Received: 30 September 2022 | Revised: 23 February 2023 | Accepted: 21 February 2023

DOI: 10.1112/jlms.12737

RESEARCH ARTICLE

Journal of the London Mathematical Society

Distribution of genus numbers of abelian number fields

Christopher Frei[1] | **Daniel Loughran**[2] | **Rachel Newton**[3]

[1]TU Graz, Institute of Analysis and Number Theory, Graz, Austria

[2]Department of Mathematical Sciences, University of Bath, Claverton Down, Bath, UK

[3]Department of Mathematics, King's College London, Strand, London, UK

Correspondence
Christopher Frei, TU Graz, Institute of Analysis and Number Theory, Steyrergasse 30/II, Graz, Austria.
Email: frei@math.tugraz.at

Funding information
EPSRC, Grant/Award Numbers: EP/T01170X/1, EP/T01170X/2, EP/S004696/1, EP/S004696/2; UKRI Future Leaders Fellowship, Grant/Award Numbers: MR/V021362/1, MR/T041609/1, MR/T041609/2

Abstract

We study the quantitative behaviour of genus numbers of abelian extensions of number fields with given Galois group. We prove an asymptotic formula for the average value of the genus number and show that any given genus number appears only 0% of the time.

MSC 2020
11R37 (primary), 11R45, 43A70, 11R29 (secondary)

Contents

1 INTRODUCTION

Let k be a number field. The Cohen–Lenstra heuristics give a prediction for the distribution of the odd part of the class groups of quadratic extensions of k [2]. These are known for the 3-torsion in the class group [3, 4], but are wide open in general. On the other hand, the 2-torsion in the class group of a quadratic extension admits a very simple description via Gauss's genus theory. It is this part of the class group that we shall focus on in this paper, in the more general setting of genus numbers of abelian extensions. There has been a recent interest in statistics regarding the genus group for other classes of field extensions, for example for cubic and quintic extensions [15, 16], with the only previous cases considered in the abelian setting being cyclic extensions of $\mathbb{Q}$ of prime degree [14]. The definition of the genus group for an abelian extension is as follows.

Definition 1.1. Let K/k be an abelian extension. The *genus field* of K/k is the largest extension $\mathfrak{G}_{K/k}$ of K that is unramified at all places of K and such that $\mathfrak{G}_{K/k}$ is an abelian extension of k. The *genus group* of K/k is the Galois group $\mathrm{Gal}(\mathfrak{G}_{K/k}/K)$. The *genus number* $\mathfrak{g}_{K/k}$ of K/k is the size of the genus group.

At archimedean places, we use the convention that $\mathbb{C}/\mathbb{R}$ is ramified.

By class field theory, there is a tower of fields $K \subset \mathfrak{G}_{K/k} \subset H_K$. Here H_K is the Hilbert class field of K and the class group $\mathrm{Cl}(K)$ of K is canonically isomorphic to $\mathrm{Gal}(H_K/K)$. The subgroup $\mathrm{Gal}(H_K/\mathfrak{G}_{K/k}) \subset \mathrm{Cl}(K)$ is called the *principal genus* of K/k and the genus group is the quotient $\mathrm{Cl}(K)/\,\mathrm{Gal}(H_K/\mathfrak{G}_{K/k})$ of the class group. Our main theorem concerns the average size of the genus number as one sums over all abelian extensions of bounded conductor with given Galois group. Write $\Phi(K/k)$ for the absolute norm of the conductor of K (viewed as an ideal in k).

Theorem 1.2. *Let G be a non-trivial finite abelian group. Then*

$$\sum_{\substack{\mathrm{Gal}(K/k)\cong G \\ \Phi(K/k)\leqslant B}} \mathfrak{g}_{K/k} \sim cB(\log B)^{\varrho(k,G)-1},$$

for some positive constant c, where

$$\varrho(k,G) = \sum_{g\in G\setminus\{\mathrm{id}_G\}} \frac{\mathrm{ord}\, g}{[k(\mu_{\mathrm{ord}\, g}) : k]}. \tag{1.1}$$

Our main result (Theorem 3.5) also gives an explicit expression for the leading constant in the asymptotic formula. To prove our results, we consider the Dirichlet series

$$\sum_{\substack{\mathrm{Gal}(K/k)\cong G \\ \Phi(K/k)\leqslant B}} \frac{\mathfrak{g}_{K/k}}{\Phi(K/k)^s}.$$

Using class field theory, we may rewrite this in terms of an idelic series, as the genus number has an idelic interpretation (Lemma 3.1). We then use Poisson summation to express this series in terms of the Dedekind zeta function of k.

Remark 1.3. It is illustrative to compare the asymptotic in Theorem 1.2 with the unweighted count of G-extensions, first established in [20]:

$$\sum_{\substack{\mathrm{Gal}(K/k)\cong G \\ \Phi(K/k)\leqslant B}} 1 \sim c' B(\log B)^{\omega(k,G)-1}, \quad \omega(k,G) = \sum_{g\in G\setminus\{\mathrm{id}_G\}} \frac{1}{[k(\mu_{\mathrm{ord}\, g}) : k]}.$$

In particular, one can interpret Theorem 1.2 as saying that the average value of the genus number is

$$\frac{c}{c'}(\log \Phi(K/k))^{\sum_{g\in G\setminus\{\mathrm{id}_G\}}(\mathrm{ord}\, g-1)/[k(\mu_{\mathrm{ord}\, g}):k]}.$$

Note that this behaviour is in stark contrast to the case of cubic and quintic extensions [15, 16] of $\mathbb{Q}$ (ordered by discriminant), where the average value of the genus number is constant.

Example 1.4.

(1) For ℓ prime, we have

$$\varrho(k, \mathbb{Z}/\ell\mathbb{Z}) = \frac{\ell(\ell-1)}{[k(\mu_\ell) : k]}.$$

In the case $k = \mathbb{Q}$, this recovers [14, Theorem 4.2] (here $\varrho(\mathbb{Q}, \mathbb{Z}/\ell\mathbb{Z}) = \ell$). All other cases are new. The following examples are all completely new.

(2) Biquadratic extensions:

$$\varrho(k, (\mathbb{Z}/2\mathbb{Z})^2) = 6.$$

(3) A cyclic extension of non-prime degree:

$$\varrho(k, \mathbb{Z}/4\mathbb{Z}) = \begin{cases} 6, & \mu_4 \not\subset k \\ 10, & \mu_4 \subset k. \end{cases}$$

Remark 1.3 and the case of quadratic fields suggest that there should be very few G-extensions with any fixed genus number g. Our next theorem confirms this by showing that every genus number occurs at most 0% of the time. Again, this is in stark contrast to the results for cubic and quintic extensions ordered by discriminant [15, 16].

Theorem 1.5. *Let k be a number field, G a non-trivial finite abelian group and $g \in \mathbb{N}$. Then*

$$\lim_{B\to\infty} \frac{|\{K/k \ :\ \mathrm{Gal}(K/k)\cong G,\ \Phi(K/k)\leqslant B \text{ and } \mathfrak{g}_{K/k} = g\}|}{|\{K/k \ :\ \mathrm{Gal}(K/k)\cong G,\ \Phi(K/k)\leqslant B\}|} = 0.$$

2 | HARMONIC ANALYSIS

To prove Theorem 1.2, we will use a formula for the genus number (Lemma 3.1) that expresses $\mathfrak{g}_{K/k}$ in terms of various invariants of the extension K/k. Most importantly for us, it reduces our task to counting abelian extensions for which a given unit is everywhere locally a norm, weighted by the products of the ramification indices. We will achieve this via a general result proved using harmonic analysis, which we state as Theorem 2.1. Let G be a finite abelian group, let F be a field and $\bar{F}$ a separable closure of F. We define a *sub-G-extension* of F to be a continuous homomorphism $\mathrm{Gal}(\bar{F}/F) \to G$. A sub-$G$-extension corresponds to a pair $(L/F, \psi)$, where L/F is a Galois extension inside $\bar{F}$ and ψ is an injective homomorphism $\mathrm{Gal}(L/F) \to G$. A *G-extension* of F is a surjective continuous homomorphism $\mathrm{Gal}(\bar{F}/F) \to G$.

Having fixed an algebraic closure $\bar{k}$ of the number field k, we write G-ext(k) for the set of G-extensions of k. For each place v of k, we fix an algebraic closure $\bar{k}_v$ and compatible embeddings $k \hookrightarrow \bar{k} \hookrightarrow \bar{k}_v$ and $k \hookrightarrow k_v \hookrightarrow \bar{k}_v$. Hence, a sub-$G$-extension φ of k induces a sub-G-extension φ_v of k_v at every place v. We write $\mathfrak{e}_v(\varphi) = \mathfrak{e}(\varphi_v) = \mathfrak{e}(L_v/k_v)$ for the ramification index of the extension L_v/k_v given by φ_v. Our main counting result is the following:

Theorem 2.1. *Let k be a number field, G a non-trivial finite abelian group and $\mathcal{A} \subset k^\times$ a finitely generated subgroup. Let S be a finite set of places of k and for $v \in S$ let Λ_v be a set of sub-G-extensions of k_v. For $v \notin S$ let Λ_v be the set of sub-G-extensions of k_v corresponding to those extensions of local fields L/k_v for which every element of $\mathcal{A}$ is a local norm from L/k_v. Let $\Lambda := (\Lambda_v)_{v\in\Omega_k}$. Then there exist $c_{k,G,\Lambda} \geqslant 0$ and $\delta = \delta(k, G, \mathcal{A}) > 0$ such that*

$$\sum_{\substack{\varphi\in G\text{-ext}(k)\\ \Phi(\varphi)\leqslant B\\ \varphi_v\in\Lambda_v\forall v\in\Omega_k}} \prod_v \mathfrak{e}_v(\varphi) = c_{k,G,\Lambda} B(\log B)^{\varrho(k,G,\mathcal{A})-1} + O(B(\log B)^{\varrho(k,G,\mathcal{A})-1-\delta}), \quad B \to \infty,$$

where

$$\varrho(k, G, \mathcal{A}) = \sum_{g\in G\setminus\{\mathrm{id}_G\}} \frac{\mathrm{ord}\, g}{[k_{\mathrm{ord}\, g} : k]} \quad \text{and} \quad k_d = k(\mu_d, \sqrt[d]{\mathcal{A}}).$$

Moreover, $c_{k,G,\Lambda} > 0$ if there exists a sub-G-extension of k that realises the given local conditions for all places v.

Theorem 2.1 has a very similar statement to [7, Theorem 3.1]; the primary difference is that the sum in Theorem 2.1 is weighted by the product of ramification indices $\prod_v \mathfrak{e}_v(\varphi)$. We prove Theorem 2.1 using the method, based upon harmonic analysis, that we developed to prove [7, Theorem 3.1], and many of the steps are formally similar. The ramification indices come into play when calculating the relevant local Fourier transforms, and these in turn change the singularity type of the resulting Dirichlet series. We now begin the proof of Theorem 2.1.

2.1 | Möbius inversion and Poisson summation

These steps are very similar to those taken in [6, Section 3] and [7, Section 3], so we shall be brief. To prove the result, we are free to increase the set S, so we assume that S contains all archimedean places of k and all places of k lying above the primes $p \leqslant |G|^2$. Moreover, we assume that $\mathcal{A} \subset \mathcal{O}_S^\times$ and that $\mathcal{O}_S$ has trivial class group. Let

$$f_{\Lambda_v} : \mathrm{Hom}(\mathrm{Gal}(\bar{k}_v/k_v), G) \to \mathbb{Z}, \quad \varphi_v \mapsto \mathbb{1}_{\Lambda_v}(\varphi_v)\mathfrak{e}_v(\varphi_v),$$

where $\mathfrak{e}_v(\varphi_v)$ denotes the ramification index of φ_v and $\mathbb{1}_{\Lambda_v}$ the indicator function of Λ_v. We let f_Λ be the product of the f_{Λ_v}. The Dirichlet series for our counting problem is

$$F(s) = \sum_{\varphi\in G\text{-ext}(k)} \frac{f_\Lambda(\varphi)}{\Phi(\varphi)^s}. \tag{2.1}$$

We perform Möbius inversion to write this as

$$F(s) = \sum_{H \subset G} \mu(G/H) \sum_{\varphi \in \mathrm{Hom}(\mathrm{Gal}(\bar{k}/k), H)} \frac{f_\Lambda(\varphi)}{\Phi(\varphi)^s}$$

where the sum is over subgroups H of G and μ denotes the Möbius function on isomorphism classes of finite abelian groups (cf. [7, Section 3.3.1]). By global class field theory, we have the identification

$$\mathrm{Hom}(\mathrm{Gal}(\bar{k}/k), H) = \mathrm{Hom}(\mathbf{A}_k^\times / k^\times, H),$$

where $\mathbf{A}_k^\times$ denotes the idèles of k. This allows us to view f_Λ as a function on $\mathrm{Hom}(\mathbf{A}_k^\times/k^\times, H)$, and leads to the expression

$$F(s) = \sum_{H \subset G} \mu(G/H) \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_k^\times/k^\times, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s}. \tag{2.2}$$

We approach the inner sums via Poisson summation. For each place v, we equip the finite group $\mathrm{Hom}(k_v^\times, H)$ with the unique Haar measure $\mathrm{d}\chi_v$ such that

$$\mathrm{vol}(\mathrm{Hom}(k_v^\times/\mathcal{O}_v^\times, H)) = 1$$

(for v archimedean, we take $\mathcal{O}_v = k_v$ by convention). The product of these measures yields a well-defined measure $\mathrm{d}\chi$ on $\mathrm{Hom}(\mathbf{A}_k^\times, H)$. We say that an element of $\mathrm{Hom}(k_v^\times, H)$ is *unramified* if it lies in the subgroup $\mathrm{Hom}(k_v^\times/\mathcal{O}_v^\times, H)$, that is, if it is trivial on $\mathcal{O}_v^\times$. The Pontryagin dual of $\mathrm{Hom}(\mathbf{A}_k^\times, H)$ is naturally identified with $\mathbf{A}_k^\times \otimes H^\wedge$, where $H^\wedge = \mathrm{Hom}(H, \mathbb{C}^\times)$ denotes the Pontryagin dual of H (similarly with $\mathbf{A}_k^\times$ replaced by $\mathbf{A}_k^\times/k^\times$ or $k_v^\times$; cf. [6, Section 3.1]).

The function f_Λ/Φ^s is a product of local functions f_{Λ_v}/Φ_v^s on $\mathrm{Hom}(k_v^\times, H)$, where $\Phi_v(\chi_v)$ is the reciprocal of the v-adic norm of the conductor of $\mathrm{Ker}\,\chi_v$. For $v \notin S$, these local functions take only the value 1 on the unramified elements by our choice of S, thus f_Λ/Φ^s extends to a well-defined continuous function on $\mathrm{Hom}(\mathbf{A}_k^\times, H)$. We define its Fourier transform to be

$$\widehat{f}_{\Lambda,H}(x; s) = \int_{\chi \in \mathrm{Hom}(\mathbf{A}_k^\times, H)} \frac{f_\Lambda(\chi)\langle \chi, x\rangle}{\Phi(\chi)^s} \mathrm{d}\chi,$$

where $x = (x_v)_v \in \mathbf{A}_k^\times \otimes H^\wedge$. Similarly, for $x_v \in k_v^\times \otimes H^\wedge$ we have the local Fourier transform

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \int_{\chi_v \in \mathrm{Hom}(k_v^\times, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi_v(\chi_v)^s} \mathrm{d}\chi_v.$$

For $\mathrm{Re}\, s \gg 1$, the global Fourier transform exists and defines a holomorphic function in this domain, and there is a Euler product decomposition

$$\widehat{f}_{\Lambda,H}(x; s) = \prod_v \widehat{f}_{\Lambda_v,H}(x_v; s). \tag{2.3}$$

As in [7, Proposition 3.9], applying Poisson summation one obtains the following:

$$\sum_{\chi\in\mathrm{Hom}(\mathbf{A}_k^\times/k^\times,H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s} = \frac{1}{|\mathcal{O}_k^\times\otimes H^\wedge|}\sum_{x\in\mathcal{O}_S^\times\otimes H^\wedge} \widehat{f}_{\Lambda,H}(x;s), \quad \mathrm{Re}\, s>1. \tag{2.4}$$

To analyse the Poisson sum, we need to calculate the Fourier transforms. We begin by studying the local Fourier transforms.

2.2 | Local Fourier transforms

We first give a formula for the ramification index via local class field theory. For any place v of k, we have the exact sequence

$$1\to\mathcal{O}_v^\times\to k_v^\times\to k_v^\times/\mathcal{O}_v^\times\to 1.$$

A choice of uniformiser gives an isomorphism $k_v^\times\cong\mathcal{O}_v^\times\bigoplus k_v^\times/\mathcal{O}_v^\times$ and thus

$$\mathrm{Hom}(k_v^\times,H)\cong\mathrm{Hom}(\mathcal{O}_v^\times,H)\bigoplus\mathrm{Hom}(k_v^\times/\mathcal{O}_v^\times,H).$$

For a character $\chi_v : k_v^\times\to H$, we write its decomposition as

$$\chi_v=(\chi_{v,\mathrm{r}},\chi_{v,\mathrm{nr}})$$

($\chi_{v,\mathrm{r}}$ is the 'ramified part' and $\chi_{v,\mathrm{nr}}$ is the 'non-ramified part'). The following lemma is standard class field theory; we include its proof for completeness.

Lemma 2.2. *We have* $\mathfrak{e}_v(\chi_v)=|\chi_v(\mathcal{O}_v^\times)|=|\operatorname{im}\chi_{v,r}|$. *If* χ_v *is tamely ramified then* $\operatorname{im}\chi_{v,r}$ *is a cyclic group and therefore* $\mathfrak{e}_v(\chi_v)=\mathrm{ord}(\chi_{v,r})$.

Proof. The result for v archimedean is immediate so let us assume that v is non-archimedean. Let K_w denote the field extension of k_v corresponding via class field theory to χ_v, and write $\mathcal{O}_w$ for the ring of integers of K_w. Let $\mathrm{ord}_v : k_v^\times\twoheadrightarrow\mathbb{Z}$ be the normalised valuation on k_v and let $\mathrm{ord}_w :$ $K_w^\times\twoheadrightarrow\mathbb{Z}$ be the normalised valuation on K_w. As $\mathrm{ord}_v=\frac{1}{\mathfrak{e}_v(\chi_v)}\mathrm{ord}_w$ and $[K_w : k_v]=\mathfrak{e}_v(\chi_v)\mathfrak{f}_v(\chi_v)$, where $\mathfrak{f}_v$ denotes the residue degree, the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_w^\times \arrow[r] \arrow[d, "N_{K_w/k_v}"] & K_w^\times \arrow[r, "\mathrm{ord}_w"] \arrow[d, "N_{K_w/k_v}"] & \mathbb{Z} \arrow[r] \arrow[d, "\mathfrak{f}_v(\chi_v)"] & 0 \\
0 \arrow[r] & \mathcal{O}_v^\times \arrow[r] & k_v^\times \arrow[r, "\mathrm{ord}_v"] & \mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

The snake lemma gives an exact sequence

$$0\to\mathcal{O}_v^\times/N_{K_w/k_v}(\mathcal{O}_w^\times)\to k_v^\times/N_{K_w/k_v}(K_w^\times)\to\mathbb{Z}/\mathfrak{f}_v(K)\mathbb{Z}\to 0.$$

The local reciprocity map gives an isomorphism $k_v^\times/N_{K_w/k_v}(K_w^\times) \to \mathrm{Gal}(K_w/k_v)$, whereby $|k_v^\times/N_{K_w/k_v}(K_w^\times)| = [K_w : k_v] = \mathfrak{e}_v(\chi_v)\mathfrak{f}_v(\chi_v)$. Therefore,

$$\mathfrak{e}_v(\chi_v) = |\mathcal{O}_v^\times/N_{K_w/k_v}(\mathcal{O}_w^\times)| = |\mathcal{O}_v^\times/\operatorname{Ker}\chi_{v,\mathrm{r}}|,$$

as required. Now let $\mathfrak{m}_v$ denote the maximal ideal of $\mathcal{O}_v$. If K_w/k_v is tamely ramified then $1 + \mathfrak{m}_v \subset N_{K_w/k_v}(\mathcal{O}_w^\times) = \operatorname{Ker}\chi_{v,\mathrm{r}}$ and hence the cyclic group $\mathbb{F}_v^\times$ surjects onto $\operatorname{im}\chi_{v,\mathrm{r}}$. □

Lemma 2.3. *Let $v \notin S$. The function f_{Λ_v} is $\mathrm{Hom}(k_v^\times/\mathcal{O}_v^\times, H)$-invariant and $f_{\Lambda_v}(\psi_v) = 1$ for all $\psi_v \in \mathrm{Hom}(k_v^\times/\mathcal{O}_v^\times, H)$.*

Proof. This follows from Lemma 2.2 and [7, Lemma 3.7]. □

For $x \in k^\times \otimes H^\wedge$, we denote by x_v the image of x under $k^\times \otimes H^\wedge \to k_v^\times \otimes H^\wedge$. By $\mathcal{A}_v$ we denote the image of our finitely generated subgroup $\mathcal{A} \subset k^\times$ under $k^\times \subset k_v^\times$. Recall that, by our choice of S, we have $\mathcal{A}_v \subset \mathcal{O}_v^\times$ for all $v \notin S$.

Lemma 2.4. *For $v \notin S$ and $x \in \mathcal{O}_S^\times \otimes H^\wedge$, let*

$$s_{x,H}(v) = -1 + \sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{A}_v, H)} \mathrm{ord}(\chi_v)\langle \chi_v, x_v\rangle.$$

Then

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = 1 + \frac{s_{x,H}(v)}{q_v^s}.$$

Proof. Using Lemma 2.3 and following the proof of [7, Lemma 3.8] gives

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi(\chi_v)^s}.$$

Now mimic the start of the proof of [7, Lemma 3.10] and apply Lemma 2.2 to obtain the result. □

2.3 | Frobenian functions

We will analyse the global Fourier transforms using the theory of frobenian functions from Serre's book [18, Section 3.3]. The parts of the theory relevant for us are also summarised in [7, Section 2]. Recall that a *class function* on a group is a function that is constant on conjugacy classes.

Definition 2.5. Let k be a number field and $\rho : \Omega_k \to \mathbb{C}$ a function on the set of places of k. Let S be a finite set of places of k. We say that ρ is *S-frobenian* if there exist

(a) a finite Galois extension K/k, with Galois group Γ, such that S contains all places that ramify in K/k, and
(b) a class function $\varphi : \Gamma \to \mathbb{C}$,

such that for all $v \notin S$ we have

$$\rho(v) = \varphi(\mathrm{Frob}_v),$$

where $\mathrm{Frob}_v \in \Gamma$ denotes the Frobenius element of v. We say that ρ is *frobenian* if it is S-frobenian for some S. A subset of Ω_k is called (S-)*frobenian* if its indicator function is (S-)frobenian.

In Definition 2.5, we adopt a common abuse of notation (see [18, Section 3.2.1]), and denote by $\mathrm{Frob}_v \in \Gamma$ the choice of some element of the Frobenius conjugacy class at v; note that $\varphi(\mathrm{Frob}_v)$ is well-defined as φ is a class function. We define the *mean* of ρ to be

$$m(\rho) = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\varphi(\gamma) \in \mathbb{C}.$$

2.4 | Global Fourier transforms

Our next aim is to show that the function $s_{x,H}$ from Lemma 2.4 is frobenian. This will allow us to obtain analytic continuations of the corresponding global Fourier transforms (possibly with branch point singularities).

For $x_v \in \mathcal{O}_v^\times \otimes H^\wedge$, we abuse notation slightly and write $x_v \in \mathcal{O}_v^{\times d} \otimes H^\wedge$ if x_v is in the image of the not necessarily injective map $\mathcal{O}_v^{\times d} \otimes H^\wedge \to \mathcal{O}_v^\times \otimes H^\wedge$.

Lemma 2.6. *Let $x \in \mathcal{O}_S^\times \otimes H^\wedge$ and let e be the exponent of H. For $v \notin S$, let*

$$d_{x,H}(v) = \max\{d \mid \gcd(e, q_v - 1) : x_v \in \mathcal{O}_v^{\times d} \otimes H^\wedge\},$$

$$d_{\mathcal{A},H}(v) = \max\{d \mid \gcd(e, q_v - 1) : \mathcal{A} \bmod v \subseteq \mathbb{F}_v^{\times d}\}.$$

Then any function $\Omega_k \to \mathbb{C}$ whose restriction to $\Omega_k \setminus S$ is either $d_{x,H}$ or $d_{\mathcal{A},H}$ is S-frobenian.

Proof. We choose a presentation $H^\wedge = \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_l\mathbb{Z}$, thus identifying $x \in \mathcal{O}_S^\times \otimes H^\wedge$ with a tuple $(x_1\mathcal{O}_S^{\times n_1}, \dots, x_l\mathcal{O}_S^{\times n_l}) \in \mathcal{O}_S^\times/\mathcal{O}_S^{\times n_1} \oplus \cdots \oplus \mathcal{O}_S^\times/\mathcal{O}_S^{\times n_l}$. Then $x_v \in \mathcal{O}_v^{\times d} \otimes H^\wedge$ if and only if $x_i \in \mathcal{O}_v^{\times (d,n_i)}$ for all $1 \leqslant i \leqslant l$.

For all $d \mid e$, let $K_d = k(\mu_d, x_1^{1/\gcd(d,n_1)}, \dots, x_l^{1/\gcd(d,n_l)})$, and define the sets

$$\mathrm{Y}_d = \mathrm{Gal}(K_e/K_d) \setminus \bigcup_{\substack{d' \mid \frac{e}{d} \\ d' \neq 1}} \mathrm{Gal}(K_e/K_{dd'}) \subset \mathrm{Gal}(K_e/k).$$

The Y_d form a partition of $\mathrm{Gal}(K_e/k)$, and each Y_d is conjugacy invariant because the involved subgroups are normal. A place $v \notin S$ satisfies $\mathrm{Frob}_v \in \mathrm{Y}_d$ if and only if d is the largest divisor of e such that v splits completely in K_d. By the observations made at the start of this proof, v splits completely in K_d if and only if $d \mid q_v - 1$ and $x_v \in \mathcal{O}_v^{\times d} \otimes H^\wedge$.

Hence, if $\varphi : \mathrm{Gal}(K_e/k) \to \mathbb{C}$ is the class function that takes the value d on Y_d, then $d_{x,H}(v) = \varphi(\mathrm{Frob}_v)$ for all $v \notin S$.

That $d_{\mathcal{A},H}$ is S-frobenian is proved in [7, Lemma 3.11]. The proof is similar to the above and we briefly recall the relevant construction as we shall use it later. For every $d \mid e$, we define the number field $k_d = k(\mu_d, \sqrt[d]{\mathcal{A}})$. The subsets

$$\Sigma_d = \mathrm{Gal}(k_e/k_d) \setminus \bigcup_{\substack{d' \mid \frac{e}{d} \\ d' \neq 1}} \mathrm{Gal}(k_e/k_{dd'}) \subset \mathrm{Gal}(k_e/k)$$

are conjugacy invariant and form a partition of $\mathrm{Gal}(k_e/k)$. Let $\varphi : \mathrm{Gal}(k_e/k) \to \mathbb{C}$ be the class function that takes the constant value d on Σ_d, for all $d \mid e$. Then $d_{\mathcal{A},H}(v) = \varphi(\mathrm{Frob}_v)$ for all $v \notin S$, so in particular it is S-frobenian. □

Proposition 2.7. *Let $x \in \mathcal{O}_S^\times \otimes H^\wedge$. Then any function $\Omega_k \to \mathbb{C}$ that sends $v \notin S$ to $s_{x,H}(v)$ is S-frobenian. Moreover, $s_{x,H}(v) \in \mathbb{R}$ for all $v \notin S$.*

Proof. For $v \notin S$, reduction modulo v yields an isomorphism $\mathrm{Hom}(\mathcal{O}_v^\times, H) \cong \mathrm{Hom}(\mathbb{F}_v^\times, H)$. If $m \mid q_v - 1$ is maximal with $\mathcal{A} \bmod v \subseteq \mathbb{F}_v^{\times m}$, then $\mathcal{A} \bmod v = \mathbb{F}_v^{\times m}$. This shows that any $\chi_v : \mathcal{O}_v^\times/\mathcal{A}_v \to H$ has order dividing $d_{\mathcal{A},H}(v)$, and for $m \mid d_{\mathcal{A},H}(v)$, the set $\{\chi_v : \mathcal{O}_v^\times/\mathcal{A}_v \to H : \chi_v \text{ has order } m\}$ can be naturally identified with $\{\chi_v : \mathcal{O}_v^\times \to H : \mathrm{Ker}\,\chi_v = \mathcal{O}_v^{\times m}\}$. Now Möbius inversion yields

$$\begin{aligned} 1 + s_{x,H}(v) &= \sum_{m \mid d_{\mathcal{A},H}(v)} m \sum_{\substack{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times, H) \\ \mathrm{Ker}\,\chi_v = \mathcal{O}_v^{\times m}}} \langle \chi_v, x_v \rangle \\ &= \sum_{m \mid d_{\mathcal{A},H}(v)} m \sum_{d \mid m} \mu\left(\frac{m}{d}\right) \sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{O}_v^{\times d}, H)} \langle \chi_v, x_v \rangle. \end{aligned}$$

Character orthogonality shows that for all $d \mid \gcd(e, q_v - 1)$ we have

$$\sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{O}_v^{\times d}, H)} \langle \chi_v, x_v \rangle = \begin{cases} |\mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{O}_v^{\times d}, H)| = |H[d]| & \text{if } d \mid d_{x,H}(v), \\ 0 & \text{otherwise,} \end{cases}$$

where $d_{x,H}(v)$ was defined in Lemma 2.6. Letting

$$F(A, B) = -1 + \sum_{m \mid A} m \sum_{d \mid \gcd(m,B)} \mu\left(\frac{m}{d}\right) |H[d]|, \tag{2.5}$$

we have shown that $s_{x,H}(v) = F(d_{\mathcal{A},H}(v), d_{x,H}(v))$. This is S-frobenian, as the functions $v \mapsto d_{\mathcal{A},H}(v)$ and $v \mapsto d_{x,H}(v)$ are S-frobenian by Lemma 2.6. From (2.5) it is also clear that $s_{x,H}(v) \in \mathbb{R}$. □

Again, we abuse notation and denote by $\mathcal{A}_v \otimes H^\wedge$ the image of the not necessarily injective map $\mathcal{A}_v \otimes H^\wedge \to k_v^\times \otimes H^\wedge$. For $v \notin S$, we have $\mathcal{A}_v \otimes H^\wedge \subseteq \mathcal{O}_v^\times \otimes H^\wedge$.

Proposition 2.8. *Let $\varrho(k, H, \mathcal{A})$ be defined as in Theorem 2.1 (with G replaced by H) and let $\varrho(k, H, \mathcal{A}, x) \in \mathbb{R}$ denote the mean of an S-frobenian function given by $s_{x,H}$ from Proposition 2.7.*

(1) *For all $x \in \mathcal{O}_S^\times \otimes H^\wedge$, we have $\varrho(k, H, \mathcal{A}, x) \leqslant \varrho(k, H, \mathcal{A}, 1)$, with equality if and only if $x_v \in \mathcal{A}_v \otimes H^\wedge\ \forall v \notin S$.*
(2) *We have $\varrho(k, H, \mathcal{A}, 1) = \varrho(k, H, \mathcal{A})$.*

Proof. Part (1) is clear because, by definition of $s_{x,H}$ and character orthogonality, for all $v \notin S$ we have $s_{x,H}(v) \leqslant s_{1,H}(v)$, with equality if and only if $\langle \chi_v, x_v \rangle = 1$ for all $\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{A}_v, H)$. For part (2), writing $k_d = k(\mu_d, \sqrt[d]{\mathcal{A}})$, it suffices to show that the mean of $s_{1,H}(v) + 1$ equals $\sum_{h \in H} \frac{\operatorname{ord} h}{[k_{\operatorname{ord} h} : k]}$. By definition, for $v \notin S$ we have

$$s_{1,H}(v) + 1 = \sum_{\chi_v : \mathcal{O}_v^\times/\mathcal{A}_v \to H} \operatorname{ord}(\chi_v).$$

We have $\mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{A}_v, H) \cong \mathrm{Hom}(\mathbb{F}_v^\times/(\mathcal{A} \bmod v), H) \cong H[d_{\mathcal{A},H}(v)]$ as abelian groups, where $d_{\mathcal{A},H}(v)$ is as in Lemma 2.6. Hence,

$$s_{1,H}(v) + 1 = \sum_{h \in H[d_{\mathcal{A},H}(v)]} \operatorname{ord} h.$$

We now recall from the proof of Lemma 2.6 that the function $d_{\mathcal{A},H}(v)$ is S-frobenian with associated Galois group $\mathrm{Gal}(k_e/k)$, where $e = \exp(H)$, determined by the subsets Σ_d. Using inclusion–exclusion, the mean of $s_{1,H}(v) + 1$ equals

$$\begin{aligned}
\frac{1}{[k_e : k]} \sum_{d \mid e} |\Sigma_d| \sum_{h \in H[d]} \operatorname{ord} h &= \frac{1}{[k_e : k]} \sum_{d \mid e} \sum_{c \mid \frac{e}{d}} \mu(c)[k_e : k_{cd}] \sum_{h \in H[d]} \operatorname{ord} h \\
&= \sum_{d \mid e} \sum_{c \mid \frac{e}{d}} \frac{\mu(c)}{[k_{cd} : k]} \sum_{h \in H[d]} \operatorname{ord} h \\
&= \sum_{f \mid e} \frac{1}{[k_f : k]} \sum_{d \mid f} \mu(f/d) \sum_{h \in H[d]} \operatorname{ord} h \\
&= \sum_{f \mid e} \frac{f|H_f|}{[k_f : k]},
\end{aligned}$$

where H_f denotes the set of elements of H of order f. It is clear that

$$\sum_{f \mid e} \frac{f|H_f|}{[k_f : k]} = \sum_{h \in H} \frac{\operatorname{ord} h}{[k_{\operatorname{ord} h} : k]},$$

whence the claim. □

Proposition 2.9. *Let $x \in \mathcal{O}_S^\times \otimes H^\wedge$. The Fourier transform satisfies*

$$\widehat{f}_{\Lambda,H}(x; s) = \zeta_k(s)^{\varrho(k,H,\mathcal{A},x)} G(H, x; s), \quad \operatorname{Re} s > 1,$$

for a holomorphic function $G(s) = G(H, x; s)$ on the region

$$\operatorname{Re} s > 1 - \frac{c}{\log(|\operatorname{Im} s| + 3)},$$

for some $c > 0$, satisfying in this region the bound

$$|G(s)| \ll (1 + |\operatorname{Im} s|)^{1/2}.$$

Moreover,

$$\lim_{s\to 1}(s-1)^{\varrho(k,H,\mathcal{A},x)}\widehat{f}_{\Lambda,H}(x;s) = (\operatorname{Res}_{s=1}\zeta_k(s))^{\varrho(k,H,\mathcal{A},x)} \prod_{v\in\Omega_k} \frac{\widehat{f}_{\Lambda_v,H}(x_v;1)}{\zeta_{k,v}(1)^{\varrho(k,H,\mathcal{A},x)}},$$

where $\zeta_{k,v}(s)$ denotes the Euler factor of the Dedekind zeta function $\zeta_k(s)$ of k at v if v is finite, and $\zeta_{k,v}(s) = 1$ otherwise. When $x = 1$ this limit is non-zero.

Proof. Recall the Euler product (2.3). The same argument as in [7, Lemma 3.6] shows that each single Euler factor $\widehat{f}_{\Lambda_v}(x_v;s)$ satisfies $\widehat{f}_{\Lambda_v}(x_v;s) \ll_{k,H} 1$ on $\operatorname{Re}(s) > 0$ and $\widehat{f}_{\Lambda_v}(1;s) > 0$ for $s \in \mathbb{R}$. We use these facts to control the finite product $\prod_{v\in S}\widehat{f}_{\Lambda_v}(x_v;s)$.

The proposition is then an application of [7, Proposition 2.3] to the Euler product $\prod_{v\notin S}\widehat{f}_{\Lambda_v,H}(x_v;s)$, which satisfies the hypotheses of [7, Proposition 2.3] by Lemma 2.4, Proposition 2.7 and the fact that $s_{x,H}(v) \leqslant |G|^2 - 1 < q_v$ by our assumption on S in Subsection 2.1 (cf. [7, Proposition 3.16]). □

2.5 | Proof of the asymptotic formula in Theorem 2.1

Recall from (2.1) the Dirichlet series $F(s)$ relevant to Theorem 2.1. Putting our results from (2.2) and (2.4) together, we have

$$F(s) = \sum_{H\subset G} \frac{\mu(G/H)}{|\mathcal{O}_k^\times \otimes H^\wedge|} \sum_{x\in\mathcal{O}_S^\times\otimes H^\wedge} \widehat{f}_{\Lambda,H}(x;s), \qquad \operatorname{Re} s > 1, \tag{2.6}$$

and the analytic properties of the Fourier transforms $\widehat{f}_{\Lambda,H}(x;s)$ were summarised in Proposition 2.9. For every proper subgroup $H \lneq G$, we see immediately from (1.1) that

$$\varrho(k,H,\mathcal{A}) < \varrho(k,G,\mathcal{A}). \tag{2.7}$$

An application of the Selberg–Delange method [19, Theorem II.5.3] now gives the following (cf. [7, Proposition 3.19]).

Proposition 2.10. *There exists $\delta = \delta(k,G,\mathcal{A}) > 0$ such that*

$$\sum_{\substack{\varphi\in G\text{-}ext(k)\\ \Phi(\varphi)\leqslant B\\ \varphi_v\in\Lambda_v \forall v\in S}} \prod_v \mathrm{e}_v(\varphi) = c_{k,G,\Lambda} B(\log B)^{\varrho(k,G,\mathcal{A})-1} + O(B(\log B)^{\varrho(k,G,\mathcal{A})-1-\delta}),$$

where

$$c_{k,G,\Lambda} = \frac{1}{\Gamma(\varrho(k,G,\mathcal{A}))|\mathcal{O}_k^\times \otimes G^\wedge|} \sum_{\substack{x\in\mathcal{O}_S^\times\otimes G^\wedge\\ \varrho(k,G,\mathcal{A},x)=\varrho(k,G,\mathcal{A})}} \lim_{s\to 1}(s-1)^{\varrho(k,G,\mathcal{A})}\widehat{f}_{\Lambda,G}(x;s).$$

Proposition 2.10 shows the validity of the asymptotic formula in Theorem 2.1, so all that remains is to study the leading constant $c_{k,G,\Lambda}$ and prove its positivity under certain assumptions.

2.6 | The leading constant in Theorem 2.1

We first determine which x contribute to the leading constant. Recall that for $x \in k^\times \otimes G^\wedge$, we denote by x_v the image of x under $k^\times \otimes G^\wedge \to k_v^\times \otimes G^\wedge$, and by $\mathcal{A}_v \otimes G^\wedge$ the image of the map $\mathcal{A}_v \otimes G^\wedge \to k_v^\times \otimes G^\wedge$. Recall from [7, Lemma 3.20] the set $\mathcal{X}(k, G, \mathcal{A})$ defined as

$$\mathcal{X}(k, G, \mathcal{A}) = \{x \in k^\times \otimes G^\wedge \,:\, x_v \in \mathcal{A}_v \otimes G^\wedge \text{ for all but finitely many } v\}.$$

In [7, Lemma 3.20], it is shown that $\mathcal{X}(k, G, \mathcal{A})$ is finite and

$$\mathcal{X}(k, G, \mathcal{A}) = \{x \in \mathcal{O}_S^\times \otimes G^\wedge \,:\, x_v \in \mathcal{A}_v \otimes G^\wedge \text{ for all } v \notin S\}. \tag{2.8}$$

Lemma 2.11. *For $x \in \mathcal{O}_S^\times \otimes G^\wedge$, we have*

$$\varrho(k, G, \mathcal{A}, x) = \varrho(k, G, \mathcal{A}) \iff x \in \mathcal{X}(k, G, \mathcal{A}).$$

Moreover, $\widehat{f}_{\Lambda_v,G}(x_v; 1) = \widehat{f}_{\Lambda_v,G}(1; 1)$ for $x \in \mathcal{X}(k, G, \mathcal{A})$ and $v \notin S$.

Proof. Let $x \in \mathcal{O}_S^\times \otimes G^\wedge$ and $v \notin S$. Recall that $s_{x,G}(v) \in \mathbb{R}$ by Proposition 2.7. From the definition of $s_{x,G}(v)$ in Lemma 2.4, we see that $s_{x,G}(v) \leqslant s_{1,G}(v)$, with equality if and only if $\langle \chi_v, x_v\rangle = 1$ for all $\chi_v \in \mathrm{Hom}(\mathcal{O}_v^\times/\mathcal{A}_v, G)$. The latter condition holds if and only if $x_v \in \mathcal{A}_v \otimes G^\wedge$. Hence, we see that

$$s_{x,G}(v) = s_{1,G}(v) \text{ for all } v \notin S \iff x \in \mathcal{X}(k, G, \mathcal{A}). \tag{2.9}$$

The equivalence in the lemma follows, as $s_{x,G}(v) \leqslant s_{1,G}(v)$ holds for all $v \notin S$ and both functions are S-frobenian by Proposition 2.7.

The equality of Fourier transforms follows from Lemma 2.4 and (2.8). $\square$

Theorem 2.12. *Under the assumptions of Theorem 2.1 and the additional assumptions on S imposed at the start of Subsection 2.1, the leading constant $c_{k,G,\Lambda}$ has the form*

$$c_{k,G,\Lambda} = \frac{(\mathrm{Res}_{s=1}\, \zeta_k(s))^{\varrho(k,G,\mathcal{A})}}{\Gamma(\varrho(k,G,\mathcal{A}))|\mathcal{O}_k^\times \otimes G^\wedge||G|^{|S_f|}} \prod_{v\notin S}\left(\sum_{\substack{\chi_v\in \mathrm{Hom}(\mathcal{O}_v^\times, G)\\ \mathcal{A}_v\subset \mathrm{Ker}\,\chi_v}} \frac{\mathrm{ord}\,\chi_v}{\Phi_v(\chi_v)}\right)\zeta_{k,v}(1)^{-\varrho(k,G,\mathcal{A})}$$

$$\times \sum_{\substack{\chi\in\mathrm{Hom}(\prod_{v\in S} k_v^\times, G)\\ \chi_v\in\Lambda_v \forall v\in S}} \left(\prod_{v\in S} \frac{\mathfrak{e}_v(\chi_v)}{\Phi_v(\chi_v)\zeta_{k,v}(1)^{\varrho(k,G,\mathcal{A})}}\right) \sum_{x\in\mathcal{X}(k,G,\mathcal{A})} \prod_{v\in S} \langle \chi_v, x_v\rangle,$$

where S_f denotes the set of non-archimedean places in S, and the product over $v \notin S$ is non-zero. Moreover, $c_{k,G,\Lambda} > 0$ if there exists a sub-G-extension of k that realises the given local conditions for all places v.

Proof. The formula follows from writing the global Fourier transform as a product of local Fourier transforms, and applying Lemma 2.4, Proposition 2.9, Proposition 2.10 and Lemma 2.11 (cf. [7, Theorem 3.22]). It remains to show that $c_{k,G,\Lambda} > 0$ if there is a sub-G-extension $\varphi : \mathrm{Gal}(\bar{k}/k) \to G$ that satisfies $\varphi_v \in \Lambda_v$ for all $v \in S$. The argument is exactly the same as in [7, Section 3.8] and hence omitted. □

Theorem 2.1 follows immediately from Proposition 2.10 and Theorem 2.12.

3 | DISTRIBUTION OF GENUS NUMBERS

In this section, we use Theorem 2.1 to prove Theorem 1.2. We begin by studying some basic properties of genus numbers.

3.1 | Genus numbers

For a Galois extension K/k of number fields and places $v \in \Omega_k$ and $w_0 \in \Omega_K$ with $w_0 \mid v$, we have the following equalities of subsets of $k_v^\times$:

$$\mathrm{N}_{K/k} \prod_{w|v} \mathcal{O}_{K,w}^\times = \mathrm{N}_{K_{w_0}/k_v} \mathcal{O}_{K,w_0}^\times = \mathcal{O}_v^\times \cap \mathrm{N}_{K_{w_0}/k_v} K_{w_0}^\times = \mathcal{O}_v^\times \cap \mathrm{N}_{K/k} \prod_{w|v} K_w^\times.$$

Hence, being the norm of an idèle of K or of an *integral* idèle of K is the same for integral idèles of k. The following result is a special case of the main theorem of [11]. It gives a purely adelic interpretation of the genus number.

Lemma 3.1 (Furuta, [11, Section 5]). *Let K/k be abelian. Then*

$$\mathfrak{g}_{K/k} = \frac{h(k) \prod_{v \in \Omega_k} \mathfrak{e}_v(K)}{[K : k][\mathcal{O}_k^\times : \mathcal{O}_k^\times \cap \mathrm{N}_{K/k} \prod_{w \in \Omega_K} \mathcal{O}_{K,w}^\times]},$$

where $\mathfrak{e}_v(K)$ denotes the ramification index of a place of K above v.

We have the following simple observations.

Lemma 3.2. *Let e be the exponent of G. Then we have*

$$\left[\mathcal{O}_k^\times : \mathcal{O}_k^\times \cap \mathrm{N}_{K/k} \prod_{w \in \Omega_K} \mathcal{O}_{K,w}^\times\right] = \left[\mathcal{O}_k^\times / \mathcal{O}_k^{\times e} : (\mathcal{O}_k^\times \cap \mathrm{N}_{K/k} \prod_{w \in \Omega_K} \mathcal{O}_{K,w}^\times)/\mathcal{O}_k^{\times e}\right].$$

Proof. Third isomorphism theorem, as every element of $\mathcal{O}_k^{\times e}$ is everywhere locally a norm by local class field theory, as observed in [7, Lemma 4.4]. □

Lemma 3.3. *Let A be a finite group and $B \subset A$ a subgroup. Then*

$$\sum_{a\in A} \mathbb{1}_B(a) = |B| = |A|/[A : B].$$

Proof. Immediate. □

We use these as follows. For a finitely generated subgroup $\mathcal{A} \subset k^\times$, we let $f_{\mathcal{A}}$ be the indicator function for G-extensions from which every element of $\mathcal{A}$ is everywhere locally a norm. For cyclic subgroups $\langle\epsilon\rangle$, we abbreviate this to $f_\epsilon = f_{\langle\epsilon\rangle}$. Then, writing e for the exponent of G, Lemmas 3.2 and 3.3 give

$$\sum_{\epsilon\in\mathcal{O}_k^\times/\mathcal{O}_k^{\times e}} f_\epsilon(K) = \frac{[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]}{[\mathcal{O}_k^\times : \mathcal{O}_k^\times \cap \mathrm{N}_{K/k}\prod_{w\in\Omega_K}\mathcal{O}_{K,w}^\times]}.$$

(Note that f_ϵ is well-defined because every element of $\mathcal{O}_k^{\times e}$ is everywhere locally a norm, see [7, Lemma 4.4].)

Thus from Lemma 3.1, we obtain the following, which is the expression we will use to study the average value of the genus number.

Proposition 3.4. *We have*

$$\sum_{\substack{\mathrm{Gal}(K/k)\cong G\\ \Phi(K/k)\leqslant B}} \mathfrak{g}_{K/k} = \frac{h(k)}{[K:k][\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]}\sum_{\epsilon\in\mathcal{O}_k^\times/\mathcal{O}_k^{\times e}}\ \sum_{\substack{\mathrm{Gal}(K/k)\cong G\\ \Phi(K/k)\leqslant B}} f_\epsilon(K)\prod_{v\in\Omega_k}\mathfrak{e}_v(K).$$

3.2 | Proof of Theorem 1.2

In this section, we prove Theorem 3.5. This is a strengthening of Theorem 1.2 that allows finitely many local conditions and also gives an explicit constant.

Theorem 3.5. *Let k be a number field and G a finite abelian group with exponent e. Let S be a finite set of places of k satisfying the conditions imposed at the start of Subsection 2.1 for $\mathcal{A} = \mathcal{O}_k^\times$. For $v \in S$ let Λ_v be a set of sub-G-extensions of k_v. Then there exist $C_{k,G,\Lambda} \geqslant 0$ and $\delta = \delta(k,G) > 0$ such that*

$$\sum_{\substack{\varphi\in G\text{-}ext(k)\\ \Phi(\varphi)\leqslant B\\ \varphi_v\in\Lambda_v\forall v\in S}} \mathfrak{g}_{K_\varphi/k} = C_{k,G,\Lambda}B(\log B)^{\varrho(k,G)-1} + O(B(\log B)^{\varrho(k,G)-1-\delta}),\quad B\to\infty.$$

The leading constant $C_{k,G,\Lambda}$ equals

$$\frac{h(k)(\mathrm{Res}_{s=1}\zeta_k(s))^{\varrho(k,G)}}{\Gamma(\varrho(k,G))|\mathcal{O}_k^\times\otimes G^\wedge||G|^{|S_f|+1}[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]}\prod_{v\notin S}\left(\sum_{\chi_v\in\mathrm{Hom}(\mathcal{O}_v^\times,G)}\frac{\mathrm{ord}\,\chi_v}{\Phi_v(\chi_v)}\right)\zeta_{k,v}(1)^{-\varrho(k,G)}$$

$$\times\sum_{\epsilon\in\mathcal{O}_k^\times/\mathcal{O}_k^{\times e}\cap Ш_\omega(k,\mu_e)}\ \sum_{\substack{\chi\in\mathrm{Hom}(\prod_{v\in S}k_v^\times,G)\\ \chi_v\in\Lambda_v\forall v\in S\\ \epsilon_v\in\mathrm{Ker}\,\chi_v\forall v\in S}}\left(\prod_{v\in S}\frac{\mathfrak{e}_v(\chi_v)}{\Phi_v(\chi_v)\zeta_{k,v}(1)^{\varrho(k,G)}}\right)\sum_{x\in\mathcal{X}(k,G,1)}\prod_{v\in S}\langle\chi_v,x_v\rangle,$$

and $C_{k,G,\Lambda} > 0$ if there exists a sub-G-extension of k that realises the given local conditions for all places $v \in S$.

In this statement, we use some notation concerning Tate–Shafarevich groups, which we now introduce. For a number field k, commutative group scheme G over k, and a finite set of places S of k, we write

$$\text{Ш}_S(k,G) = \operatorname{Ker}\left(\mathrm{H}^1(k,G) \to \prod_{v\notin S} \mathrm{H}^1(k_v,G)\right), \quad \text{Ш}_\omega(k,G) = \varinjlim_{S} \text{Ш}_S(k,G).$$

We are interested in the case $G = \mu_n$, where by Kummer theory we have

$$\text{Ш}_\omega(k,\mu_n) = \{x \in k^\times/k^{\times n} \;:\; x_v \in k_v^{\times n} \text{ for all but finitely many } v\}.$$

The natural map $\mathcal{O}_k^\times/\mathcal{O}_k^{\times n} \to k^\times/k^{\times n}$ is injective and we write $\mathcal{O}_k^\times/\mathcal{O}_k^{\times n} \cap \text{Ш}_\omega(k,\mu_n)$ to mean the intersection taken inside $k^\times/k^{\times n}$.

Proof of Theorem 3.5. As in Proposition 3.4, we have

$$\sum_{\substack{\varphi\in G\text{-ext}(k)\\ \Phi(\varphi)\leqslant B\\ \varphi_v\in\Lambda_v \forall v\in S}} \mathfrak{g}_{K_\varphi/k} = \frac{h(k)}{|G|[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]} \sum_{\epsilon\in\mathcal{O}_k^\times/\mathcal{O}_k^{\times e}} \sum_{\substack{\varphi\in G\text{-ext}(k)\\ \Phi(\varphi)\leqslant B\\ \varphi_v\in\Lambda_v \forall v\in S}} f_\epsilon(K_\varphi) \prod_{v\in\Omega_k} \mathfrak{e}_v(K_\varphi), \tag{3.1}$$

where K_φ denotes the fixed field of $\operatorname{Ker}\varphi$ in $\bar{k}$ and e is the exponent of G.

We now prepare to apply Theorem 2.1. For $\epsilon \in k^\times$, define $(\Lambda,\epsilon) := ((\Lambda,\epsilon)_v)_{v\in\Omega_k}$ as follows. For $v \notin S$, let $(\Lambda,\epsilon)_v$ be the set of sub-G-extensions of k_v corresponding to those extensions of local fields L/k_v for which ϵ is a local norm from L/k_v. For $v \in S$, let $(\Lambda,\epsilon)_v$ be the subset of Λ_v consisting of those extensions L/k_v for which ϵ is a local norm from L/k_v. Note that this definition only depends on the image of ϵ in $k^\times/k^{\times e}$, and for $v \in S$ the set $(\Lambda,\epsilon)_v$ may be empty.

Applying Theorems 2.1 and 2.12 (with $\mathcal{A}$ generated by ϵ) to the inner sum of (3.1) yields

$$\sum_{\substack{\varphi\in G\text{-ext}(k)\\ \Phi(\varphi)\leqslant B\\ \varphi_v\in\Lambda_v \forall v\in S}} f_\epsilon(K_\varphi) \prod_{v\in\Omega_k} \mathfrak{e}_v(K_\varphi) = c_{k,G,(\Lambda,\epsilon)} B(\log B)^{\varrho(k,G,\epsilon)-1} + O(B(\log B)^{\varrho(k,G,\epsilon)-1-\delta}),$$

where

$$\varrho(k,G,\epsilon) = \sum_{g\in G\setminus\{\mathrm{id}_G\}} \frac{\operatorname{ord} g}{[k_{\operatorname{ord} g,\epsilon} : k]} \quad \text{and } k_{d,\epsilon} = k(\mu_d, \sqrt[d]{\epsilon}) \tag{3.2}$$

and $c_{k,G,(\Lambda,\epsilon)} \geqslant 0$ is as in Theorem 2.12, with local conditions coming from Λ and the requirement that ϵ is everywhere locally a norm. If these two sets of conditions are not compatible, that is, there are no G-extensions φ with $\varphi_v \in \Lambda_v$ for all $v \in S$ from which a given ϵ is everywhere locally a norm, then $c_{k,G,(\Lambda,\epsilon)} = 0$ and this ϵ does not contribute to the sum in (3.1). Note that if $c_{k,G,(\Lambda,1)} = 0$ then there are no G-extensions φ with $\varphi_v \in \Lambda_v$ for all $v \in S$ and hence $c_{k,G,(\Lambda,\epsilon)} = 0$ for all $\epsilon \in \mathcal{O}_k^\times/\mathcal{O}_k^{\times e}$. The next lemma shows that the main term in (3.1) comes from those ϵ lying in $\mathcal{O}_k^\times/\mathcal{O}_k^{\times e} \cap \text{Ш}_\omega(k,\mu_e)$.

Lemma 3.6. *We have $\varrho(k, G, \epsilon) \leqslant \varrho(k, G)$, with equality if and only if $\epsilon \in \mathcal{O}_k^\times / \mathcal{O}_k^{\times e} \cap Ш_\omega(k, \mu_e)$.*

Proof. It follows from the definition (3.2) that $\varrho(k, G, \epsilon) \leqslant \varrho(k, G, 1)$, with equality if and only if $\epsilon \in k(\mu_d)^{\times d}$ for all $d \mid e$. This is equivalent to $\epsilon \in k_v^{\times e}$ for all but finitely many places v of k (see [7, Theorem 1.6], for example). $\square$

Thus, the main term in (3.1) is

$$\frac{h(k)}{|G|[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]} \sum_{\epsilon \in \mathcal{O}_k^\times / \mathcal{O}_k^{\times e} \cap Ш_\omega(k, \mu_e)} \sum_{\substack{\varphi \in G\text{-ext}(k) \\ \Phi(\varphi) \leqslant B \\ \varphi_v \in \Lambda_v \forall v \in S}} f_\epsilon(K_\varphi) \prod_{v \in \Omega_k} \mathfrak{e}_v(K_\varphi)$$

$$= \frac{h(k)}{|G|[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]} \sum_{\epsilon \in \mathcal{O}_k^\times / \mathcal{O}_k^{\times e} \cap Ш_\omega(k, \mu_e)} c_{k,G,(\Lambda,\epsilon)} B (\log B)^{\varrho(k,G)-1} + O(B (\log B)^{\varrho(k,G)-1-\delta}).$$

Hence in the setting of Theorem 3.5, we obtain the stated asymptotic formula with the leading constant

$$C_{k,G,\Lambda} = \frac{h(k)}{|G|[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]} \sum_{\epsilon \in \mathcal{O}_k^\times / \mathcal{O}_k^{\times e} \cap Ш_\omega(k, \mu_e)} c_{k,G,(\Lambda,\epsilon)}. \tag{3.3}$$

Applying Theorem 2.12 to the term for $\epsilon = 1$ already shows that $C_{k,G,\Lambda}$ is positive if there exists a sub-G-extension of k that realises the local conditions imposed by Λ for all places $v \in S$. It remains to prove that $C_{k,G,\Lambda}$ has the form claimed in Theorem 3.5.

We begin by noting that the sum in (3.3) has either one or two terms. To see this, let 2^r be the largest power of 2 dividing e. It follows from [17, Theorem 9.1.11] that $Ш_\omega(k, \mu_e)$ is trivial unless $k(\mu_{2^r})/k$ is non-cyclic, in which case $Ш_\omega(k, \mu_e) \cong \mathbb{Z}/2\mathbb{Z}$ (see [7, Lemma 4.9]).

We next show that the elements $\epsilon \in \mathcal{O}_k^\times / \mathcal{O}_k^{\times e} \cap Ш_\omega(k, \mu_e)$ can only be non-trivial at a uniformly bounded (in terms of $[k : \mathbb{Q}]$) subset of the places in S. We write ϵ_v for the image of ϵ in $k_v^\times / k_v^{\times e}$. Recall that a place v of a number field L is said to *split* (or *decompose*) in an extension M/L if there exist at least two distinct places of M above v.

Lemma 3.7. *Let $\epsilon \in \mathcal{O}_k^\times / \mathcal{O}_k^{\times e} \cap Ш_\omega(k, \mu_e)$, where e is the exponent of G. Let 2^r be the largest power of 2 dividing e and let R be a set of places of k containing all places above 2 that do not split in $k(\mu_{2^r})/k$. Then $\epsilon_v \in k_v^{\times e}$ for all $v \notin R$.*

Proof. By definition, there exists a cofinite set of places T such that $\epsilon_v \in k_v^{\times e}$ for all $v \in T$. Let $U = \Omega_k \setminus R$. By Grunwald–Wang [17, Theorem 9.1.11], we have

$$\mathrm{Ker}\left(k^\times / k^{\times e} \to \prod_{v \in T} k_v^\times / k_v^{\times e} \right) = \mathrm{Ker}\left(k^\times / k^{\times e} \to \prod_{v \in T \cup U} k_v^\times / k_v^{\times e} \right),$$

proving that $\epsilon_v \in k_v^{\times e}$ for all $v \notin R$. $\square$

By Lemma 3.7 and (2.8), we have $\mathcal{X}(k, G, \epsilon) = \mathcal{X}(k, G, 1)$ for $\epsilon \in Ш_\omega(k, \mu_e)$. Together with Theorem 2.12, Lemma 3.6, Lemma 3.7 and our assumptions on S, this shows that, for

$\epsilon \in \mathcal{O}_k^\times/\mathcal{O}_k^{\times e} \cap \text{Ш}_\omega(k,\mu_e)$,

$$c_{k,G,(\Lambda,\epsilon)} = \frac{(\operatorname{Res}_{s=1}\zeta_k(s))^{\varrho(k,G)}}{\Gamma(\varrho(k,G))|\mathcal{O}_k^\times \otimes G^\wedge||G|^{|S_f|}} \prod_{v\notin S}\left(\sum_{\chi_v\in\operatorname{Hom}(\mathcal{O}_v^\times,G)} \frac{\operatorname{ord}\chi_v}{\Phi_v(\chi_v)}\right)\zeta_{k,v}(1)^{-\varrho(k,G)}$$
$$\times \sum_{\substack{\chi\in\operatorname{Hom}(\prod_{v\in S}k_v^\times,G)\\ \chi_v\in\Lambda_v\forall v\in S\\ \epsilon_v\in\operatorname{Ker}\chi_v\forall v\in S}} \left(\prod_{v\in S}\frac{\mathfrak{e}_v(\chi_v)}{\Phi_v(\chi_v)\zeta_{k,v}(1)^{\varrho(k,G)}}\right)\sum_{x\in\mathcal{X}(k,G,1)}\prod_{v\in S}\langle\chi_v,x_v\rangle.$$

Plugging this into (3.3) gives the correct leading constant for Theorem 3.5. □

3.3 | Remarks on Theorem 3.5

The constant c in Theorem 1.2 is equal to $C_{k,G,\Lambda}/|\operatorname{Aut}(G)|$, where $C_{k,G,\Lambda}$ is as in Theorem 3.5 and Λ_v is taken to be the set of all sub-G-extensions of k_v for each $v\in S$. This is because in the counting function in Theorem 1.2 we do not fix a choice of isomorphism from $\operatorname{Gal}(K/k)$ to G. Next, we observe that the exponent occurring in Theorem 1.2 is an integer.

Lemma 3.8. *The number $\varrho(k,G)$ is a non-negative integer.*

Proof. Let $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. We have

$$\varrho(k,G) = \sum_{n>1}\frac{n}{[k(\mu_n):k]}\#\{g\in G : \operatorname{ord} g = n\}.$$

It suffices to note that $[k(\mu_n):k] \mid \varphi(n)$ and that $\varphi(n)\mid \#\{g\in G : \operatorname{ord} g = n\}$, as if $g\in G$ has order n then so does g^a for all $1\leqslant a\leqslant n$ with $\gcd(a,n)=1$, and these elements are distinct. □

Next we show that the group $\mathcal{O}_k^\times/\mathcal{O}_k^{\times e}\cap\text{Ш}_\omega(k,\mu_e)$, which occurs in the formula for the constant $C_{k,G,\Lambda}$ in Theorem 3.5, can be non-trivial.

Example 3.9. Here we give an example of a number field k such that the map

$$\mathcal{O}_k^\times/\mathcal{O}_k^{\times 8} \to \prod_{v\in\Omega_k}\mathcal{O}_v^\times/\mathcal{O}_v^{\times 8}$$

is not injective and hence $\mathcal{O}_k^\times/\mathcal{O}_k^{\times e}\cap\text{Ш}_\omega(k,\mu_e)\cong\mathbb{Z}/2$.

Take $k=\mathbb{Q}(\sqrt{7})$. Then it is well-known that 16 is an 8th power everywhere locally in k, but not globally an 8th power (Wang's counter-example to Grunwald's theorem). Note that 2 is ramified in k, so that $(2)=\mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$. Then $\mathfrak{p}^8/(16)$ is the trivial ideal. But the class number of k is 1 so, writing $\mathfrak{p}=(a)$, we have that $a^8/16$ is a unit that is an 8th power everywhere locally but not an 8th power globally, as required.

Explicitly, we have $\mathfrak{p}=(3+\sqrt{7})$, so we may take $a=\sqrt{7}+3$. Then $u=a^8/16=32257+12192\sqrt{7}$ is the sought-after unit. Note that $u=\epsilon^4$, where $\epsilon=8+3\sqrt{7}$ is the fundamental unit.

4 | ZERO DENSITY WITH FIXED GENUS NUMBER

In this section, we prove Theorem 1.5. Let e again denote the exponent of G. From Lemma 3.1, we see at once that any G-extension K/k satisfies

$$\mathfrak{g}_{K/k} \geqslant \frac{h(k)}{|G|[\mathcal{O}_k^\times : \mathcal{O}_k^{\times e}]} \prod_{v \in \Omega_k} \mathfrak{e}_v(K) \gg 2^{\omega(K/k)},$$

where $\omega(K/k)$ denotes the number of places of k that ramify in K/k. With this observation, Theorem 1.5 follows immediately from the following result.

Theorem 4.1. *Let k be a number field, G a finite abelian group and $r \in \mathbb{N}$. Then*

$$\lim_{B \to \infty} \frac{|\{K/k \ :\ \mathrm{Gal}(K/k) \cong G,\ \Phi(K/k) \leqslant B \ \text{and}\ \omega(K/k) \leqslant r\}|}{|\{K/k \ :\ \mathrm{Gal}(K/k) \cong G,\ \Phi(K/k) \leqslant B\}|} = 0. \tag{4.1}$$

Proof. We show that the limit in (4.1) is smaller than any $\varepsilon > 0$. To this end, we will apply Chebyshev's inequality in the form of [8, Lemma 5.1], which is a straightforward generalisation of its special case [5, Lemma 3.1] for $k = \mathbb{Q}$.

Let z be a fixed positive constant, chosen sufficiently large in terms of k, G and ε. Write $P(z) = \{\mathfrak{p} \ :\ N(\mathfrak{p}) \leqslant z\}$ for the set of all non-zero prime ideals of $\mathcal{O}_k$ with norm bounded by z. Moreover, fix a sufficiently large finite set S_0 of places of k.

For any $B > 1$, let

$$\mathscr{A} = \{K/k \ :\ \mathrm{Gal}(K/k) \cong G \text{ and } \Phi(K/k) \leqslant B\}$$

and write $N = |\mathscr{A}|$. For any prime ideal $\mathfrak{p} \in S_0$, we take $\mathscr{A}_\mathfrak{p} = \mathscr{A}$. For $\mathfrak{p} \notin S_0$, we take

$$\mathscr{A}_\mathfrak{p} = \{K \in \mathscr{A} \ :\ \mathfrak{p} \text{ ramifies in } K\}.$$

For any distinct prime ideals $\mathfrak{p}, \mathfrak{q}$, write $\mathscr{A}_{\mathfrak{p},\mathfrak{q}} = \mathscr{A}_\mathfrak{p} \cap \mathscr{A}_\mathfrak{q}$. To determine the cardinalities of the sets $\mathscr{A}_\mathfrak{p}$ and $\mathscr{A}_{\mathfrak{p},\mathfrak{q}}$ asymptotically for $B \to \infty$, we apply [7, Theorem 3.1]. We take $\mathcal{A}$ in the statement of [7, Theorem 3.1] to be the trivial subgroup. For $v \in S_0$, we take $\Lambda_v = \mathrm{Hom}(k_v^\times, G)$. For $v \in S \setminus S_0$, we take

$$\Lambda_v = \{\chi \in \mathrm{Hom}(k_v^\times, G) \ :\ \chi \text{ is ramified}\}.$$

As S_0 is sufficiently large, the explicit description of the leading constant in [7, Theorem 3.22] applies to any finite set of places $S \supset S_0$. Hence, applying [7, Theorems 3.1 and 3.22] with $S = S_0$, $S = S_0 \cup \{\mathfrak{p}\}$ and $S = S_0 \cup \{\mathfrak{p}, \mathfrak{q}\}$, respectively, we obtain the estimates

$$\begin{aligned}
N = |\mathscr{A}| &= c_{k,G} B(\log B)^{\omega(k,G)-1} + O(B(\log B)^{\omega(k,G)-1-\alpha}),\\
|\mathscr{A}_\mathfrak{p}| &= \delta_\mathfrak{p} N + R_\mathfrak{p},\\
|\mathscr{A}_{\mathfrak{p},\mathfrak{q}}| &= \delta_\mathfrak{p}\delta_\mathfrak{q} N + R_{\mathfrak{p},\mathfrak{q}},
\end{aligned}$$

where $\omega(k, G) > 0$ is given in Remark 1.3, $\alpha = \alpha(k, G) > 0$, $c_{k,G} > 0$,

$$R_{\mathfrak{p}} = O_{\mathfrak{p}}(B(\log B)^{\omega(k,G)-1-\alpha}), \quad R_{\mathfrak{p},\mathfrak{q}} = O_{\mathfrak{p},\mathfrak{q}}(B(\log B)^{\omega(k,G)-1-\alpha}),$$

and $\delta_{\mathfrak{p}}$ is given as follows. For $\mathfrak{p} \in S_0$ we have $\delta_{\mathfrak{p}} = 1$, and for $\mathfrak{p} \notin S_0$ corresponding to the place v, we have

$$\delta_{\mathfrak{p}} = \frac{\sum_{\chi_v \in \Lambda_v} \frac{1}{\Phi_v(\chi_v)}}{\sum_{\chi_v \in \mathrm{Hom}(k_v^\times, G)} \frac{1}{\Phi_v(\chi_v)}}.$$

Here we have used the fact that Euler factors for places $v \in S \setminus S_0$ can be split off the formula for the constant $c_{k,G,\Lambda}$ given in [7, Theorem 3.22], as explained in the proof of [7, Lemma 4.5]. We evaluate $\delta_{\mathfrak{p}}$ further as follows. By [7, Lemma 3.10], we have, for $v \notin S_0$,

$$\frac{1}{|G|} \sum_{\chi_v \in \mathrm{Hom}(k_v^\times, G)} \frac{1}{\Phi_v(\chi_v)} = 1 + (|\,\mathrm{Hom}(\mathbb{F}_v^\times, G)| - 1)q_v^{-1} = 1 + (|G[q_v - 1]| - 1)q_v^{-1}.$$

As the unramified homomorphisms χ_v contribute exactly the '1' in the above formula, we also get that

$$\frac{1}{|G|} \sum_{\chi_v \in \Lambda_v} \frac{1}{\Phi_v(\chi_v)} = (|\,\mathrm{Hom}(\mathbb{F}_v^\times, G)| - 1)q_v^{-1} = (|G[q_v - 1]| - 1)q_v^{-1},$$

and hence

$$\delta_{\mathfrak{p}} = \frac{(|G[q_v - 1]| - 1)q_v^{-1}}{1 + (|G[q_v - 1]| - 1)q_v^{-1}} \geqslant \frac{G[q_v - 1] - 1}{2q_v} \geqslant \frac{1}{2q_v}$$

for sufficiently large v with $\gcd(q_v - 1, e) > 1$. As the set of v satisfying the latter condition has positive density by Chebotarev, we have shown that the series

$$\sum_{\mathfrak{p}} \delta_{\mathfrak{p}}$$

diverges. For any field $K \in \mathscr{A}$, we clearly have

$$\omega_z(K/k) := |\{\mathfrak{p} \in P(z) \ : \ K \in \mathscr{A}_{\mathfrak{p}}\}| \leqslant \omega(K/k),$$

hence we are interested in bounding

$$E(B; z, r) = \{K \in \mathscr{A} \ : \ \omega_z(K/k) \leqslant r\}$$

for sufficiently large B. To do so, we consider the mean

$$\begin{aligned} M(z) &:= \frac{1}{N} \sum_{K \in \mathscr{A}} \omega_z(K/k) = \frac{1}{N} \sum_{\mathfrak{p} \in P(z)} |\mathscr{A}_{\mathfrak{p}}| \\ &= \sum_{\mathfrak{p} \in P(z)} \delta_{\mathfrak{p}} + O_z((\log B)^{-\alpha}) = U(z) + O_z((\log B)^{-\alpha}), \end{aligned}$$

where we have written $U(z) = \sum_{\mathfrak{p}\in P(z)} \delta_{\mathfrak{p}}$. As the sum over $\delta_{\mathfrak{p}}$ diverges, we may choose z large enough so that $U(z) > 4r$. Then we have $M(z) > U(z)/2 > 2r$ for all sufficiently large B. By [8, Lemma 5.1], we get

$$\frac{E(B;z,r)}{N} \leqslant \frac{4}{M(z)^2}\left(U(z) + \frac{1}{N}\sum_{\mathfrak{p},\mathfrak{q}\in P(z)} |R_{\mathfrak{p},\mathfrak{q}}| + \frac{2U(z)}{N}\sum_{\mathfrak{p}\in P(z)} |R_{\mathfrak{p}}| + \left(\frac{1}{N}\sum_{\mathfrak{p}\in P(z)} |R_{\mathfrak{p}}|\right)^2\right),$$

where $R_{\mathfrak{p},\mathfrak{p}}$ is interpreted as $R_{\mathfrak{p}}$. The expression on the left-hand side of (4.1) is bounded above by

$$\lim_{B\to\infty} \frac{E(B;z,r)}{N} \leqslant \frac{16}{U(z)^2}(U(z) + 0 + 0 + 0) = \frac{16}{U(z)} < \varepsilon,$$

provided z is chosen large enough. □

5 | NARROW GENUS NUMBERS AND GENERALISATIONS

We finish by discussing the narrow genus number $\mathfrak{g}^+_{K/k}$. For abelian K/k, this is defined analogously to Definition 1.1, but instead taking the largest extension of K that is abelian over k and unramified only at all non-archimedean places of K. Warning: some authors take this as the definition of the genus number; this is due to Fröhlich's original convention [9] and is, for example, the definition used in [14]. As $\mathfrak{g}^+_{K/k} \geqslant \mathfrak{g}_{K/k}$, it is clear that an analogue of Theorem 1.5 holds for narrow genus numbers as well.

Analogously to Lemma 3.1, we have the formula (see [12, Theorem 4])

$$\mathfrak{g}^+_{K/k} = \frac{h^+(k)\prod_{v\in\Omega_k^{\mathrm{f}}} \mathfrak{e}_v(K)}{[K:k][\mathcal{O}_k^{\times,+} : \mathcal{O}_k^{\times,+} \cap \mathrm{N}_{K/k}\prod_{w\in\Omega_K} \mathcal{O}_{K,w}^{\times}]}, \tag{5.1}$$

where $h^+(k)$ denotes the narrow class number of k, $\mathcal{O}_k^{\times,+}$ denotes the group of totally positive units of k, and Ω_k^{f} denotes the set of finite places of k.

The narrow genus number and the genus number only differ by a power of 2. More precisely, $\mathfrak{g}^+_{K/k}/\mathfrak{g}_{K/k}$ divides 2^{r_1} where r_1 is the number of real places of k. This can be seen by taking the quotient of (5.1) by the expression in Lemma 3.1 and recalling that $h^+(k)/h(k) = 2^{r_1}/[\mathcal{O}_k^{\times} : \mathcal{O}_k^{\times,+}]$ (see [1, Exercise 3], for example). Moreover, for odd degree extensions of $\mathbb{Q}$ the genus number and the narrow genus number coincide, see [10, 2.9 Proposition].

Using (5.1) in place of Lemma 3.1 during the proof of Theorem 3.5, one can obtain an asymptotic formula for the sum of $\mathfrak{g}^+_{K/k}$ with the same order of magnitude, but a different leading constant.

More generally, Horie [13] has defined the genus field with respect to an arbitrary modulus of K and given a formula for the corresponding generalisation of the genus number, see [13, Corollary of Theorem 2]. For moduli induced from a fixed modulus of k, our methods can also be used to give an asymptotic formula for the sum of these generalised genus numbers, again having the same order of magnitude as in Theorem 3.5 but with a different leading constant.

ACKNOWLEDGEMENTS

We thank Alex Bartel for useful discussions on genus groups and Hendrik Lenstra for asking the question that led to Theorem 1.5. We thank the anonymous referee for their careful reading of our paper. Christopher Frei was supported by EPSRC Grant EP/T01170X/1 and EP/T01170X/2. Daniel Loughran was supported by UKRI Future Leaders Fellowship MR/V021362/1. Rachel Newton was supported by EPSRC Grant EP/S004696/1 and EP/S004696/2, and UKRI Future Leaders Fellowship MR/T041609/1 and MR/T041609/2.

JOURNAL INFORMATION

The *Journal of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, 2nd ed., London Mathematical Society, London, 2010.
2. H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Mathematics, vol. 1068, Springer, Berlin, 1984, pp. 33–62.
3. B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), 116–138.
4. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. Lond. Ser. A **322** (1971), no. 1551, 405–420.
5. J. Ellenberg, L. B. Pierce, and M. M. Wood, *On ℓ-torsion in class groups of number fields*, Algebra Number Theory **11** (2017), no. 8, 1739–1778.
6. C. Frei, D. Loughran, and R. Newton, *The Hasse norm principle for abelian extensions*, Amer. J. Math. **140** (2018), no. 6, 1639–1685.
7. C. Frei, D. Loughran, and R. Newton, *Number fields with prescribed norms*, Comment. Math. Helv. **97** (2022), 133–181. (With an appendix by Y. Harpaz and O. Wittenberg.)
8. C. Frei and M. Widmer, *Average bounds for the ℓ-torsion in class groups of cyclic extensions*, Res. Number Theory **4** (2018), 34. https://doi.org/10.1007/s40993-018-0127-9
9. A. Fröhlich, *The genus field and genus group in finite number fields. I, II*, Mathematika **6** (1959), 40–46, 142–146.
10. A. Fröhlich, *Central extensions*, Galois groups, and ideal class groups of number fields, Contemporary Mathematics, vol. 24 (1983), American Mathematical Society, Providence, RI.
11. Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. **29** (1967), 281–285.
12. S. J. Gurak, *Ideal-theoretic characterization of the relative genus field*, J. Reine Angew. Math. **296** (1977), 119–124.
13. M. Horie, *On the genus field in algebraic number fields*, Tokyo J. Math. **6** (1983), no. 2, 363–380.
14. H. H. Kim, *Genus numbers of cyclic and dihedral extensions of prime degree*, Acta Arith. **192** (2020), no. 3, 289–300.
15. K. J. McGown, F. Thorne, and A. Tucker, *Counting quintic fields with genus number one*, Math. Res. Lett., to appear.
16. K. J. McGown and A. Tucker, *Statistics of genus numbers of cubic fields*, Ann. Inst. Fourier, Online first, 19 p.
17. J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, Berlin, 2008.
18. J.-P. Serre, *Lectures on $N_X(p)$*. Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012.
19. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, 3rd ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015.
20. M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), no. 1, 102–128.