subset \bar{K}$ is a Galois extension of K that contains no primitive pth root of unity for any prime $p \in S$, and ι is an isomorphism between the Galois group of F/K and G that induces an isomorphism $A \otimes_{\mathbb{Z}[G]} \mathcal{O}_F^\times \cong V$ of A-modules. If (F,ι) is in $\mathcal{F}$, then the class group Cl_F is naturally a G-module via the isomorphism ι. Let $\Delta_{F/K}$ denote the ideal norm of the relative discriminant of F/K. For a positive real number B, let $\mathcal{F}_{\Delta\leqslant B} = \{(F,\iota) \in \mathcal{F} : \Delta_{F/K} \leqslant B\}$.

HEURISTIC 2.1 (Cohen–Lenstra–Martinet heuristics). With the above notation, assume that $\mathcal{F}$ is infinite, and let f be a 'reasonable' $\mathbb{C}$-valued function on $\mathcal{M}$. Then:

(a) the limit

$$\lim_{B\to\infty} \frac{\sum_{(F,\iota)\in\mathcal{F}_{\Delta\leqslant B}} f(R \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F)}{\#\mathcal{F}_{\Delta\leqslant B}} \tag{2.2}$$

exists;
(b) the limit

$$\lim_{\mathbf{B}\to\infty} \frac{\sum_{M\in\mathcal{M}_{\leqslant\mathbf{B}}} w_P(M)f(M)}{\sum_{M\in\mathcal{M}_{\leqslant\mathbf{B}}} w_P(M)} \tag{2.3}$$

exists;
(c) the two limits (2.2) and (2.3) are equal.

The notion of a 'reasonable' function was left undefined in [5] and [7], and has never been made precise.

Let us briefly highlight some of the differences between Heuristic 2.1 and [7, Hypothesis 6.6].

While Cohen–Martinet assume that the families of fields under consideration are non-empty, we assume in Heuristic 2.1 that $\mathcal{F}$ is infinite. If $\mathcal{F}$ was finite, then Heuristic 2.1 would almost certainly be false for any reasonable interpretation of the word 'reasonable', so we avoid dependencies on some form of the inverse Galois problem.

The original heuristics did not include the condition that the fields F should not contain a primitive pth root of unity for any $p \in S$. However, work by Malle [15] suggests that if that condition was omitted, then for those primes p that do divide the order of the group of roots of unity of F for a positive proportion of all $(F,\iota) \in \mathcal{F}$, the probability measure governing the p-primary parts of the class groups would likely need to be modified.

Considering pairs (F,ι) consisting of a number field and an isomorphism between its Galois group and G, as in Heuristic 2.1, is one way of making precise the original formulations of Cohen–Lenstra and Cohen–Martinet, who speak of the family of extensions of K 'with Galois group G'. In the above formulation, some concrete conjectures of [6] become trivially true. An example of this is [6, (2)(a)], where it is conjectured that if C_3 is a cyclic group of order 3, then among Galois number fields with Galois group isomorphic to C_3 and with class number 7, each of the two isomorphism classes of non-trivial C_3-modules of order 7 appears with probability 50%. We do not know how to make the notion of a family of fields 'with Galois group G' precise in a natural way that would render this and similar examples well defined, but not trivial.

In [7, Hypothesis 6.6], the analogue of the expected value (2.3), which is denoted by $M_u^S(f)$ there, is defined as a sum over representatives of isomorphism classes of all finite $\mathcal{O}$-modules, where $\mathcal{O}$ is a maximal $\mathbb{Z}$-order of $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$. This differs in two ways from Heuristic 2.1.

Firstly, in that version the sums that are analogous to the numerator and denominator of expression (2.3) contain summands corresponding to modules M whose order is divisible by primes not in S, even when $f(M)$ depends only on the isomorphism class of $\mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} M$. It can be easily deduced from [5, Proposition 5.6] that this is a purely cosmetic difference. In particular, one can show that if S' is a subset of S, and $f(M)$ only depends on the isomorphism class of $\mathbb{Z}_{(S')} \otimes_{\mathbb{Z}_{(S)}} M$, then Heuristic 2.1 holds if and only if it holds with S replaced by S'.

Secondly, in [7, Hypothesis 6.6] the expected value $M_u^S(f)$ does not depend on the quotient R of $\mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} \mathcal{O} \cong \mathbb{Z}_{(S)}[G]$, and that is certainly not what was intended: if the set S is finite and non-empty, and the function f satisfies $f(M) = 0$ for all those $\mathbb{Z}_{(S)}[G]$-modules M that are annihilated by the kernel of the map $\mathbb{Z}_{(S)}[G] \to R$, and $f(M) = 1$ for all other $\mathbb{Z}_{(S)}[G]$-modules, then the limit in (2.2) is zero, while $M_u^S(f)$ is non-zero.

REMARK 2.4.   There are some curious functions that may be considered reasonable, but for which the limit (2.3) does not exist when S is too large. Suppose, for example, that S contains almost all prime numbers, and that R is the product of two rings T and T', where $T \cong T' \cong \mathbb{Z}_{(S)}$, so that A is a product of two $\mathbb{Q}$-algebras $C = \mathbb{Q} \otimes_{\mathbb{Z}_{(S)}} T$ and $C' = \mathbb{Q} \otimes_{\mathbb{Z}_{(S)}} T'$, both isomorphic to $\mathbb{Q}$. Take $P = \{0\}$. Define $f(M) = 1$ if $\#(T \otimes_R M) > \#(T' \otimes_R M)$, and $f(M) = 0$ otherwise. If B_C is fixed and $B_{C'}$ tends to ∞, then the limit of

$$\frac{\sum_{M \in \mathcal{M}_{\leqslant \mathbf{B}}} w_P(M) f(M)}{\sum_{M \in \mathcal{M}_{\leqslant \mathbf{B}}} w_P(M)}$$

is 0; while if $B_{C'}$ is fixed and B_C tends to ∞, then that limit is 1. From this observation it can be deduced that the limit in (2.3) does not exist. Such examples can be realised in the context of number fields: let C_2 be a cyclic group of order 2 and S_3 the symmetric group on a set of 3 elements, suppose that $F/\mathbb{Q}$ is Galois with Galois group isomorphic to $C_2 \times S_3$ such that the inertia groups at ∞ are subgroups of S_3 of order 2, and let S contain almost all prime numbers. Then F contains two imaginary quadratic subfields, one that is contained in a subextension that is Galois over $\mathbb{Q}$ with Galois group isomorphic to S_3, and one that is not, and the question of how often the order of the S-class group of the former is greater than that of the latter cannot be answered by Heuristic 2.1. We leave it to the reader to check that this example can indeed be realised in the framework of Heuristic 2.1 with a judicious choice of A and V.

If instead S is finite, then all the relevant sums converge absolutely, and the limit (2.3) is well defined. This adds to our reasons for demanding in Conjecture 1.5 that S be finite.

3.   *Commensurability of automorphism groups*

In this section, we recall the formalism of commensurability from [2], and deduce the existence of the probability measure $\mathbb{P}$ as described in the introduction.

A *group isogeny* is a group homomorphism $f \colon H \to G$ with $\# \ker f < \infty$ and $(G : fH) < \infty$, and its *index* $\mathrm{i}(f)$ is defined to be $(G : fH)/\# \ker f$. For a ring R, an *R-module isogeny* is an R-module homomorphism that is an isogeny as a map of additive groups. A *ring isogeny* is a ring homomorphism that is an isogeny as a map of additive groups. The index of an isogeny of one of the latter two types is defined as the index of the induced group isogeny on the additive groups.

If X, Y are objects of a category $\mathcal{C}$, then a *correspondence* from X to Y in $\mathcal{C}$ is a triple $c = (W, f, g)$, where W is an object of $\mathcal{C}$ and $f \colon W \to X$ and $g \colon W \to Y$ are morphisms in $\mathcal{C}$; we will often write $c \colon X \rightleftharpoons Y$ to indicate a correspondence. A *group commensurability* is a correspondence $c = (W, f, g)$ in the category of groups for which both f and g are isogenies. For a ring R, we define an *R-module commensurability* to be a correspondence of R-modules that is a commensurability of additive groups, and a *ring commensurability* is defined analogously.

If $c = (W, f, g)$ is a commensurability of groups, or of rings, or of modules over a ring, then its index is defined as $\mathrm{i}(c) = \mathrm{i}(g)/\mathrm{i}(f)$.

Let R be a ring, and let $c = (N, f, g)\colon L \rightleftharpoons M$ be a correspondence of R-modules. We define the *endomorphism ring* $\mathrm{End}c$ of c to be the subring $\{(\lambda, \nu, \mu) \in (\mathrm{End}L) \times (\mathrm{End}N) \times (\mathrm{End}M) : \lambda f = f\nu,\ \mu g = g\nu\}$ of the product ring $(\mathrm{End}L) \times (\mathrm{End}N) \times (\mathrm{End}M)$. There are natural ring homomorphisms $\mathrm{End}c \to \mathrm{End}L$ and $\mathrm{End}c \to \mathrm{End}M$ sending (λ, ν, μ) to λ and μ, respectively; we shall write $\mathrm{e}(c)\colon \mathrm{End}L \rightleftharpoons \mathrm{End}M$ for the ring correspondence consisting of $\mathrm{End}c$ and those two ring homomorphisms. Similarly, we define the *automorphism group* $\mathrm{Aut}c$ of c to be the group $(\mathrm{End}c)^{\times}$, and we write $\mathrm{a}(c)\colon \mathrm{Aut}L \rightleftharpoons \mathrm{Aut}M$ for the group correspondence consisting of $\mathrm{Aut}c$ and the natural maps $\mathrm{Aut}c \to \mathrm{Aut}L$, $\mathrm{Aut}c \to \mathrm{Aut}M$.

The following result is a special case of [**2**, Theorem 1.2].

THEOREM 3.1. *Let G be a finite group, let A be a quotient of $\mathbb{Q}[G]$ by some two-sided ideal, let S be a set of prime numbers, let R be the image of $\mathbb{Z}_{(S)}[G]$ in A, and let L, M be finitely generated R-modules. Then:*

(a) *there is an R-module commensurability $L \rightleftharpoons M$ if and only if the A-modules $A \otimes_R L$ and $A \otimes_R M$ are isomorphic;*

(b) *if $c\colon L \rightleftharpoons M$ is an R-module commensurability, then $\mathrm{e}(c)\colon \mathrm{End}L \rightleftharpoons \mathrm{End}M$ is a ring commensurability, and $\mathrm{a}(c)\colon \mathrm{Aut}L \rightleftharpoons \mathrm{Aut}M$ is a group commensurability;*

(c) *if c, $c'\colon L \rightleftharpoons M$ are R-module commensurabilities, then one has*

$$\mathrm{i}(\mathrm{e}(c)) = \mathrm{i}(\mathrm{e}(c')), \quad \mathrm{i}(\mathrm{a}(c)) = \mathrm{i}(\mathrm{a}(c')).$$

NOTATION 3.2. For the rest of the section, let G, A, S, and R be as in Theorem 3.1. If L and M are finitely generated R-modules such that there exists a commensurability $L \rightleftharpoons M$, then we define $\mathrm{ia}(L, M) = \mathrm{i}(\mathrm{a}(c))$ for any commensurability $c\colon L \rightleftharpoons M$.

LEMMA 3.3. *Let L, M, and N be finitely generated R-modules such that there are commensurabilities $L \rightleftharpoons M$ and $M \rightleftharpoons N$. Then there is a commensurability $L \rightleftharpoons N$, and we have $\mathrm{ia}(L, M)\mathrm{ia}(M, N) = \mathrm{ia}(L, N)$.*

Proof. See [**2**, Theorem 7.3]. $\square$

PROPOSITION 3.4. *Let P be a finitely generated projective R-module, let L_0 and M_0 be finite R-modules, let $L = P \oplus L_0$, and $M = P \oplus M_0$. Then there is an R-module commensurability $L \rightleftharpoons M$, and we have*

$$\mathrm{ia}(L, M) = \frac{\#\mathrm{Hom}(P, M_0) \cdot \#\mathrm{Aut}M_0}{\#\mathrm{Hom}(P, L_0) \cdot \#\mathrm{Aut}L_0}.$$

Proof. By Theorem 3.1(a), there exist commensurabilities $L \rightleftharpoons M$, $P \rightleftharpoons L$, and $P \rightleftharpoons M$. We will first compute $\mathrm{ia}(P, L)$ and $\mathrm{ia}(P, M)$. The split exact sequence

$$0 \to L_0 \to L \xrightarrow{\pi} P \to 0,$$

where π is the natural projection map, induces a surjective map

$$\mathrm{Aut}L \to \mathrm{Aut}L_0 \times \mathrm{Aut}P,$$

whose kernel is easily seen to be canonically isomorphic to $\mathrm{Hom}(P, L_0)$. It follows that if c is the commensurability $(L, \pi, \mathrm{id})\colon P \rightleftharpoons L$, then the map $\mathrm{Aut}c \to \mathrm{Aut}L$ is an isomorphism, while the map $\mathrm{Aut}c \to \mathrm{Aut}P$ is onto, with kernel of cardinality $\#\mathrm{Hom}(P, L_0) \cdot \#\mathrm{Aut}L_0$. Hence,

$\mathrm{ia}(P, L) = \mathrm{i}(\mathrm{a}(c)) = \#\mathrm{Hom}(P, L_0) \cdot \#\mathrm{Aut}L_0$, and analogously for $\mathrm{ia}(P, M)$. By Lemma 3.3, we therefore have that

$$\mathrm{ia}(L, M) = \frac{\mathrm{ia}(P, M)}{\mathrm{ia}(P, L)} = \frac{\#\mathrm{Hom}(P, M_0) \cdot \#\mathrm{Aut}M_0}{\#\mathrm{Hom}(P, L_0) \cdot \#\mathrm{Aut}L_0},$$

as claimed. $\qquad\square$

For the rest of the section, assume that S is a finite set of prime numbers that are good for A, and let $\mathcal{M}$ and $\mathcal{P}$ be sets of finitely generated R-modules as in the introduction.

LEMMA 3.5. *Let V be a finitely generated A-module. Then there exists a unique $P_V \in \mathcal{P}$ such that $A \otimes_R P_V \cong_A V$. Moreover, if M is a finitely generated R-module such that $A \otimes_R M \cong_A V$, then there exists a unique $M_0 \in \mathcal{M}$ such that $M \cong P_V \oplus M_0$.*

Proof. Let T be any finitely generated subgroup of V such that $\mathbb{Q}T = V$. Then $P = RT$ is a finitely generated R-submodule of V such that $A \otimes_R P = V$. By [**18**, Corollary 11.2], the ring R is a maximal $\mathbb{Z}_{(S)}$-order in A. It follows from [**18**, Theorems 18.1 and 2.44] that P is a projective R-module, and is isomorphic to a unique element P_V of $\mathcal{P}$.

Let M be a finitely generated R-module such that $A \otimes_R M \cong_A V$, let M_{tors} be the R-submodule of M consisting of $\mathbb{Z}_{(S)}$-torsion elements, and let $\bar{M} = M/M_{\mathrm{tors}}$ be the $\mathbb{Z}_{(S)}$-torsion-free quotient. It follows from [**18**, Theorem 18.10, §18 Exercise 3] that $\bar{M} \cong_R P_V$. Since P_V is projective, we have $M \cong_R P_V \oplus M_{\mathrm{tors}}$, and M_{tors} is isomorphic to a unique element M_0 of $\mathcal{M}$. $\qquad\square$

Recall from the introduction that if V is a finitely generated A-module, and $P_V \in \mathcal{P}$ is such that $A \otimes_R P_V \cong_A V$, then we define $\mathcal{M}_V = \{P_V \oplus M_0 : M_0 \in \mathcal{M}\}$. By Lemma 3.5, every finitely generated R-module M satisfying $A \otimes_R M \cong_A V$ is isomorphic to a unique element of $\mathcal{M}_V$. We now state and prove the main result of the section.

PROPOSITION 3.6. *Under the assumptions of Notation 3.2, suppose that S is a finite set of prime numbers that are good for A, let V be a finitely generated A-module, and let $P_V \in \mathcal{P}$ be such that $A \otimes_R P_V \cong V$. Then:*

(a) *there exists a unique discrete probability distribution $\mathbb{P}_V$ on $\mathcal{M}$ such that for all L_0, $M_0 \in \mathcal{M}$ we have*

$$\frac{\mathbb{P}_V(L_0)}{\mathbb{P}_V(M_0)} = \frac{\#Hom(P_V, M_0) \cdot \#Aut(M_0)}{\#Hom(P_V, L_0) \cdot \#Aut(L_0)};$$

(b) *there exists a unique discrete probability distribution $\mathbb{P}$ on $\mathcal{M}_V$ such that for any isomorphism $L \oplus E \cong M$ of R-modules, where L and M are in $\mathcal{M}_V$, and E is finite, we have*

$$\mathbb{P}(L) = (Aut\, M : Aut\, L) \cdot \mathbb{P}(M),$$

where the inclusion $Aut L \subset Aut M$ is the obvious one;
(c) *for all $E \in \mathcal{M}$, we have $\mathbb{P}(P_V \oplus E) = \mathbb{P}_V(E)$.*

Proof. For $L_0 \in \mathcal{M}$, write

$$w(L_0) = \frac{1}{\#\mathrm{Hom}(P_V, L_0) \cdot \#\mathrm{Aut}(L_0)}.$$

By [**7**, Theorem 3.6], the sum $\sum_{L_0 \in \mathcal{M}} w(L_0)$ converges, to α, say, so that we may define the probability distribution $\mathbb{P}_V$ on $\mathcal{M}$ by $\mathbb{P}_V(L_0) = w(L_0)/\alpha$ for $L_0 \in \mathcal{M}$. It satisfies the conclusion of part (a), and is clearly the unique such distribution. This proves part (a).

We now prove part (b). By combining the convergence of $\sum_{L_0 \in \mathcal{M}} w(L_0)$ with Proposition 3.4, we see that for all $M \in \mathcal{M}_V$, the sum $\sum_{L \in \mathcal{M}_V} \mathrm{ia}(L, M)$ also converges, to β_M, say, so that we may define a probability distribution $\mathbb{P}$ on $\mathcal{M}_V$ by $\mathbb{P}(L) = \mathrm{ia}(L, M)/\beta_M$ for $L \in \mathcal{M}_V$. Note that it follows from Lemma 3.3 that the definition of $\mathbb{P}$ is independent of the choice of module $M \in \mathcal{M}_V$. If there is an isomorphism $L \oplus E \cong M$ of R-modules, where L and M are in $\mathcal{M}_V$ and E is finite, and ι is the inclusion $L \hookrightarrow L \oplus E \cong M$, then by definition, we have $\mathrm{ia}(L, M) = \mathrm{ia}(c)$, where c is the commensurability $c = (L, \mathrm{id}, \iota) \colon L \rightleftharpoons M$. Thence it immediately follows that $\mathbb{P}$ satisfies the conclusion of part (b), and it is clearly the unique such probability distribution.

Part (c), finally, follows from Proposition 3.4. □

4. Class groups of imaginary abelian fields

In this section, we prove Theorem 1.1, and use it to give a disproof of Heuristic 2.1. We begin by establishing some notation for the section and recalling some well-known facts that will also be useful in the next section.

Generalities on group rings

Let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let G be a finite abelian group, with dual $\hat{G} = \mathrm{Hom}(G, \bar{\mathbb{Q}}^\times)$. For $\chi, \chi' \in \hat{G}$, we write $\chi \sim \chi'$ if $\ker \chi = \ker \chi'$, or equivalently if there exists $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with $\chi = \sigma \circ \chi'$. Each $\chi \in \hat{G}$ extends to a ring homomorphism $\chi \colon \mathbb{Q}[G] \to \bar{\mathbb{Q}}$, of which the image is the cyclotomic field $\mathbb{Q}(\chi(G))$, and the natural map $\mathbb{Q}[G] \to \prod_{\chi \in \hat{G}/\sim} \mathbb{Q}(\chi(G))$ is an isomorphism of $\mathbb{Q}$-algebras.

Let S be a set of prime numbers not dividing $\#G$, and write $T = \mathbb{Z}_{(S)}[G]$, which is a maximal $\mathbb{Z}_{(S)}$-order in $\mathbb{Q}[G]$. For $\chi \in \hat{G}$, the image $\chi(T)$ of T in $\mathbb{Q}(\chi(G))$ is the ring $\mathbb{Z}_{(S)}[\chi(G)]$, which is a Dedekind domain. We have a ring isomorphism $T \cong \prod_{\chi \in \hat{G}/\sim} \chi(T)$, so each T-module M decomposes as a direct sum $\bigoplus_{\chi \in \hat{G}/\sim}(\chi(T) \otimes_T M)$, which leads to a group isomorphism $\mathrm{G}(T) \cong \bigoplus_{\chi \in \hat{G}/\sim} \mathrm{G}(\chi(T))$, where we recall from the introduction that G denotes the Grothendieck group.

Since for each $\chi \in \hat{G}$ the ring $\chi(T) = \mathbb{Z}_{(S)}[\chi(G)]$ is a Dedekind domain, by [**19**, Theorems 1.4.12 and 3.1.13], there is a canonical isomorphism $\mathrm{G}(\chi(T)) \cong \mathrm{Cl}_{\chi(T)} \oplus \mathbb{Z}$, where $\mathrm{Cl}_{\chi(T)}$ is the class group of the $\mathbb{Z}_{(S)}$-order $\chi(T)$, and in particular is finite. Explicitly, the projection map $\mathrm{G}(\chi(T)) \to \mathbb{Z}$ is defined by sending the class of a finitely generated $\chi(T)$-module M to $\dim_{\mathbb{Q}(\chi(G))}(\mathbb{Q}(\chi(G)) \otimes_{\chi(T)} M)$, and a canonical splitting $\mathbb{Z} \to \mathrm{G}(\chi(T))$ is given by $1 \mapsto [\chi(T)]$; moreover, if the $\chi(T)$-module M is a non-zero ideal of $\chi(T)$, then the element $[M]$ of $\mathrm{G}(\chi(T))$ projects to the ideal class of M under the projection map to $\mathrm{Cl}_{\chi(T)}$. In particular, if M is a finite T-module, then the class $[M]$ in $\mathrm{G}(T)$ is contained in the torsion subgroup $\mathrm{G}(T)_{\mathrm{tors}} \cong \bigoplus_{\chi \in \hat{G}/\sim} \mathrm{Cl}_{\chi(T)}$.

The Cohen–Lenstra–Martinet prediction

In this subsection, we show that Heuristic 2.1 implies that if $c \in G$ is an element of order 2, and we choose $A = \mathbb{Q}[G]/(1 + c)$, $R = \mathbb{Z}_{(S)}[G]/(1 + c)$, and P to be the zero A-module in the heuristic, then the class of $R \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ is equidistributed in $\mathrm{G}(R)_{\mathrm{tors}}$ as (F, ι) varies over $\mathcal{F}$. The main technical ingredient is Theorem 4.2. It is a generalisation of [**5**, Corollary 3.7] from the trivial character to arbitrary Dirichlet characters.

Let $\mathcal{M}(T)$ be a set of finite T-modules such that for every finite T-module M there is a unique $M' \in \mathcal{M}(T)$ satisfying $M \cong M'$. For $M \in \mathcal{M}(T)$, $\mathbf{s} = (s_\chi)_{\chi \in \hat{G}/\sim} \in \mathbb{C}^{\hat{G}/\sim}$, and $\mathbf{u} = (u_\chi)_{\chi \in \hat{G}/\sim} \in (\mathbb{Z}_{\geqslant 0})^{\hat{G}/\sim}$, we recall the following definitions from [5] and [7]:

$$|M|^{\mathbf{s}} = \prod_{\chi \in \hat{G}/\sim} \#(\chi(T) \otimes_T M)^{s_\chi},$$

$$S_{\mathbf{u}}(M) = \#\{T\text{-linear surjections } Q \to M\},$$

where Q is a projective T-module such that $\dim_{\mathbb{Q}(\chi(G))}(\mathbb{Q}(\chi(G)) \otimes_T Q) = u_\chi$ for all $\chi \in \hat{G}$; it is easy to see that $S_{\mathbf{u}}(M)$ is well defined, that is, does not depend on the choice of Q;

$$w_{\mathbf{u}}(M) = \frac{S_{\mathbf{u}}(M)}{|M|^{\mathbf{u}}} \cdot \frac{1}{\#\mathrm{Aut}M},$$

$$w_{\boldsymbol{\infty}}(M) = \lim_{\mathbf{u} \to \boldsymbol{\infty}} w_{\mathbf{u}}(M),$$

where we recall that the notation $\mathbf{u} \to \boldsymbol{\infty}$ was defined at the beginning of Section 2. Observe that for $\mathbf{u} \in (\mathbb{Z}_{\geqslant 0})^{\hat{G}/\sim}$, one has $|M|^{\mathbf{u}} = \#\mathrm{Hom}(Q, M)$, where Q is as in the definition of $S_{\mathbf{u}}$. Moreover, if for all $\chi \in \hat{G}$ the ranks u_χ are 'large', then 'most' homomorphisms $Q \to M$, in a precisely quantifiable sense, are surjective. Making this precise, one deduces that $w_{\boldsymbol{\infty}}(M) = 1/\#\mathrm{Aut}(M)$. If $\mathbf{u}$ and $\mathbf{s}$ are as above, and $f \colon \mathcal{M}(T) \to \mathbb{C}$ is any function, we define the following quantities when the respective limit exists:

$$Z_{\mathbf{u}}(f, \mathbf{s}) = \lim_{\mathbf{B} \to \boldsymbol{\infty}} \sum_{M \in \mathcal{M}(T)_{\leqslant \mathbf{B}}} w_{\mathbf{u}}(M)|M|^{-\mathbf{s}} f(M),$$

$$Z(f, \mathbf{s}) = Z_{\boldsymbol{\infty}}(f, \mathbf{s}) = \lim_{\mathbf{u} \to \boldsymbol{\infty}} Z_{\mathbf{u}}(f, \mathbf{s}),$$

$$Z_{\mathbf{u}}(\mathbf{s}) = Z_{\mathbf{u}}(\mathbf{1}, \mathbf{s}), \quad Z(\mathbf{s}) = Z(\mathbf{1}, \mathbf{s}),$$

where $\mathbf{1}$ denotes the function $M \mapsto 1$ for all $M \in \mathcal{M}(T)$, and $\mathcal{M}(T)_{\leqslant \mathbf{B}}$ is defined analogously to $\mathcal{M}_{\leqslant \mathbf{B}}$ from Section 2. If T' is a quotient of T, we also define $Z_{\mathbf{u}}^{T'}(f, \mathbf{s})$ analogously to $Z_{\mathbf{u}}(f, \mathbf{s})$, and $Z^{T'}(f, \mathbf{s})$ analogously to $Z(f, \mathbf{s})$, but with the sums running only over T-modules that factor through T', that is, that are annihilated by the kernel of the quotient map $T \to T'$, and we again set $Z^{T'}(\mathbf{s}) = Z^{T'}(\mathbf{1}, \mathbf{s})$. With these definitions, the limit in (2.3) can be rewritten as

$$\lim_{\mathbf{s} \to \mathbf{s}_P} \frac{Z^R(f, \mathbf{s})}{Z^R(\mathbf{s})}, \tag{4.1}$$

where $\mathbf{s}_P = (\dim_{\mathbb{Q}(\chi(G))}(\mathbb{Q}(\chi(G)) \otimes_T P))_{\chi \in \hat{G}/\sim}$, provided that the limit $\lim_{\mathbf{s} \to \mathbf{s}_P} Z^R(f, \mathbf{s})$ exists and is finite and that $Z^R(\mathbf{s}_P) \neq 0$. We stress that this is true even if the infinite sum $Z^R(\mathbf{s}_P)$ diverges, in which case both the limit in (2.3) and that in (4.1) are equal to 0.

If $T' = \chi(T)$ for some $\chi \in \hat{G}/\sim$, then $Z_{\mathbf{u}}^{T'}(f, \mathbf{s})$ as a function of $\mathbf{s}$ depends only on the entry s_χ of $\mathbf{s}$, and similarly for $\mathbf{u}$, so we will write $Z_{u_\chi}^{\chi(T)}(f, s_\chi)$ in this case. In particular, if f is multiplicative in direct sums of the form $M = \bigoplus_{\chi \in \hat{G}/\sim} M_\chi$, where for each $\chi \in \hat{G}/\sim$, the summand M_χ is a $\chi(T)$-module, then one has

$$Z_{\mathbf{u}}(f, \mathbf{s}) = \prod_{\chi \in \hat{G}/\sim} Z_{u_\chi}^{\chi(T)}(f, s_\chi).$$

Recall from the discussion at the beginning of the section that for each $\chi \in \hat{G}$ we have a canonical isomorphism $G(\chi(T)) \cong \mathrm{Cl}_{\chi(T)} \oplus \mathbb{Z}$, and that if M is a finite $\chi(T)$-module, then $[M] \in G(\chi(T))$ is contained in the torsion subgroup $\mathrm{Cl}_{\chi(T)}$ of $G(\chi(T))$.

THEOREM 4.2. *Let $\hat{G}'$ be a subset of $\hat{G}$, let $T' = \prod_{\chi \in \hat{G}'/\sim} \chi(T)$, let $\phi = (\phi_\chi)_{\chi \in \hat{G}'/\sim}$: $\bigoplus_{\chi \in \hat{G}'/\sim} Cl_{\chi(T)} \to \mathbb{C}^\times$ be a group homomorphism, and define $f\colon \mathcal{M}(T) \to \mathbb{C}$ by $f(M) = 0$ if M does not factor through T', and $f(M) = \phi([M])$ otherwise. For $\chi \in \hat{G}'/\sim$, define $\tau_\chi = 0$ if ϕ_χ is trivial, and $\tau_\chi = -1/[\mathbb{Q}(\chi(G)) : \mathbb{Q}]$ otherwise. Assume that S contains all but finitely many prime numbers. Then for all $\mathbf{s} \in \mathbb{C}^{\hat{G}/\sim}$ satisfying $\Re s_\chi > \tau_\chi$ for all $\chi \in \hat{G}'/\sim$, we have*

$$\mathrm{Z}(f, \mathbf{s}) = \mathrm{Z}^{T'}(f, \mathbf{s}) = \prod_{\chi \in \hat{G}'/\sim} \prod_{k=1}^{\infty} L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s_\chi + k),$$

where $L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s)$ denotes the Dirichlet L-function corresponding to the Dirichlet character ϕ_χ^{-1} of the field $\mathbb{Q}(\chi(G))$ with the Euler factors at prime ideals not dividing any element of S omitted.

Proof. The proof proceeds very similarly to those of [5, Corollary 3.7; 7, Corollary 3.9(ii)], so we only sketch the main steps.

One has, for all M, M_1, $M_2 \in \mathcal{M}(T)$ and $\mathbf{u}$, $\mathbf{v} \in (\mathbb{Z}_{\geqslant 0})^{\hat{G}/\sim}$, the identities

$$\mathrm{S}_{\mathbf{u}+\mathbf{v}}(M) = \sum_{N \subset M} \mathrm{S}_{\mathbf{u}}(N) \mathrm{S}_{\mathbf{v}}(M/N)(\#N)^{\mathbf{v}}$$

with the sum running over submodules N of M, and

$$\sum_{M \in \mathcal{M}(T)} (w_{\mathbf{u}}(M) \cdot \#\{N \subset M : N \cong M_1, M/N \cong M_2\}) = w_{\mathbf{u}}(M_1) w_{\mathbf{u}}(M_2);$$

see [5, Proposition 3.2, Theorem 3.5]. Using the fact that f is multiplicative in short exact sequences of modules, one deduces from these two identities and a short calculation that there is a formal identity of Dirichlet series $\mathrm{Z}_{\mathbf{u}+\mathbf{v}}(f, \mathbf{s}) = \mathrm{Z}_{\mathbf{u}}(f, \mathbf{s}) \cdot \mathrm{Z}_{\mathbf{v}}(f, \mathbf{u} + \mathbf{s})$. In particular, if $\mathbf{1}_\chi \in (\mathbb{Z}_{\geqslant 0})^{\hat{G}/\sim}$ denotes the element that has χ-entry 1 and all other entries equal to 0, then

$$\mathrm{Z}_{\mathbf{u}+\mathbf{1}_\chi}(f, \mathbf{s}) = \mathrm{Z}_{\mathbf{u}}(f, \mathbf{s}) \cdot \mathrm{Z}_1^{\chi(T)}(f, u_\chi + s_\chi).$$

A direct calculation shows that for each $\chi \in \hat{G}$, one has $\mathrm{Z}_1^{\chi(T)}(f, s) = L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s+1)$. It follows that for all $\mathbf{u} \in (\mathbb{Z}_{\geqslant 0})^{\hat{G}/\sim}$, one has a formal identity between Dirichlet series

$$\mathrm{Z}_{\mathbf{u}}(f, \mathbf{s}) = \prod_{\chi \in \hat{G}'/\sim} \prod_{k=1}^{u_\chi} L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s_\chi + k). \tag{4.3}$$

By [14, Chapter VIII, Theorems 5 and 7], the Dirichlet series for $L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s+1)$ converges for $\Re s > \tau_\chi$, and for all $k \in \mathbb{Z}_{\geqslant 2}$, the Dirichlet series for $L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s+k)$ converges absolutely for $\Re s > \tau_\chi$. It follows from this and from a classical result of Landau on convergence of products of Dirichlet series (see [13, Theorem 54]) that equation (4.3) is an equality of analytic functions, valid whenever $\Re s_\chi > \tau_\chi$ for all $\chi \in \hat{G}'/\sim$. Finally, since, for every $s \in \mathbb{C}$ with $\Re s > \tau_\chi$, one has $L_{\mathbb{Q}(\chi(G))}^{(S)}(\phi_\chi^{-1}, s+k) = 1 + O(2^{-k})$, we may take the limit of equation (4.3) as $\mathbf{u} \to \infty$, and the result follows. $\square$

Now, let $c \in G$ be an element of order 2, let $A = \mathbb{Q}[G]/(1+c)$, let $R = \mathbb{Z}_{(S)}[G]/(1+c)$, let P be the zero A-module, and let $\mathcal{M}$ and $\mathcal{F}$ be as in the introduction. Let $\hat{G}' = \{\chi \in \hat{G} : \chi(c) = -1\}$, so that $\mathrm{G}(R)_{\mathrm{tors}} \cong \bigoplus_{\chi \in \hat{G}'/\sim} \mathrm{Cl}_{\chi(T)}$. For a group homomorphism $\phi = (\phi_\chi)_{\chi \in \hat{G}'/\sim}\colon \mathrm{G}(R)_{\mathrm{tors}} \to \mathbb{C}^\times$, define $f_\phi\colon \mathcal{M} \to \mathbb{C}^\times$ by $f_\phi(M) = \phi([M])$ for all $M \in \mathcal{M}$.

PROPOSITION 4.4.   *Suppose that for all group homomorphisms $\phi\colon G(R)_{tors} \to \mathbb{C}^\times$, Heuristic* 2.1 *holds with $K = \mathbb{Q}$, with R and P as just defined, and with $f = f_\phi$. Then, as (F, ι) ranges over $\mathcal{F}$, the class of $R \otimes_{\mathbb{Z}[G]} Cl_F$ in $G(R)_{tors}$ is equidistributed.*

Proof.   It follows from Theorem 4.2 that if $\phi = (\phi_\chi)_{\chi \in \hat{G}'/\sim}$ is a group homomorphism as in the hypotheses, then the limit (2.3) for $f = f_\phi$ is equal to

$$\lim_{s \to 0} \prod_{\chi \in \hat{G}'/\sim} \prod_{k=1}^{\infty} \left(\frac{L^{(S)}_{\mathbb{Q}(\chi(G))}(\phi_\chi^{-1}, s+k)}{\zeta^{(S)}_{\mathbb{Q}(\chi(G))}(s+k)} \right),$$

where $\zeta^{(S)}_{\mathbb{Q}(\chi(G))}(s)$ denotes the Dedekind zeta function of the field $\mathbb{Q}(\chi(G))$ with the Euler factors at prime ideals not dividing any element of S omitted. If ϕ is non-trivial, that is, at least one ϕ_χ is non-trivial, then for any such χ the pole of the Dedekind zeta function of $\mathbb{Q}(\chi(G))$ at $s = 1$ ensures that this limit is 0. If $x \in G(R)_{tors}$ is arbitrary, and $f_x\colon \mathcal{M} \to \mathbb{C}$ is defined by $f_x(M) = 1$ if $[M] = x$ and $f_x(M) = 0$ otherwise, then by the usual Fourier theory (which, in this case, is character theory of finite abelian groups), we have

$$f_x = \frac{1}{\#G(R)_{tors}} \sum_\phi \overline{\phi(x)} \cdot f_\phi,$$

where the sum runs over all homomorphisms $\phi\colon G(R)_{tors} \to \mathbb{C}^\times$. Thus, the limit (2.3) for $f = f_x$ is $\frac{1}{\#G(R)_{tors}}$, with the only non-zero contribution coming from the trivial homomorphism, as claimed. $\square$

In the remainder of the section, we will show that the conclusion of Proposition 4.4 is, in fact, false, in general.

Roots of unity

Let $F/\mathbb{Q}$ be an imaginary abelian field with Galois group G, and let $c \in G$ be the automorphism of F given by complex conjugation. We write $\hat{G}^- = \{\chi \in \hat{G} : \chi(c) = -1\}$, and $T^- = T/(1 + c)$; the latter ring may be identified with $\prod_{\chi \in \hat{G}^-/\sim} \chi(T)$, and one has

$$G(T^-) \cong \bigoplus_{\chi \in \hat{G}^-/\sim} G(\chi(T)). \tag{4.5}$$

For each $m \in \mathbb{Z}_{>0}$, we denote by ζ_m a primitive mth root of unity in some algebraic closure of F. Let U be the set of prime numbers $q \in S$ for which F contains ζ_q. Recall from the introduction that μ_F denotes the group of roots of unity in F.

PROPOSITION 4.6.   *The group $T^- \otimes_{\mathbb{Z}[G]} \mu_F$ is cyclic of order $\prod_{q \in U} q$.*

Proof.   Since μ_F is finite cyclic, the group $\mathbb{Z}_{(S)} \otimes_\mathbb{Z} \mu_F$ is cyclic of order equal to the largest divisor of $\#\mu_F$ that is a product of primes in S. If q is a prime number for which q^2 divides $\#\mu_F$, then q divides $[F : \mathbb{Q}] = \#G$, and therefore $q \notin S$. This implies that $\mathbb{Z}_{(S)} \otimes_\mathbb{Z} \mu_F$ is cyclic of order $\prod_{q \in U} q$. It is also a $\mathbb{Z}_{(S)}[G]$-module on which c acts as -1, so it equals $T^- \otimes_{\mathbb{Z}[G]} \mu_F$. $\square$

For each $q \in U$, denote by $\varphi_q\colon T^- \to \text{End}\langle\zeta_q\rangle \cong \mathbb{Z}/q\mathbb{Z}$ the ring homomorphism that describes the T^--module structure of $\langle\zeta_q\rangle$.

PROPOSITION 4.7.   *For each $q \in U$ there is an element $\chi_q \in \hat{G}^-$, unique up to $\sim$, such that φ_q factors as $T^- \to \chi_q(T) \to \mathbb{Z}/q\mathbb{Z}$, and it is characterised by the subfield $F^{\ker \chi_q} \subset F$ being*

equal to $\mathbb{Q}(\zeta_q)$. Also, if $\mathfrak{p}_q$ denotes the kernel of $\chi_q(T) \to \mathbb{Z}/q\mathbb{Z}$, then the image of the element $[T^- \otimes_{\mathbb{Z}[G]} \mu_F] \in G(T^-)$ under the isomorphism (4.5) equals the image of $(\chi_q(T)/\mathfrak{p}_q)_{q \in U}$ under the natural inclusion $\bigoplus_{q \in U} G(\chi_q(T)) \subset \bigoplus_{\chi \in \hat{G}^-/\sim} G(\chi(T))$.

Proof. Since $\mathbb{Z}/q\mathbb{Z}$ is a field, the map φ_q factors through exactly one of the components in the decomposition $T^- = \prod_{\chi \in \hat{G}^-/\sim} \chi(T)$, say through $\chi_q(T)$. By the irreducibility of the qth cyclotomic polynomial, the induced map $G \to \chi_q(G) \to (\mathbb{Z}/q\mathbb{Z})^\times$ is surjective, and since q does not divide $\#G$, the map $\chi_q(G) \to (\mathbb{Z}/q\mathbb{Z})^\times$ is injective, so the map $\chi_q(G) \to (\mathbb{Z}/q\mathbb{Z})^\times$ is an isomorphism. This shows that $\ker \chi_q = \ker(G \to (\mathbb{Z}/q\mathbb{Z})^\times)$, so we have indeed $F^{\ker \chi_q} = \mathbb{Q}(\zeta_q)$. In particular, the order of χ_q equals $q - 1$, so $\chi_q \neq \chi_{q'}$ for distinct $q, q' \in U$. We have an isomorphism of T^--modules $T^- \otimes_{\mathbb{Z}[G]} \mu_F \cong \bigoplus_{q \in U} \chi_q(T)/\mathfrak{p}_q$, and this implies the last assertion. $\square$

Maximal ideals

Let $\chi \in \hat{G}^-$. We describe the set of non-zero prime ideals of the Dedekind domain $\chi(T) = \mathbb{Z}_{(S)}[\chi(G)]$, which for non-empty S coincides with the set $\mathrm{Maxspec}\chi(T)$ of its maximal ideals. Denote by $[\chi] \in \hat{G}^-$ the equivalence class of χ under $\sim$. For each $p \in S$, let an embedding of $\bar{\mathbb{Q}}$ in an algebraic closure $\bar{\mathbb{Q}}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers be fixed, so that the group $\hat{G} = \mathrm{Hom}(G, \bar{\mathbb{Q}}^\times)$ may be identified with $\mathrm{Hom}(G, \bar{\mathbb{Q}}_p^\times)$; for $\psi, \psi' \in [\chi]$, we write $\psi \sim_p \psi'$ if there exists $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ with $\psi' = \sigma \circ \psi$. For each $(p, \psi) \in S \times [\chi]$, the map ψ induces a ring homomorphism $\psi \colon \chi(T) \to \bar{\mathbb{Q}}_p$ of which the image is contained in the discrete valuation ring $\mathbb{Z}_p[\psi(G)]$; we write $\mathfrak{m}_{p,\psi}$ for the kernel of the resulting map from $\chi(T)$ to the residue class field of $\mathbb{Z}_p[\psi(G)]$. This kernel is a non-zero prime ideal of $\chi(T)$. Each non-zero prime ideal of $\chi(T)$ is of the form $\mathfrak{m}_{p,\psi}$ with $(p, \psi) \in S \times [\chi]$, and one has $\mathfrak{m}_{p,\psi} = \mathfrak{m}_{p',\psi'}$ if and only if $p = p'$ and $\psi \sim_p \psi'$.

EXAMPLE 4.8. The prime ideal $\mathfrak{p}_q$ of $\chi_q(T)$ occurring in Proposition 4.7 equals $\mathfrak{m}_{q,\omega_q}$, where $\omega_q \colon G \to \mathbb{Z}_q^\times$ is the unique group homomorphism for which the induced map $G \to (\mathbb{Z}/q\mathbb{Z})^\times$ describes the G-module structure of $\langle \zeta_q \rangle$. The character $\omega_q \in \hat{G}$ is called the *Teichmüller character at q*.

Bernoulli numbers

Let $\chi \in \hat{G}^-$, and let $f(\chi) \in \mathbb{Z}_{>0}$ be minimal with $F^{\ker \chi} \subset \mathbb{Q}(\zeta_{f(\chi)})$. For each $t \in \mathbb{Z}$ that is coprime to $f(\chi)$, denote by η_t the restriction to $F^{\ker \chi}$ of the automorphism of $\mathbb{Q}(\zeta_{f(\chi)})$ that sends $\zeta_{f(\chi)}$ to $\zeta_{f(\chi)}^t$; note that η_t belongs to the Galois group $\mathrm{Gal}(F^{\ker \chi}/\mathbb{Q})$, which may be identified with $G/\ker \chi$ and with $\chi(G)$, and indeed we shall view η_t as an element of the cyclotomic field $\mathbb{Q}(\chi(G))$. We define the Bernoulli number

$$\beta(\chi) = \sum_{\substack{1 \leqslant t \leqslant f(\chi), \\ \gcd(t, f(\chi))=1}} \frac{t}{f(\chi)} \cdot \eta_t^{-1},$$

which is also an element of the cyclotomic field $\mathbb{Q}(\chi(G))$. For each $(p, \psi) \in S \times [\chi]$, the character ψ induces a field embedding $\mathbb{Q}(\chi(G)) \to \bar{\mathbb{Q}}_p$, which we simply denote by ψ. The following result relates the image $\psi(\beta(\chi))$ of the Bernoulli number to the ψ-component $\mathbb{Z}_p[\psi(G)] \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ of the class group of F.

PROPOSITION 4.9. (a) *Let $\chi \in \hat{G}^-$ and $(p, \psi) \in S \times [\chi]$. If $q \in U$ is such that $\chi \sim \chi_q$, assume $(p, \psi) \neq (q, \omega_q)$, where ω_q is as in Example 4.8. Let g be the rank of $\mathbb{Z}_p[\psi(G)]$ as a $\mathbb{Z}_p$-module. Then the order of $\mathbb{Z}_p[\psi(G)] \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ equals a unit of $\mathbb{Z}_p[\psi(G)]$ times $\psi(\beta(\chi))^g$.*
(b) *Let $q \in U$. Then $\mathbb{Z}_q[\omega_q(G)] \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F = \{0\}$, and $q \cdot \omega_q(\beta(\chi_q)) \in \mathbb{Z}_q^\times$.*

Proof. Part (a) is, stated with different notation, the same as [**16**, Theorem 2, Chapter 1, §10]. The first assertion of part (b) is [**16**, Remark 1, Chapter 1, §10] following the same theorem. For the second assertion of (b), note that by Proposition 4.7 we have $F^{\ker \chi_q} = \mathbb{Q}(\zeta_q)$, so $f(\chi_q) = q$, and therefore

$$q \cdot \omega_q(\beta(\chi)) = \sum_{t=1}^{q-1} t \cdot \omega_q(\eta_t)^{-1}.$$

Here, $\omega_q(\eta_t)$ is a $(q-1)$th root of unity in $\mathbb{Z}_q$, and, by definition of ω_q and η_t, it maps to $(t \bmod q)$ in $\mathbb{Z}/q\mathbb{Z}$. Hence, $q \cdot \omega_q(\beta(\chi_q))$ is an element of $\mathbb{Z}_q$ that maps to $(q-1 \bmod q)$ and therefore belongs to $\mathbb{Z}_q^\times$. $\qquad\square$

The following result describes, for each $\chi \in \hat{G}^-$, the finite $\chi(T)$-module $\chi(T) \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ up to Jordan–Hölder isomorphism in terms of Bernoulli numbers. We let $\mathfrak{p}_q$ be the prime ideal of $\chi_q(T)$ introduced in Proposition 4.7.

PROPOSITION 4.10.   *Let $\chi \in \hat{G}^-$.*

(a) *If there does not exist $q \in U$ such that $\chi \sim \chi_q$, then one has $\beta(\chi) \in \chi(T)$, and the $\chi(T)$-modules $\chi(T) \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ and $\chi(T)/(\beta(\chi))$ have isomorphic Jordan–Hölder series.*
(b) *If $q \in U$ is such that $\chi = \chi_q$, then one has $\mathfrak{p}_q \beta(\chi) \subset \chi(T)$, and the $\chi(T)$-modules $\chi(T) \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ and $\chi(T)/\mathfrak{p}_q \beta(\chi)$ have isomorphic Jordan–Hölder series.*

Proof. In case (a), one sees from Proposition 4.9(a) that for every non-zero prime ideal $\mathfrak{m} = \mathfrak{m}_{p,\psi}$ of $\chi(T)$ the element $\beta(\chi) \in \mathbb{Q}(\chi(G))$ has non-negative valuation at $\mathfrak{m}$, so one has $\beta(\chi) \in \chi(T)$. In case (b), Proposition 4.9 shows that the same assertion has the single exception $\mathfrak{m} = \mathfrak{p}_q = \mathfrak{m}_{q,\omega_q}$, and that $\beta(\chi)$ has valuation -1 at $\mathfrak{p}_q$; so in that case one has $\mathfrak{p}_q \beta(\chi) \subset \chi(T)$.

Proposition 4.9 implies that $\beta(\chi) \neq 0$, so all $\chi(T)$-modules occurring in Proposition 4.10 are finite; and two finite $\chi(T)$-modules have isomorphic Jordan–Hölder series if and only if, for each non-zero prime ideals $\mathfrak{m} = \mathfrak{m}_{p,\psi}$ of $\chi(T)$, their $\mathfrak{m}$-primary parts have the same cardinality. In case (a), Proposition 4.9(a) shows that this is indeed the case for the two modules $\chi(T) \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F$ and $\chi(T)/(\beta(\chi))$. In case (b), there is again a single $\mathfrak{m} = \mathfrak{m}_{q,\omega_q}$ that requires special treatment; Proposition 4.9(b) shows that in this exceptional case both modules have trivial $\mathfrak{m}$-primary parts. $\qquad\square$

We are now ready to prove Theorem 1.1. We first recall the statement.

THEOREM 4.11.   *Let $F/\mathbb{Q}$ be a finite imaginary abelian extension, let G be its Galois group, let $c \in G$ denote complex conjugation, let S be a set of prime numbers not dividing $\#G$, and let $T^- = \mathbb{Z}_{(S)}[G]/(1+c)$. Then we have $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F] = [T^- \otimes_{\mathbb{Z}[G]} \mu_F]$ in $\mathrm{G}(T^-)$.*

Proof. We will compute $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F] \in \mathrm{G}(T^-) \cong \bigoplus_{\chi \in \hat{G}^-/\sim} \mathrm{G}(\chi(T))$ component by component, and compare the result with Proposition 4.7. Let $\chi \in \hat{G}^-$. If for all $q \in U$ one has $\chi \not\sim \chi_q$, then by Proposition 4.10(a) the χ-component $[\chi(T) \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F]$ equals $[\chi(T)/(\beta(\chi))]$, and the exact sequence

$$0 \longrightarrow \chi(T) \xrightarrow{\beta(\chi)} \chi(T) \longrightarrow \chi(T)/(\beta(\chi)) \longrightarrow 0$$

shows that $[\chi(T)/(\beta(\chi))] = 0$. If, on the other hand, $q \in U$ is such that $\chi = \chi_q$, then one has $[\chi(T) \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F] = [\chi(T)/\mathfrak{p}_q \beta(\chi)]$, and the exact sequence

$$0 \longrightarrow \mathfrak{p}_q \xrightarrow{\beta(\chi)} \chi(T) \longrightarrow \chi(T)/\mathfrak{p}_q \beta(\chi) \longrightarrow 0$$

shows that $[\chi(T)/\mathfrak{p}_q\beta(\chi)] = [\chi(T)] - [\mathfrak{p}_q] = [\chi(T)/\mathfrak{p}_q]$. Comparing this description of $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F]$ with the description of $[T^- \otimes_{\mathbb{Z}[G]} \mu_F]$ given by Proposition 4.7, one finds that they are equal. $\qquad\square$

COROLLARY 4.12. *Under the hypotheses of Theorem 4.11, suppose that for all $q \in U$, the class group of $\mathbb{Q}(\zeta_{q-1})$ is trivial. Then $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F] = 0$ in $\mathrm{G}(T^-)$.*

Proof. By Theorem 4.11, we have $[T^- \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F] = [T^- \otimes_{\mathbb{Z}[G]} \mu_F]$ in $\mathrm{G}(T^-)$. Since for all $q \in U$, the class group of $\mathbb{Q}(\zeta_{q-1})$ is trivial, the ideals $\mathfrak{p}_q$ from Proposition 4.7 are principal for all $q \in U$, so the result follows from Proposition 4.7. $\qquad\square$

Counterexample to the Cohen–Lenstra–Martinet heuristics

We will now show that the conclusion of Corollary 4.12 contradicts the conclusion of Proposition 4.4, thus disproving Heuristic 2.1.

Let G be a cyclic group of order 58, let S contain all prime numbers except 2 and 29, and let $c \in G$ be the unique element of order 2. With these choices, if $F/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to G such that complex conjugation is given by c, then $T^- \cong \mathbb{Z}_{(S)} \times \mathbb{Z}_{(S)}[\zeta_{29}]$. Let $R = T^-$, let P be the zero A-module, and let $\mathcal{M}$ and $\mathcal{F}$ be as in the introduction. With these choices, $\mathcal{F}$ is the family of imaginary cyclic number fields of degree 58. The group $\mathrm{G}(R)_{\mathrm{tors}}$ is isomorphic to the class group $\mathrm{Cl}_{\mathbb{Z}_{(S)}[\zeta_{29}]}$, which one can check to be elementary abelian of order 8. For every F in the family under consideration except for $F = \mathbb{Q}(\zeta_{59})$, the set U that was introduced before Proposition 4.6 is either empty or equal to $\{3\}$. It follows from Corollary 4.12 that, unless $F = \mathbb{Q}(\zeta_{59})$, the class $[R \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F]$ in $\mathrm{G}(R)$ is 0, contradicting the conclusion of Proposition 4.4.

5. *Arakelov class groups of real abelian fields*

In this section, we reinterpret Theorem 4.11 in terms of so-called oriented Arakelov class groups, proving Theorem 1.4 along the way. This reinterpretation leads to a more general result, Theorem 5.4, which pertains to all finite abelian extensions of $\mathbb{Q}$, and which might conceivably be true in much greater generality; see Question 5.5.

We will use the generalities on group rings explained at the beginning of Section 4. In particular, G still denotes a finite abelian group, and we retain the notation S, T, $\hat{G}$.

Assume that S does not contain any prime numbers dividing $2 \cdot \#G$. Let F be a real abelian number field with Galois group G over $\mathbb{Q}$, and let $\mathcal{O}$ denote the ring of integers of F. If $k \neq \mathbb{Q}$ is a subfield of F that is cyclic over $\mathbb{Q}$, let $\alpha_k = \mathrm{Norm}_{\mathbb{Q}(\zeta_f)/k}(1 - \zeta_f)$, where $f \in \mathbb{Z}_{>0}$ is minimal with $k \subset \mathbb{Q}(\zeta_f)$, and ζ_f denotes an arbitrarily chosen primitive fth root of 1 in an algebraic closure of F. Let D be the subgroup of $F^\times$ generated by the G-orbits of α_k for all subfields $k \neq \mathbb{Q}$ of F that are cyclic over $\mathbb{Q}$. We follow Mazur–Wiles [16] in defining the *group of cyclotomic units* of F to be $C = D \cap \mathcal{O}^\times = \ker(|\mathrm{Norm}_{F/\mathbb{Q}}|\colon D \to \mathbb{Q}^\times)$. This group forms a $\mathbb{Z}[G]$-submodule of $\mathcal{O}^\times$. We will write $-_{(S)}$ for $\mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} -$. We will write the T-modules $D_{(S)}$, $C_{(S)}$, $\mathcal{O}_{(S)}^\times$ additively, so that $C_{(S)}$ is the kernel of the map $D_{(S)} \to D_{(S)}$, $x \mapsto \mathrm{Norm}_{F/\mathbb{Q}} x$, where $\mathrm{Norm}_{F/\mathbb{Q}} = \sum_{g \in G} g \in T$.

PROPOSITION 5.1. *The T-module $C_{(S)}$ is isomorphic to $T/(\sum_{g \in G} g)$.*

Proof. We will use without further explicit mention the facts that the ring $\mathbb{Z}_{(S)}$ is flat over $\mathbb{Z}$, and, for every $\chi \in \hat{G}$, the ring $\chi(T)$ is flat over T.

By [16, Theorem 1, Chapter 1, §10], the subgroup C has finite index in $\mathcal{O}^\times$. It follows that the annihilator of $C_{(S)}$ in T is generated by $\sum_{g \in G} g \in T$. The assertion of the proposition is

therefore equivalent to the statement that for every non-trivial $\chi \in \hat{G}$, the module $\chi(T) \otimes_T C_{(S)}$ is free of rank 1 over $\chi(T)$, which we will now prove.

First, suppose that $\chi \in \hat{G}$ is faithful, non-trivial. In particular, G is non-trivial, cyclic. Then for all $k \subsetneq F$ distinct from $\mathbb{Q}$, we have $\chi(T) \otimes_T T\alpha_k = 0$, since all elements of $T\alpha_k$ are fixed by a proper subgroup of G, while χ is faithful. Since the image of $\mathrm{Norm}_{F/\mathbb{Q}} \in T$ in the quotient $\chi(T)$ is 0, we have

$$\chi(T) \otimes_T C_{(S)} = \chi(T) \otimes_T \ker(\mathrm{Norm}_{F/\mathbb{Q}} \colon D_{(S)} \to D_{(S)})$$
$$= \chi(T) \otimes_T D_{(S)} = \chi(T) \otimes_T T\alpha_F,$$

so $\chi(T) \otimes_T C_{(S)}$ is cyclic.

Now, we deduce the general case. Let $\chi \in \hat{G}$ be arbitrary non-trivial, and let $F' \subset F$ be the fixed field of $\ker \chi$. Temporarily write $C_{F,(S)} = C_{(S)}$, and let $C_{F',(S)} = \mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} C_{F'}$, where $C_{F'}$ is the analogously defined group of cyclotomic units of F'. The image of the element $\mathrm{Norm}_{F/F'} = \sum_{g \in \ker \chi} g$ of T in the quotient $\chi(T)$ is $[F : F']$, which is invertible in $\chi(T)$. It follows that $\chi(T) \otimes_T C_{F,(S)} = \chi(T) \otimes_T \mathrm{Norm}_{F/F'}(C_{F,(S)})$. Moreover, it follows from a direct calculation, which we leave to the reader, that $\mathrm{Norm}_{F/F'} C_{F,(S)} \subset C_{F',(S)}$, and in fact, we have equality, since $\mathrm{Norm}_{F/F'}$ acts as $[F : F']$, and thus invertibly, on $C_{F',(S)} \subset C_{F,(S)}$. In summary, we have $\chi(T) \otimes_T C_{F,(S)} = \chi(T) \otimes_T C_{F',(S)}$. The assertion therefore follows from the special case proved above, applied to F' in place of F. □

The map $G \to G$ given by $g \mapsto g^{-1}$ for all $g \in G$ extends $\mathbb{Z}_{(S)}$-linearly to an isomorphism between T and its opposite ring T^{opp}. If M is any T-module, then the above isomorphism makes $\mathrm{Hom}(M, \mathbb{Z}_{(S)})$ and $\mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ into T-modules, which we denote by M^* and $M^\vee$, respectively.

We can now prove Theorem 1.4. Let us recall the statement.

THEOREM 5.2. *Let $F/\mathbb{Q}$ be a finite real abelian extension, let G be its Galois group, let S be a set of prime numbers not dividing $2 \cdot \#G$, and let $T = \mathbb{Z}_{(S)}[G]$. Then we have the equality $[T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F] = [T] - [\mathbb{Z}_{(S)}]$ in $\mathrm{G}(T)$, where $[\mathbb{Z}_{(S)}]$ denotes the class of $\mathbb{Z}_{(S)}$ with the trivial G-action.*

Proof. Recall from the exact sequence (1.3) that we have the equality

$$[T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F] = [(\mathcal{O}_{(S)}^\times)^*] + [(T \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F)^\vee]$$

in $\mathrm{G}(T)$. By [16, Theorem 1, Chapter 1, §10], we have $[\mathcal{O}_{(S)}^\times / C_{(S)}] = [T \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F]$, or dually,

$$[(C_{(S)})^* / (\mathcal{O}_{(S)}^\times)^*] = [(T \otimes_{\mathbb{Z}[G]} \mathrm{Cl}_F)^\vee],$$

whence $[T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F] = [(C_{(S)})^*]$. The theorem therefore follows from Proposition 5.1. □

Theorem 5.2 expresses that the class of the T-module $T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$ in $\mathrm{G}(T)$ is 'as simple as it can be' given the $\mathbb{Q}[G]$-module structure of $\mathbb{Q}[G] \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$. Indeed, as the discussion at the beginning of Section 4 shows, the class $[T \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F]$ in $\mathrm{G}(T)$ is determined by its images under the projection $\mathrm{G}(T) \to \mathrm{G}(T)/\mathrm{G}(T)_{\mathrm{tors}}$ and under the canonical splitting $\mathrm{G}(T) \to \mathrm{G}(T)_{\mathrm{tors}}$; the former is determined by the $\mathbb{Q}[G]$-module structure of $\mathbb{Q}[G] \otimes_{\mathbb{Z}[G]} \mathrm{Ar}_F$, and the theorem implies that the latter is 0.

Theorems 5.2 and 4.11 can be elegantly combined into one statement, using the so-called oriented Arakelov class group of a number field F, defined by Schoof in [20]. To explain this, we will briefly recall the definition and the most salient properties of the oriented Arakelov class group, and refer the reader to [20] for details.

Let $F/\mathbb{Q}$ be a finite extension, let Id_F be the group of fractional ideals of $\mathcal{O}_F$, and let $F_{\mathbb{R}}$ denote the $\mathbb{R}$-algebra $\mathbb{R} \otimes_{\mathbb{Q}} F$. The maximal compact subgroup $c(F_{\mathbb{R}}^{\times})$ of $F_{\mathbb{R}}^{\times}$ is isomorphic to $\{\pm 1\}^{\mathfrak{r}} \times \{z \in \mathbb{C}^{\times} : |z| = 1\}^{\mathfrak{c}}$, where $\mathfrak{r}$ and $\mathfrak{c}$ denote the set of real, respectively, complex places of F. It contains the group μ_F of roots of unity of F as a subgroup. We have canonical maps $\mathrm{Id}_F \to \mathbb{R}_{>0}$ and $F_{\mathbb{R}}^{\times} \to \mathbb{R}_{>0}$, the first given by the ideal norm, and the second given by the absolute value of the $\mathbb{R}$-algebra norm. Let $\mathrm{Id}_F \times_{\mathbb{R}_{>0}} F_{\mathbb{R}}^{\times}$ be the fibre product with respect to these maps. The *oriented Arakelov class group* $\widetilde{\mathrm{Pic}}_F^0$ of F is defined as the cokernel of the map $F^{\times} \to \mathrm{Id}_F \times_{\mathbb{R}_{>0}} F_{\mathbb{R}}^{\times}$ that sends $\alpha \in F^{\times}$ to $(\alpha\mathcal{O}_F, \alpha)$. It is a compact abelian Aut_F-module, whose dual $\mathrm{Hom}(\widetilde{\mathrm{Pic}}_F^0, \mathbb{R}/\mathbb{Z})$ will be denoted by $\widetilde{\mathrm{Ar}}_F$. One has an exact sequence of finitely generated discrete Aut_F-modules

$$0 \to \mathrm{Ar}_F \to \widetilde{\mathrm{Ar}}_F \to \mathrm{Hom}(c(F_{\mathbb{R}}^{\times})/\mu_F, \mathbb{R}/\mathbb{Z}) \to 0.$$

Let K be an algebraic number field, let F/K be a finite Galois extension, let G be its Galois group, let S is any set of odd prime numbers, let Σ be the set of infinite places of K, and for $v \in \Sigma$ let $I_v \subset G$ denote an inertia subgroup at v. Then one has an isomorphism of $\mathbb{Z}_{(S)}[G]$-modules

$$\mathbb{Z}_{(S)} \otimes_{\mathbb{Z}} \mathrm{Hom}(c(F_{\mathbb{R}}^{\times}), \mathbb{R}/\mathbb{Z}) \cong \bigoplus_{v \in \Sigma} \mathrm{Ind}_{G/I_v} \tau_v,$$

where Ind_{G/I_v} denotes the induction from I_v to G, and

$$\tau_v = \begin{cases} \mathbb{Z}_{(S)}[I_v]/\langle \sum_{g \in I_v} g \rangle, & v \text{ is real}, \\ \mathbb{Z}_{(S)}, & v \text{ is complex}. \end{cases}$$

Let d be the degree of K over $\mathbb{Q}$. By combining the above observation with the exact sequence (1.3), we deduce the equalities

$$[\widetilde{\mathrm{Ar}}_{F,(S)}] - [\mathrm{Ar}_{F,(S)}] = d \cdot [\mathbb{Z}_{(S)}[G]] - \sum_{v \in \Sigma}[\mathbb{Z}_{(S)}[G/I_v]] - [\mu_{F,(S)}^{\vee}],$$

and hence

$$[\widetilde{\mathrm{Ar}}_{F,(S)}] = d \cdot [\mathbb{Z}_{(S)}[G]] - \sum_{v \in \Sigma}[\mathbb{Z}_{(S)}[G/I_v]] + [(\mathcal{O}_{F,(S)}^{\times})^*] + [\mathrm{Cl}_{F,(S)}^{\vee}] - [\mu_{F,(S)}^{\vee}] \tag{5.3}$$

in $\mathrm{G}(\mathbb{Z}_{(S)}[G])$, where $\mathbb{Z}_{(S)}[G/I_v]$ denotes the permutation module with a $\mathbb{Z}_{(S)}$-basis given by the set of cosets G/I_v, and with G acting by left multiplication. Note that this equality holds for *all* finite Galois extensions, not just abelian ones. From this equality, together with Theorems 5.2 and 4.11, one easily deduces the following result.

THEOREM 5.4. *Let $F/\mathbb{Q}$ be a finite abelian extension, let G be its Galois group, let S be a set of prime numbers not dividing $2 \cdot \#G$, and let $T = \mathbb{Z}_{(S)}[G]$. Then we have the equality $[T \otimes_{\mathbb{Z}[G]} \widetilde{\mathrm{Ar}}_F] = [T] - [\mathbb{Z}_{(S)}]$ in $\mathrm{G}(T)$.*

The theorem suggests the following question.

QUESTION 5.5. *Let K be an algebraic number field, let d be its degree over $\mathbb{Q}$, let F/K be a finite Galois extension, let G be its Galois group, let S be a set of prime numbers not dividing $2 \cdot \#G$, and let $T = \mathbb{Z}_{(S)}[G]$. Is the class of $\widetilde{\mathrm{Ar}}_{F,(S)}$ in $\mathrm{G}(T)$ equal to $d \cdot [T] - [\mathbb{Z}_{(S)}]$?*

Equation (5.3) shows that the answer to Question 5.5 is affirmative when the natural map $\mathrm{G}(T) \to \mathrm{G}(\mathbb{Q} \otimes_{\mathbb{Z}_{(S)}} T)$ is injective, which is the case for example when S is finite, as can be deduced from Lemma 3.5 and [**18**, Theorem 21.4].

6. Enumerating number fields

In this section, we give our second disproof of the Cohen–Lenstra–Martinet heuristics. We begin by proving Theorem 1.2, and then compare its consequences with the predictions of Heuristic 2.1.

Our disproof suggests that the discriminant is not a good invariant to use for purposes of arithmetic statistics, and we investigate alternatives.

Let $\bar{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and let $\mathcal{C}(x)$ be the set of all fields $F \subset \bar{\mathbb{Q}}$ that are Galois over $\mathbb{Q}$ with cyclic Galois group of order 4 and whose discriminant is at most x. If $k \subset \bar{\mathbb{Q}}$ is a quadratic field, let $\mathcal{C}_k(x) = \{F \in \mathcal{C}(x) : k \subset F\}$. If n is a positive integer, let $\sigma_0(n)$ denote the number of positive divisors of n. The following result is a more precise version of Theorem 1.2.

THEOREM 6.1. *Define*
$$t = \frac{24 + \sqrt{2}}{24} \cdot \prod_{p \equiv 1 (\mathrm{mod}\ 4)} \left(1 + \frac{2}{(p+1)\sqrt{p}}\right) - 1,$$

where p ranges over primes. If $k \subset \bar{\mathbb{Q}}$ is a quadratic field, and d is its discriminant, then define p_k by

(i) $p_k = 0$ *if $d < 0$ or d has at least one prime divisor that is congruent to 3 (mod 4);*

(ii) $p_k = \frac{\sigma_0(d)}{t \cdot \prod_{p|d}(p+1)\sqrt{p}}$ *if $d > 0$, all odd prime divisors of d are congruent to 1 (mod 4), and d is even, where the product runs over all prime divisors of d;*

(iii) $p_k = \frac{\sigma_0(d)}{16t \cdot \prod_{p|d}(p+1)\sqrt{p}}$ *if $d > 0$ and all prime divisors of d are congruent to 1 (mod 4), where the product runs over all prime divisors of d.*

Then:

(a) *in case (i) the set $\mathcal{C}_k(x)$ is empty for all real numbers x;*

(b) *in the other two cases, the limit*
$$\lim_{x \to \infty} \frac{\#\mathcal{C}_k(x)}{\#\mathcal{C}(x)}$$

exists, and is equal to p_k;

(c) *one has $\sum_k p_k = 1$, where the sum runs over all quadratic fields in $\bar{\mathbb{Q}}$.*

Proof. First we prove part (a). If k is a quadratic field, and F is a cyclic quartic field containing k, then any place of $\mathbb{Q}$ that ramifies in k must be totally ramified in F, so k must be real, and only primes that are congruent to 1 or 2 (mod 4) can ramify in k. This proves the first assertion.

Now, we prove part (b). Let k be a quadratic field, let d be its discriminant, and assume that d is positive and not divisible by any primes that are congruent to 3 (mod 4). We will use the estimates of [**17**]. Write $d = 2^\beta d'$, where $\beta \in \{0, 3\}$, and d' is a product of distinct prime numbers that are congruent to 1 (mod 4). Then the discriminant of any cyclic quartic field containing k is of the form $n = 2^\alpha d'^3 a^2$, where a is an odd square-free positive integer that is coprime to d', and $\alpha = 11$ if $\beta = 3$, and $\alpha \in \{0, 4, 6\}$ if $\beta = 0$ (see [**17**]). Note that $k = \mathbb{Q}(\sqrt{n})$, so the discriminant of a cyclic quartic field determines its unique quadratic subfield. Let $h(n)$

be the number of cyclic quartic fields inside $\bar{\mathbb{Q}}$ of discriminant n. By [**17**, equation (3.3)], we have

$$h(n) = \begin{cases} 2\sigma_0(d') : & \alpha = 11, \\ \sigma_0(d') : & \alpha = 6, \\ \frac{1}{2}\sigma_0(d') : & \alpha = 0 \text{ or } 4. \end{cases}$$

For a real number x, let $\gamma(x)$ denote the number of square-free positive integers that are at most x and coprime to $2d$. It follows from the above discussion, that if d is odd, then

$$\#\mathcal{C}_k(x) = \sum_{a \leqslant \sqrt{x/d^3}} h(d^3 a^2) + \sum_{a \leqslant \sqrt{x/(2^4 d^3)}} h(2^4 d^3 a^2) + \sum_{a \leqslant \sqrt{x/(2^6 d^3)}} h(2^6 d^3 a^2)$$

$$= \sigma_0(d)\left(\tfrac{1}{2}\gamma\left(\sqrt{x/d^3}\right) + \tfrac{1}{2}\gamma\left(\sqrt{x/(2^4 d^3)}\right) + \gamma\left(\sqrt{x/(2^6 d^3)}\right) \right),$$

where the sums run over square-free positive integers a that are coprime to $2d$; while if d is even, then

$$\#\mathcal{C}_k(x) = \sum_{a \leqslant \sqrt{x/(2^{11} d'^3)}} h(2^{11} d'^3 a^2) = 2\sigma_0(d')\gamma\left(\sqrt{x/(2^{11} d'^3)}\right),$$

with the sum again running over square-free positive integers a that are coprime to $2d$. A standard estimate shows that for a positive integer m, we have

$$\gamma(x) = \frac{6x}{\pi^2} \prod_{p|2d} \frac{p}{p+1} + O(x^{1/2}),$$

where p ranges over primes. Combining this estimate with the above formulae for $\#\mathcal{C}_k(x)$ yields

$$\#\mathcal{C}_k(x) = \sigma_0(d)\frac{3x^{1/2}}{d^{3/2}\pi^2} \prod_{p|d} \frac{p}{p+1} + O(x^{1/4})$$

$$= \sigma_0(d)\frac{3x^{1/2}}{\pi^2} \prod_{p|d} \frac{1}{(p+1)\sqrt{p}} + O(x^{1/4})$$

if d is odd, and

$$\#\mathcal{C}_k(x) = \sigma_0(d')\frac{x^{1/2}}{2^{5/2} d'^{3/2}\pi^2} \prod_{p|d'} \frac{p}{p+1} + O(x^{1/4})$$

$$= \sigma_0(d')\frac{x^{1/2}}{2^{5/2}\pi^2} \prod_{p|d'} \frac{1}{(p+1)\sqrt{p}} + O(x^{1/4})$$

if d is even, where again p ranges over primes. On the other hand, by [**17**] we have

$$\#\mathcal{C}(x) = \frac{3}{\pi^2} t x^{1/2} + O(x^{1/3}(\log x)^3),$$

whence part (b) of the theorem follows.

The last part is readily verified by an easy direct computation, and we leave this to the reader. $\square$

THEOREM 6.2. *Let $\mathcal{C}(x)$ be the set of cyclic quartic fields inside $\bar{\mathbb{Q}}$ with discriminant at most x, and let $\mathcal{C}'(x) \subset \mathcal{C}(x)$ be the subset of those for which the class number of the quadratic subfield is not divisible by 3. Then the limit $\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x)$ exists, and one has*

$$\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x) \approx 0.9914.$$

Proof. For a quadratic field k and a positive real number x, let $p_k(x) = \#\mathcal{C}_k(x)/\#\mathcal{C}(x)$. Then by Theorem 6.1 one has $\lim_{x \to \infty} p_k(x) = p_k$, where p_k is defined as in that theorem.

Let $\mathcal{K}$ be any set of real quadratic fields. Then we claim that

$$\lim_{x \to \infty} \sum_{k \in \mathcal{K}} p_k(x) = \sum_{k \in \mathcal{K}} \lim_{x \to \infty} p_k(x). \tag{6.3}$$

This is clear when $\mathcal{K}$ is finite. In general, for every finite $\mathcal{K}' \subset \mathcal{K}$, we have

$$\liminf_{x \to \infty} \sum_{k \in \mathcal{K}} p_k(x) \geqslant \liminf_{x \to \infty} \sum_{k \in \mathcal{K}'} p_k(x),$$

so applying identity (6.3) to finite subsets of $\mathcal{K}$, we obtain

$$\liminf_{x \to \infty} \sum_{k \in \mathcal{K}} p_k(x) \geqslant \sup_{\substack{\mathcal{K}' \subset \mathcal{K} \\ \text{finite}}} \sum_{k \in \mathcal{K}'} \lim_{x \to \infty} p_k(x) = \sum_{k \in \mathcal{K}} \lim_{x \to \infty} p_k(x), \tag{6.4}$$

where the last equality follows from the fact that all the summands are non-negative. By Theorem 6.1(c) one has $\sum_k \lim_{x \to \infty} p_k(x) = 1$, where the sum runs over all real quadratic fields. By combining this with inequality (6.4) applied to the complement of $\mathcal{K}$ in the set of all real quadratic fields in place of $\mathcal{K}$, one deduces that $\limsup_{x \to \infty} \sum_{k \in \mathcal{K}} p_k(x) \leqslant \sum_{k \in \mathcal{K}} \lim_{x \to \infty} p_k(x)$, whence the claimed equality (6.3) follows.

When applied to the set $\mathcal{K}$ of real quadratic fields whose class number is not divisible by 3, this shows that the limit $\lim_{x \to \infty} \#\mathcal{C}'(x)/\#\mathcal{C}(x)$ exists. Moreover, by summing p_k from Theorem 6.1 over those real quadratic fields of discriminant less than 3.1×10^9 whose class number is, respectively, is not, divisible by 3 one obtains sufficiently tight upper and lower bounds on that limit to obtain the estimate in the theorem. $\square$

REMARK 6.5. If, in Heuristic 2.1, we take $G = \langle g | g^4 = \mathrm{id} \rangle$, $A = \mathbb{Q}[G]/(1 + g) \cong \mathbb{Q}$, $S = \{3\}$ (so that in particular $R \cong \mathbb{Z}_{(3)}$), the module P to be free of rank 1 over R, and

$$f \colon M \mapsto \begin{cases} 0, & 3 \mid \#M; \\ 1, & 3 \nmid \#M, \end{cases}$$

then the value of (2.2) is nothing but the limit $\lim_{x \to \infty} \#\mathcal{C}'(x)/\mathcal{C}(x)$ referred to in Theorem 6.2. The same argument as in the proof of the theorem shows that, more generally, if one chooses A and G as just described, S to be any set of odd primes, the projective module P to have rank 1 over R, and f to be any computable bounded $\mathbb{C}$-valued function on $\mathcal{M}$, then the limit (2.2) exists and can be computed to any desired precision.

Theorem 6.2 contradicts the predictions of Heuristic 2.1, as we will now explain. As just remarked, the limit $\lim_{x \to \infty} \#\mathcal{C}'(x)/\mathcal{C}(x)$ of Theorem 6.2 is equal to the value of (2.2) for suitable choices of G, A, S, P, and f. The value of (2.3), on the other hand, with these choices is the same as with a different choice, namely, as with $G' = \langle h | h^2 = \mathrm{id} \rangle$, $A' = \mathbb{Q}[G']/(1 + h) \cong A$, and $S' = S$, $P' = P$, and $f' = f$. With that latter choice, the value of (2.3) was computed in [6, (1.2)(b)] to be ≈ 0.8402, and thus not equal to the value of (2.2), which is given by Theorem 6.2. This completes our disproof of Heuristic 2.1.

The above disproof relies on the observation that enumerating number fields by non-decreasing discriminant has the undesirable feature that certain fields may appear with positive

probability as intermediate fields, so that Heuristic 2.1 for those number fields clashes with that for the intermediate fields. We conjecture that instead enumerating fields by the ideal norm $c_{F/K}$ of the product of the primes of $\mathcal{O}_K$ that ramify in F/K does not exhibit this feature. The following is a result in support of this conjecture. Recall that if $\mathcal{F}$ is a set of pairs (F, ι) as in the introduction, where all fields F are Galois extensions of a given field K, then for every positive real number B we define $\mathcal{F}_{c \leqslant B} = \{(F, \iota) \in \mathcal{F} : c_{F/K} \leqslant B\}$.

PROPOSITION 6.6. *Let K be a number field, let $\bar{K}$ be an algebraic closure of K, let G be a finite abelian group, let V be a finitely generated $\mathbb{Q}[G]$-module, and let $\mathcal{F}$ be the set of all pairs (F, ι), where $F \subset \bar{K}$ is a Galois extension of K, and ι is an isomorphism between the Galois group of F/K and G that induces an isomorphism $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_F^\times \cong V$ of $\mathbb{Q}[G]$-modules. Assume that $\mathcal{F}$ is not empty. Let $k \subset \bar{K}$ be a field properly containing K. Then the limit $\lim_{B \to \infty} \#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : k \subset F\}/\#\mathcal{F}_{c \leqslant B}$ is zero.*

Proof. Let T be an infinite set of prime ideals of $\mathcal{O}_K$ with odd residue characteristics that are not totally split in k/K. Then for any $F \subset \bar{K}$ that contains k, and for all $\mathfrak{p} \in T$, we have $F \otimes_K K_{\mathfrak{p}} \not\cong K_{\mathfrak{p}}^{\#G}$ as $K_{\mathfrak{p}}$-algebras, where $K_{\mathfrak{p}}$ denotes the field of fractions of the completion of $\mathcal{O}_K$ at $\mathfrak{p}$. It follows that for all positive real numbers B, we have

$$\#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : k \subset F\} \leqslant \#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : \forall \mathfrak{p} \in T: F \otimes_K K_{\mathfrak{p}} \not\cong K_{\mathfrak{p}}^{\#G}\}.$$

By [21, Theorem 2.1], for every finite subset T' of T, each of the following limits exists, and there is an equality

$$\lim_{B \to \infty} \frac{\#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : \forall \mathfrak{p} \in T': F \otimes_K K_{\mathfrak{p}} \not\cong K_{\mathfrak{p}}^{\#G}\}}{\#\mathcal{F}_{c \leqslant B}}$$

$$= \prod_{\mathfrak{p} \in T'} \left(\lim_{B \to \infty} \frac{\#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : F \otimes_K K_{\mathfrak{p}} \not\cong K_{\mathfrak{p}}^{\#G}\}}{\#\mathcal{F}_{c \leqslant B}} \right),$$

moreover, [21, Theorem 2.1] also implies that each of the factors on the right-hand side is bounded away from 1 uniformly for all $\mathfrak{p} \in T$. Thus, we have

$$\limsup_{B \to \infty} \frac{\#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : k \subset F\}}{\#\mathcal{F}_{c \leqslant B}}$$

$$\leqslant \prod_{\mathfrak{p} \in T} \left(\lim_{B \to \infty} \frac{\#\{(F, \iota) \in \mathcal{F}_{c \leqslant B} : F \otimes_K K_{\mathfrak{p}} \not\cong K_{\mathfrak{p}}^{\#G}\}}{\#\mathcal{F}_{c \leqslant B}} \right) = 0,$$

as claimed.   □

7. *Reasonable functions*

In this section, we address the question of which functions may qualify as 'reasonable' for the purposes of Conjecture 1.5. We begin by proving Theorem 1.6, which suggests that demanding that $\mathbb{E}(|f|)$ should exist is likely not a sufficient criterion. After that, we offer two possible interpretations of the word 'reasonable'.

From now on, let (X, p) be an infinite discrete probability space such that $p(x) > 0$ for all $x \in X$, where we recall from the introduction that $p(x)$ is shorthand for $p(\{x\})$, and let Y be the probability space $X^{\mathbb{Z}_{\geqslant 1}}$ with the induced product probability measure (see, for example, [12, §38]). When referring to subsets of a measure space, we will say 'almost all' to mean a subset whose complement has measure 0.

Let us reformulate Theorem 1.6, using the above notation.

THEOREM 7.1. *For almost all sequences $y = (y_i)_i \in Y$, there exists a function $f \colon X \to \mathbb{R}_{\geqslant 0}$ whose expected value $\mathbb{E}(f)$ is finite, but for which the average $\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} f(y_i)$ of f on y does not exist in $\mathbb{R}$.*

The idea of the proof will be to show that, for a typical $(y_i)_i \in Y$, there are many elements $x \in X$ that occur much earlier in $(y_i)_i$ than one would expect. The function f then gives those elements a large weight.

PROPOSITION 7.2. *For almost all sequences $y = (y_i)_i \in Y$ it is true that for all $\epsilon \in \mathbb{R}_{>0}$ there exist infinitely many $x \in X$ such that for some $i \leqslant \epsilon/p(x)$, one has $y_i = x$.*

Proof. Let $\epsilon \in \mathbb{R}_{>0}$ be given, and let U be a finite subset of X. First, we claim that for almost all sequences $y = (y_i)_i \in Y$ there exists $x \in X \setminus U$ such that for some $i \leqslant \epsilon/p(x)$, one has $y_i = x$. If x is an element of X, let E_x be the set of $y = (y_i)_i \in Y$ for which $y_i \neq x$ for all $i \leqslant \epsilon/p(x)$. The probability of the event E_x, meaning the measure of $E_x \subset Y$, is equal to $(1 - p(x))^{\lfloor \epsilon/p(x) \rfloor}$, which tends to $e^{-\epsilon}$, as $p(x)$ tends to 0, and in particular is uniformly bounded away from 1 for all but finitely many $x \in X$. If $x_1, x_2, \ldots, x_k$ are distinct elements of X, then the events E_{x_i} are generally not independent, but the probability of E_{x_k} given that all of $E_{x_1}, \ldots, E_{x_{k-1}}$ occur is clearly less than or equal to the probability of E_{x_k}. It follows that the probability that E_x occurs for all $x \in X \setminus U$ is at most $\prod_{x \in X \setminus U}(1 - p(x))^{\lfloor \epsilon/p(x) \rfloor} = 0$. This proves the claim.

Since the number of finite subsets U of X is countable, it follows from countable subadditivity that if $\epsilon \in \mathbb{R}_{>0}$ is given, then for almost all $y = (y_i)_i \in Y$ it is true that for all finite subsets U of X there exists $x \in X \setminus U$ such that for some $i \leqslant \epsilon/p(x)$, one has $y_i = x$. This implies that if $\epsilon \in \mathbb{R}_{>0}$ is given, then for almost all $y = (y_i)_i \in Y$ there exist infinitely many $x \in X$ such that for some $i \leqslant \epsilon/p(x)$, one has $y_i = x$. By applying this conclusion to countably infinitely many $\epsilon_n \in \mathbb{R}_{>0}$ in place of ϵ, where $(\epsilon_n)_{n \in \mathbb{Z}_{\geqslant 1}}$ is a sequence converging to 0, and by invoking countable subadditivity again, we deduce the proposition. $\square$

We are now ready to prove Theorem 7.1.

Proof of Theorem 7.1. Let $y = (y_i)_i \in Y$ be a sequence for which the conclusion of Proposition 7.2 holds. Then there is a sequence $x_1, x_2, \ldots$ of distinct elements of X such that for each $n \in \mathbb{Z}_{\geqslant 1}$, we have $\min\{i \in \mathbb{Z}_{\geqslant 1} : y_i = x_n\} \leqslant n^{-3}/p(x_n)$.

For $n \in \mathbb{Z}_{\geqslant 1}$, let $i(n) = \min\{j \in \mathbb{Z}_{\geqslant 1} : y_j = x_n\} \leqslant n^{-3}/p(x_n)$. For $x \in X$, define $f(x) = 0$ if $x \neq x_n$ for any $n \in \mathbb{Z}_{\geqslant 1}$, and $f(x_n) = n^{-2}/p(x_n)$. Then we have $\mathbb{E}(f) = \sum_{n \in \mathbb{Z}_{\geqslant 1}} n^{-2}$, which converges. On the other hand, for every $n \in \mathbb{Z}_{\geqslant 1}$, one has

$$\frac{1}{i(n)} \sum_{j=1}^{i(n)} f(y_j) \geqslant \frac{f(x_n)}{i(n)} \geqslant \frac{n^{-2}/p(x_n)}{n^{-3}/p(x_n)} = n,$$

which gets arbitrarily large, as n varies, so the limit $\lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} f(y_j)$ does not exist. $\square$

Let us now discuss two possible interpretations of the word 'reasonable' in Conjecture 1.5. As will hopefully become clear, this section should be treated as an invitation to the reader to join in our speculations. If $\mathcal{M}_V$ is as in Conjecture 1.5, let $f \colon \mathcal{M}_V \to \mathbb{C}$ be a function. For a positive integer j, the jth moment of f is defined to be $\sum_{M \in \mathcal{M}_V}(f(M)^j \mathbb{P}(M))$ if the sum converges absolutely.

CONJECTURE 7.3 (Supplement 1 to Conjecture 1.5). *If* $f\colon \mathcal{M}_V \to \mathbb{C}$ *is a function such that for all* $j \in \mathbb{Z}_{\geqslant 1}$, *the* jth *moment of* $|f|$ *exists in* $\mathbb{R}$, *then* f *is 'reasonable' for the purposes of Conjecture 1.5.*

All bounded functions on $\mathcal{M}_V$, and many unbounded functions of arithmetic interest satisfy this condition. This applies to all examples in [6], with the exception of the functions $f(M) = \#M$, and $f(M) = (\#M)^2$, which often have expected value ∞. Note that in [6] the set S of prime numbers was not assumed to be finite. Here, when we talk about the examples in [6], we mean the analogues in our setting of the functions considered there. On the other hand, it can be shown that if $X = \mathcal{M}_V$, $A \neq 0$, and S is non-empty, so that $\mathcal{M}_V$ is infinite, then for the function constructed in the proof of Theorem 7.1 the second moment does not exist.

Let us call a class $\mathcal{R}$ of $\mathbb{C}$-valued functions on X *promising* if for all $f \in \mathcal{R}$, the expected value $\mathbb{E}(f)$ exists, and for almost all sequences $y = (y_i)_i \in Y$ it is true that for all $f \in \mathcal{R}$ we have $\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} f(y_i) = \mathbb{E}(f)$. By the law of large numbers, for any function $f\colon X \to \mathbb{C}$ for which $\mathbb{E}(f)$ exists, the set $\mathcal{R} = \{f\}$ is promising. It immediately follows that any countable set $\mathcal{R}$ of such functions is promising. On the other hand, Theorem 7.1 implies that the class of all functions $f\colon X \to \mathbb{C}$ for which $\mathbb{E}(f)$ exists is not promising. An affirmative answer to the following question would strengthen our confidence in Conjecture 7.3.

QUESTION 7.4. Is the class of all functions $f\colon \mathcal{M}_V \to \mathbb{C}$ for which for all $j \in \mathbb{Z}_{\geqslant 1}$, the jth moment of $|f|$ exists in $\mathbb{R}$ promising?

We have the following weak result in this direction.

PROPOSITION 7.5. *The class of all bounded* $\mathbb{C}$-valued functions on X is promising.

Proof. For any $c \in \mathbb{R}_{>0}$, let $\mathcal{R}_c$ be the class of all functions $f\colon X \to \mathbb{C}$ for which $\sup_{x \in X} |f(x)| \leqslant c$. We will first show that for all $c \in \mathbb{R}_{>0}$, the class $\mathcal{R}_c$ is promising.

Let $X_1 \subset X_2 \subset \ldots$ be a sequence of finite subsets of X such that $\lim_{j \to \infty} \sum_{x \in X_j} p(x) = 1$. Fix $c \in \mathbb{R}_{>0}$, and let $\epsilon \in \mathbb{R}_{>0}$ be arbitrary. Then we may choose $X_{j(\epsilon)}$ such that $\sum_{x \in X \setminus X_{j(\epsilon)}} p(x) \leqslant \epsilon/c$. Moreover, by the strong law of large numbers, there exists a subset $Y_c(\epsilon) \subset Y$ of measure 1 with the following property: for all $y = (y_i)_i \in Y_c(\epsilon)$ there is an $N_y(\epsilon) \in \mathbb{Z}_{\geqslant 1}$ such that for all $x \in X_{j(\epsilon)}$ and for all $n \geqslant N_y(\epsilon)$ one has $|\frac{1}{n} \cdot \#\{i \leqslant n : y_i = x\} - p(x)| \leqslant \epsilon/(c \cdot \#X_{j(\epsilon)})$. It follows that for all $y \in Y_c(\epsilon)$, for all $f \in \mathcal{R}_c$, and for all $n \geqslant N_y(\epsilon)$ one has

$$\left| \frac{1}{n} \sum_{i=1}^{n} f(y_i) - \mathbb{E}(f) \right| = \left| \sum_{x \in X} \left(\tfrac{1}{n} \cdot \#\{i \leqslant n : y_i = x\} - p(x) \right) \cdot f(x) \right|$$

$$\leqslant \sum_{x \in X_{j(\epsilon)}} \left| \left(\tfrac{1}{n} \cdot \#\{i \leqslant n : y_i = x\} - p(x) \right) \cdot f(x) \right|$$

$$+ \sum_{x \in X \setminus X_{j(\epsilon)}} \left| \left(\tfrac{1}{n} \cdot \#\{i \leqslant n : y_i = x\} - p(x) \right) \cdot f(x) \right|$$

$$\leqslant \epsilon + \sum_{x \in X \setminus X_{j(\epsilon)}} \tfrac{1}{n} \cdot \#\{i \leqslant n : y_i = x\} \cdot |f(x)| + \sum_{x \in X \setminus X_{j(\epsilon)}} p(x)|f(x)|$$

$$\leqslant \epsilon + \left(1 - \sum_{x \in X_{j(\epsilon)}} \tfrac{1}{n} \cdot \#\{i \leqslant n : y_i = x\} \right) \cdot c + \epsilon$$

$$\leqslant 2\epsilon + \left(1 - \sum_{x \in X_{j(\epsilon)}} \left(p(x) - \frac{\epsilon}{c \cdot \#X_{j(\epsilon)}}\right)\right) \cdot c$$

$$\leqslant 4\epsilon.$$

Therefore, if $(\epsilon_n)_{n \in \mathbb{Z}_{\geqslant 1}}$ is a sequence of positive real numbers converging to 0, then the intersection $Y_c = \bigcap_{n \in \mathbb{Z}_{\geqslant 1}} Y_c(\epsilon_n)$ has measure 1 and has the property that for every $y = (y_i)_i \in Y_c$ and for every $f \in \mathcal{R}_c$ one has $\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^n f(y_i) = \mathbb{E}(f)$.

If $(c_n)_{n \in \mathbb{Z}_{\geqslant 1}}$ is a sequence of positive real numbers tending to ∞, then the class of all bounded functions is equal to $\bigcup_{n \in \mathbb{Z}_{\geqslant 1}} \mathcal{R}_{c_n}$, and the intersection $\bigcap_{n \in \mathbb{Z}_{\geqslant 1}} Y_{c_n}$ has measure 1 and has the property that for every sequence $y = (y_i)_i$ in this intersection and for every bounded function f one has $\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^n f(y_i) = \mathbb{E}(f)$. This completes the proof. $\square$

We will now describe a completely different approach to the question of reasonableness, which is based on the idea that one can distinguish between 'highly artificial' functions, such as those that are constructed in the proof of Theorem 7.1, and 'natural' functions that one cares about in practice by the ease with which they can be computed.

Let A, S, R and V be as in Conjecture 1.5, and suppose that S is non-empty and $A \neq 0$. Let Q be the set of non-increasing sequences $(n_i \in \mathbb{Z}_{\geqslant 0} : i \in \mathbb{Z}_{\geqslant 0})$ that have only finitely many non-zero terms. Let $\mathrm{Maxspec}(\mathrm{Z}(R))$ be the finite set of maximal ideals of the centre $\mathrm{Z}(R)$ of R. It follows from [**7**, Lemma 2.7] that the set $\mathcal{M}$ is canonically in bijection with the set $Q^{\mathrm{Maxspec}(\mathrm{Z}(R))}$, and by Lemma 3.5 we also have a bijection between $\mathcal{M}_V$ and $Q^{\mathrm{Maxspec}(\mathrm{Z}(R))}$.

CONJECTURE 7.6 (Supplement 2 to Conjecture 1.5). If $f \colon \mathcal{M}_V \to \mathbb{Z}$ is a function such that $\mathbb{E}(|f|)$ exists in $\mathbb{R}$, and the function $Q^{\mathrm{Maxspec}(\mathrm{Z}(R))} \to \mathbb{Z}$ induced by f is computable in polynomial time, where the input is given in unary notation, then f is 'reasonable' for the purposes of Conjecture 1.5.

The functions that one typically cares about in practice, including all those given as examples in [**6**] for which S is finite, are computable in polynomial time. On the other hand, we do not expect the function that was constructed in the proof of Theorem 7.1 for y being the sequence of class groups in a family of number fields to be computable in polynomial time. Indeed, to define $f(M)$, one needs to know roughly the first $\#\mathrm{Aut}(M)$ terms of the sequence y, and $\#\mathrm{Aut}(M)$ is exponential in the size of the input.

References

1. A. AGBOOLA, 'On counting rings of integers as Galois modules', *J. reine angew. Math.* 663 (2012) 1–31.
2. A. BARTEL and H. W. LENSTRA, Jr., 'Commensurability of automorphism groups', *Compos. Math.* 153 (2017) 323–346.
3. M. BHARGAVA and I. VARMA, 'The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders', *Proc. Lond. Math. Soc.* 112 (2016) 235–266.

4. J. W. S. CASSELS and A. FRÖHLICH (eds), 'Algebraic number theory', *Proceedings of an Instructional Conference Organized by the London Mathematical Society* (*a NATO Advanced Study Institute*) *with the Support of the International Mathematical Union* (Academic Press, London, 1967).

5. H. COHEN and H. W. LENSTRA, JR., 'Heuristics on class groups of number fields', *Number theory, Noordwijkerhout* 1983, Lecture Notes in Mathematics 1068 (Springer, Berlin, 1984) 33–62.

6. H. COHEN and J. MARTINET, 'Class groups of number fields: numerical heuristics', *Math. Comp.* 48 (1987) 123–137.

7. H. COHEN and J. MARTINET, 'Étude heuristique des groupes de classes des corps de nombres', *J. reine angew. Math.* 404 (1990) 39–76.

8. C. W. CURTIS and I. REINER, *Methods of representation theory*, vol. I (John Wiley and Sons, New York, 1981).

9. B. DATSKOVSKY and D. J. WRIGHT, 'Density of discriminants of cubic fields', *J. reine angew. Math.* 386 (1988) 116–138.

10. H. DAVENPORT and H. HEILBRONN, 'On the density of discriminants of cubic fields. II', *Proc. Roy. Soc. Lond. A* 322 (1971) 405–420.

11. C. GREITHER, 'Some cases of Brumer's conjecture for abelian CM extensions of totally real fields', *Math. Z.* 233 (2000) 515–534.

12. P. R. HALMOS, *Measure theory*, Graduate Texts in Mathematics 18 (Springer, New York, 1974).

13. G. H. HARDY and M. RIESZ, *The general theory of Dirichlet's series* (Cambridge University Press, Cambridge, 1915).

14. S. LANG, *Algebraic number theory*, 2nd edn, Graduate Texts in Mathematics 110 (Springer, New York, 1986).

15. G. MALLE, 'Cohen–Lenstra heuristics and roots of unity', *J. Number Theory* 128 (2008) 2823–2835.

16. B. MAZUR and A. WILES, 'Class fields of abelian extensions of $\mathbb{Q}$', *Invent. Math.* 76 (1984) 179–330.

17. Z. M. OU and K. S. WILLIAMS, 'On the density of cyclic quartic fields', *Canad. Math. Bull.* 44 (2001) 97–104.

18. I. REINER, *Maximal orders* (Academic Press, London, 1975).

19. J. ROSENBERG, *Algebraic K-theory and its applications*, Graduate Texts in Mathematics 147 (Springer, New York, 1994).

20. R. SCHOOF, 'Computing Arakelov class groups', *Algorithmic number theory*, MSRI Publications 44 (Cambridge University Press, Cambridge, 2008) 447–495.

21. M. M. WOOD, 'On the probabilities of local behaviors in abelian field extensions', *Compos. Math.* 146 (2010) 102–128.

Alex Bartel
School of Mathematics and Statistics
University of Glasgow
University Place
Glasgow G12 8SQ
United Kingdom

alex.bartel@glasgow.ac.uk

Hendrik W. Lenstra Jr.
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
RA Leiden 2300
The Netherlands

hwl@math.leidenuniv.nl