

AN EXPONENT OF 1.04273 FOR THE UNIT DISTANCE PROBLEM

ERIC NASLUND*

ABSTRACT. Let $u(U)$ count the unordered pairs at distance one in a finite planar set U . We construct finite sets U_j with $|U_j| \rightarrow \infty$ and $u(U_j)/|U_j|^{1.04273} \rightarrow \infty$. The largest exponent previously claimed, 1.0358, is in the author's unpublished manuscript. The method is the number-field construction of OpenAI and Sawin: unit distances come from elements of relative norm one in quadratic extensions, and the fields come from an infinite pro-2 class field tower. The new ingredients are quadratic extensions of mixed signature, with an exact average over their norm-one units, and a tower over the real quadratic field $\mathbb{Q}(\sqrt{241})$, in which 2, 3 and 5 split. Its Golod–Shafarevich function contains two copies of the local conditions at these primes but only one constant term, and the extra room lets the tower be ramified only above 2, 3 and 5; the root discriminant of its fields is about 286. The relative zeta value is bounded through the zeta function of the degree-512 field generated over $\mathbb{Q}(\sqrt{241})$ by the square roots of its $\{2, 3, 5\}$ -units, which is the product of the Dedekind zeta function of $\mathbb{Q}(\sqrt{241})$ and 255 quadratic Hecke L -functions. Finite facts and numerical inequalities are certified by exact computation and interval arithmetic. A significant portion of this work was verified in Lean, reducing the result with exponent 1.0427 to an explicit zeta function inequality (Palomar registry, PALOMAR-2026-10-01-000018, version 1).

***AI Methodology.** This work was done with extensive AI use, with agents developing the mathematics and writing the paper. I supervised and prompted the AI agents that produced this work. While this has been edited to improve readability, I recommend the reader also make use of their AI model of choice to ask the paper questions. The construction over $\mathbb{Q}(\sqrt{241})$, the computations that certify it, the Lean formalization of the reduction of the proof of exponent 1.0427 to one explicit zeta inequality (Remark 4.40), and this paper were produced with a combination of Claude Opus 5.5, ChatGPT Sol 5.6, ChatGPT Astra 6, working as agents in Claude Code and Codex. The construction adapts the author's previous manuscript [23], which was also written with AI tools.

1. INTRODUCTION

For a finite set $U \subset \mathbb{R}^2$, let

$$u(U) = \#\{\{x, y\} \subset U : |x - y| = 1\}, \quad u(n) = \max_{|U|=n} u(U),$$

where the pairs are unordered and the distance is Euclidean. The unit distance problem of Erdős [6] asks for the order of growth of $u(n)$. Our main result is the following.

Theorem 1.1. *There are finite sets $U_j \subset \mathbb{R}^2$, with $|U_j| \rightarrow \infty$, such that*

$$\frac{u(U_j)}{|U_j|^{1.04273}} \longrightarrow \infty.$$

In particular, $u(n) \geq n^{1.04273}$ for arbitrarily large integers n .

The largest exponent previously claimed, 1.0358324, is in the author's unpublished manuscript [23]. Theorem 1.1 uses the same number-field method with several new ingredients: fields of mixed signature, averaged over their norm-one units; an infinite pro-2 extension of the real quadratic field $\mathbb{Q}(\sqrt{241})$, with restricted ramification and a nonabelian local Galois group at the primes above 2; an explicit bound for the relative zeta value (defined in Subsection 1.2) from the quadratic L -functions

Date: September 30, 2026.

of a Kummer field of degree 512; and optimized *profiles*: smooth or locally constant weight functions at the archimedean places and at finitely many primes, whose product determines, through its superlevel sets, the region in which lattice points are counted. Subsection 1.3 describes them. The theorem concerns an unbounded sequence of cardinalities. Its proof uses no unproved hypothesis, such as the generalized Riemann hypothesis, but it is computer-assisted: finite facts about the tower and several numerical inequalities are verified by exact computation and interval arithmetic, as described in Subsection 1.6.

1.1. **Background.** Erdős [6] showed that a suitable section of a scaled integer lattice gives

$$u(n) \geq n^{1+c_0/\log \log n}$$

for some $c_0 > 0$ and arbitrarily large n , and he conjectured that this is essentially optimal [6, 7]. The best upper bound,

$$u(n) = O(n^{4/3}),$$

is due to Spencer, Szemerédi and Trotter [34]; Székely [36] gave a proof by crossing numbers.

In 2026 a team at OpenAI [27] disproved Erdős’s conjecture. They constructed sets with $u(U) \geq |U|^{1+\delta}$ for a fixed $\delta > 0$ and arbitrarily large $|U|$, replacing the integer lattice by ideal lattices in number fields of large degree and small root discriminant. Alon, Bloom, Gowers, Litt, Sawin, Shankar, Tsimerman, Wang and Wood [1] simplified the argument and obtained $\delta \approx 6 \cdot 10^{-38}$. Sawin [32] made every step explicit and sharpened it, and reached the exponent 1.014114.

Improvements followed within days in online discussions. On the Erdős Problems forum, mlewko [20] reached 1.031849 in Sawin’s criterion with finite data found by ChatGPT, and on MathOverflow spiderduckpig [35] adjusted these data to reach 1.031883. In a comment the next day, spiderduckpig proposed a structural change: in the Golod–Shafarevich step of Sawin’s argument [32, Lemma 11], replace the unweighted count of relations by a count weighted by degree in the Zassenhaus filtration (recalled in Section 2). This was reported to give $\delta \geq 0.0333487$ [35]. Weighted counts of this kind underlie the towers of [23] and of the present paper. The author’s MathOverflow answer [21] then combined this count with covolume counting, dyadic ramification and Euler products over a fixed subfield. The manuscript [23] is a formal write-up of that construction, and it records $\delta = 0.0358324$. Table 1 lists the explicit exponents, and the repository [28] records further bounds posted online.

TABLE 1. Explicit lower bounds $u(n) \geq n^{1+\delta}$ for arbitrarily large n , in increasing order. The exponents are rounded down and constant factors are omitted. The last column gives the kind of source; apart from Erdős’s, none of these bounds had appeared in a refereed journal when this paper was written.

Exponent	Source	Main new input	Kind of source
$1 + c_0/\log \log n$	Erdős [6]	integer lattice	journal
$1 + \delta, \delta > 0$	OpenAI [27]	ideal lattices from class field towers	manuscript
$1 + 6 \cdot 10^{-38}$	Alon et al. [1]	simplified argument	preprint
1.014114	Sawin [32]	explicit and sharpened criterion	preprint
1.015263	Emmerich [4]	optimized parameters	preprint
1.031185	Emmerich, Cordella [5]	extended range of primes	online certificate
1.031849	mlewko [20]	finite data found by ChatGPT	forum post
1.0333487	spiderduckpig [35]	weighted Zassenhaus count	online post
1.0358324	Naslund [23, 21]	covolume counting, dyadic ramification, fixed-subfield Euler products	manuscript, online post
1.04273	this paper	see Subsection 1.3	

1.2. The construction in outline. The construction carries Erdős's lattice argument to number fields of large degree. Let K be such a field, of degree $2d$, with an involution ι whose fixed field is F . We take the points of a translated ideal lattice of K that lie in a bounded region of $K \otimes \mathbb{R}$. A complex embedding in which ι acts as complex conjugation maps them injectively to the plane. It sends every difference of relative norm one over F to a unit vector, so two points whose difference has relative norm one are at distance one. The exponent is then set by a balance between four quantities, each normalized as d^{-1} times the logarithm of a count. First, equal-norm choices: if a prime $\mathfrak{p}$ of F splits in K as $\mathfrak{P} \cdot \iota\mathfrak{P}$, the $k+1$ ideals $\mathfrak{P}^j(\iota\mathfrak{P})^{k-j}$, $0 \leq j \leq k$, all have relative norm $\mathfrak{p}^k$. When the construction uses these $k+1$ ideals, we say that $\mathfrak{p}$ is used with exponent k , and we call the primes so used the *selected primes*. Second, ideal classes: a choice of exponents $0 \leq j_{\mathfrak{p}} \leq k_{\mathfrak{p}}$, one at each selected prime $\mathfrak{p}$ (used with exponent $k_{\mathfrak{p}}$), gives the product of the ideals $\mathfrak{P}^{j_{\mathfrak{p}}}(\iota\mathfrak{P})^{k_{\mathfrak{p}}-j_{\mathfrak{p}}}$. For the choices whose ideals $\prod_{\mathfrak{p}} \mathfrak{P}^{j_{\mathfrak{p}}}$ lie in one class of $\text{Cl}(K)$ modulo the image of $\text{Cl}(F)$, there are elements of relative norm one that generate these products times one fixed fractional ideal, and keeping the most frequent class loses at most a factor equal to the order of that quotient (Lemma 5.6). Through the class-number formula, this loss is governed by the root discriminant λ of K and by the *relative zeta value* $L_F(1)$, where $L_F(s) = \zeta_K(s)/\zeta_F(s)$. Third, the region: its shape decides how many pairs of points with difference of relative norm one lie in it, and its volume fixes the number of points. Fourth, density: using a prime $\mathfrak{p}$ with exponent k also makes the ideal lattice denser by the factor $N\mathfrak{p}^k$; since the exponent $1 + \delta$ is measured against the number of points, this costs $\delta k \log N\mathfrak{p}$ before division by d .

Quantitatively, suppose that such fields exist with $d \rightarrow \infty$ and a fixed root discriminant λ . Let (b, c) be the signature of F , so that $d = b + 2c$, and put $\theta = c/d$; thus 2θ is the proportion of non-real embeddings of F . Suppose also that the selected primes have *uniform local types*: they are all the primes of F above the primes r of a fixed finite set $\mathcal{R}$, each of them splits in K , and all those above a given r have the same absolute ramification index e_r and residue degree f_r (Definitions 2.41 and 5.4). Then F has exactly $d/(e_r f_r)$ primes above each r , and we use all of them with a common exponent k_r . If the points are taken from one translate of a fixed ideal lattice, with no further weighting at the selected primes (*unweighted shell profiles*, Definition 6.5), the exponent $1 + \delta$ is attained when

$$(1.2) \quad \sum_{r \in \mathcal{R}} \frac{\log(k_r + 1) - \delta k_r f_r \log r}{e_r f_r} - \left(\frac{1}{2} - \delta\right) \log \lambda - C + \mathcal{A}_{\delta}(\theta) > 0.$$

Here C is an upper bound for $d^{-1} \log L_F(1)$, and

$$\mathcal{A}_{\delta}(\theta) = (1 - \delta) \log 2 + (1 - \theta) \log \pi + (1 - 2\theta) J_{\mathbb{R}} + \theta J_{\mathbb{C}}$$

is the archimedean contribution. In it, $J_{\mathbb{R}}$ and $J_{\mathbb{C}}$ are the functionals of the profiles at the real and at the complex places of F (Definition 5.22); they compare how much a profile overlaps its translates by elements of relative norm one with its mass. We call the left side of (1.2) the *margin*. Proposition 5.26, the geometric transfer, makes this precise for quadratic extensions K/F with K totally imaginary, F with a real place and K/F unramified at every finite place: under conditions on the profiles, if the margin is bounded below by a positive constant along such a family, then there are finite sets $U_j \subset \mathbb{R}^2$ with $|U_j| \rightarrow \infty$ and $u(U_j)/|U_j|^{1+\delta} \rightarrow \infty$. Section 6 allows general *shell profiles*, weighted sums of indicator functions of sets defined by valuations (Definition 6.5 and Proposition 6.21). This replaces each summand of the sum over $\mathcal{R}$ in (1.2) by $\log \mathcal{F}_{\delta,r}/(e_r f_r)$, where $\mathcal{F}_{\delta,r}$ is the value of the local functional of Definition 6.1 at the shell profile used above r ; we still call the resulting left side the margin (Corollary 6.23). Section 8 proves a positive lower bound for it at $\delta = 0.04273$.

The fields must form an infinite family of growing degree with fixed λ and fixed types at the selected primes. Such families come from *towers*, pro-2 extensions with restricted ramification and prescribed local Galois groups, when these are infinite. Golod–Shafarevich arguments [10] show

that a tower is infinite when an explicit function of $t \in (0, 1)$, built from the number of generators of its Galois group and from its local conditions, takes a negative value; here that function is the *Golod–Shafarevich function* P_B of (2.37), and Proposition 2.39 proves the criterion for it. The use of Frobenius conditions to control splitting in such towers goes back to Hajir, Maire and Ramakrishna [11].

1.3. New ingredients. The construction differs from those of Sawin [32] and of [23] in four ways.

Mixed signature. In Sawin’s construction, and in [23], the field K is a CM field: complex conjugation is central in $\text{Gal}(K/\mathbb{Q})$, F is totally real, every norm-one element has modulus one at every archimedean place, and the norm-one units are finite. Here K is totally imaginary and Galois over $B = \mathbb{Q}(\sqrt{241})$, and F is the fixed field of one complex conjugation ι_1 , which is not central: its conjugacy class has at least 2^{15} elements, so $\theta \geq \theta_* = 65535/131072$ (Theorem 2.42) and almost every place of F is complex. Above a complex place of F the two coordinates of a norm-one element can have moduli e^u and e^{-u} , and the norm-one units, of rank c , move u along a lattice. Averaging over a fundamental domain of that lattice counts the resulting pairs of points exactly, and the class-number formula cancels the regulator of these units together with the capitulation kernel, the kernel of $\text{Cl}(F) \rightarrow \text{Cl}(K)$ (Proposition 5.2). Mixed signature therefore costs only a factor π per complex place of F , and a profile that couples the two coordinates at that place more than repays it.

A tower over $\mathbb{Q}(\sqrt{241})$. Over a totally real base field in which every prime at which the tower is ramified splits completely, the Golod–Shafarevich function has a local term for every prime of the base above such a prime, but only one constant term (in (2.37), the terms $2\psi_D$ and $4\psi_{C_2 \times C_2}$, and the constant 1). The field $B = \mathbb{Q}(\sqrt{241})$ is the real quadratic field of smallest discriminant in which 2, 3 and 5 all split. Over B we prescribe a nonabelian dyadic local Galois group of order 32 at each of the two primes above 2, a tame local group $C_2 \times C_2$ at each of the four primes above 3 and 5, and conditions that make the Frobenius elements have order dividing 4 at the two primes above 29 and at the prime 7, which is inert in B . The relations are counted through their images in the Zassenhaus filtration, and one dyadic relation is implied by the others through Hilbert reciprocity. The resulting tower is infinite, it is ramified only above 2, 3 and 5, and its Galois group has 8 generators. The fields of Theorem 2.42 have root discriminant

$$\lambda = 2^{9/4} \sqrt{3615} \approx 286.0, \quad 3615 = 3 \cdot 5 \cdot 241.$$

Sawin’s fields come from a pro-2 tower of unramified extensions of $\mathbb{Q}(\sqrt{3 \cdot 5 \cdots 43})$, so they are ramified over $\mathbb{Q}$ at 2 and at the thirteen odd primes up to 43, and their root discriminant is about $1.6 \cdot 10^8$. Theorem 2.42 states the family of fields.

The zeta value. Every field K of Theorem 2.42 contains the Kummer field $E = B(\sqrt{V})$, of degree 512 over $\mathbb{Q}$, where V is the group of $\{2, 3, 5\}$ -units of B (the units of $\mathcal{O}_B[1/30]$) modulo squares. Its Dedekind zeta function is the product of ζ_B and 255 quadratic Hecke L -functions of B , which we evaluate rigorously with approximate functional equations (Sections 3 and 4). Together with refinements from the known types of primes in the fields of the tower (Definition 2.41), this gives the bound $C = 0.04871285$ for $d^{-1} \log L_F(1)$ (Theorem 4.2). It replaces Louboutin’s bound [16], which Sawin uses, and the Euler products over a fixed multiquadratic subfield of [23].

Profiles and shells. Sawin counts points in a region bounded in the sup norm by packing, and [23] counts them by covolume in a Euclidean ball. We use a Gaussian profile at the real places of F ; at the complex places, a Student–Bernstein profile, which couples the two coordinates (Definition 7.1); and shell profiles at the selected primes (Definition 6.5). We count points by Poisson summation (Sections 5–7). Table 2 compares Sawin’s example with the present construction.

1.4. Why the exponent improves. Write $\ell = \log \lambda$,

$$J = \sum_{r \in \mathcal{R}} \frac{\log(k_r + 1)}{e_r f_r}, \quad H = \sum_{r \in \mathcal{R}} \frac{k_r \log r}{e_r},$$

TABLE 2. Sawin’s example and the present construction. The pairs (e, f) are absolute ramification indices and residue degrees of the selected primes of F ; Sawin’s residue degrees are at most 2.

	Sawin [32]	this paper
base field of the tower	$\mathbb{Q}(\sqrt{3 \cdot 5 \cdots 43})$	$\mathbb{Q}(\sqrt{241})$
primes ramified in the tower	2 and 3, 5, $\dots$, 43	those above 2, 3, 5
fields K	CM, $\theta = 0$	mixed signature, $\theta \geq \theta_*$
selected primes, (e, f)	22 primes up to 179	2: (8, 4); 3, 5: (2, 2); 7: (1, 8); 29: (1, 4)
root discriminant λ	about $1.6 \cdot 10^8$	$2^{9/4} \sqrt{3615} \approx 286.0$
$\ell = \log \lambda$	18.90	5.656
zeta term	$1 + \log \log \lambda \approx 3.94$	$C = 0.04871285$
exponent $1 + \delta$	1.014114	1.04273

so that the sum in (1.2) is $J - \delta H$. Sawin’s criterion [32, Proposition 10] applies to Galois CM fields K of unbounded degree, with maximal totally real subfield F , whose relative root discriminant $(|\Delta_K|/|\Delta_F|)^{1/d}$ is λ , and counts points in a region bounded in the sup norm, with a parameter $R > 1$. In his example, as for our fields, K/F is unramified at every finite place, so that $|\Delta_K| = |\Delta_F|^2$ and $\lambda = \text{rd}(K)$ (Definition 2.40). Rearranged, his criterion gives arbitrarily large sets with $u(U) \gg |U|^{1+\delta}$ whenever (1.3) holds; inequality (1.4) is (1.2) with $\mathcal{A}_\delta(\theta)$ written out and regrouped:

$$(1.3) \quad (J - \delta H) + (\log 2\pi - \tfrac{1}{2}\ell - 1 - \log \ell) + (2 \log(1 - R^{-1}) - 2\delta \log(2R + e^{-H/2})) \geq 0,$$

$$(1.4) \quad (J - \delta H) + (\log 2 + (1 - \theta) \log \pi - \tfrac{1}{2}\ell - C) + (\delta \ell - \delta \log 2 + (1 - 2\theta)J_{\mathbb{R}} + \theta J_{\mathbb{C}}) > 0.$$

In both, the three groups are the gain from equal-norm choices, the loss in selecting a common ideal class, and the count of points together with the shape of the region.

The fields. The dominant change is in ℓ . Sawin’s example has $\ell > 18.9$; here $\ell < 5.657$, so the term $-\frac{1}{2}\ell$ improves by more than 6.6 per unit of d . The price is paid in the first group: Sawin selects 22 primes with residue degree at most 2, and we select only the primes above 2, 3, 5, 7 and 29, several with residue degree 4 or 8.

Ideal-class selection. Both criteria use the analytic class-number formula, which is exact in either signature; they differ in how they bound the zeta value. At $\theta = 0$ the constants agree, and the groups differ only in C against $1 + \log \ell$. In Sawin’s criterion, $1 + \log \ell$ is the sum of $1 - \log 2 + \log \ell$, which is Louboutin’s bound [16, Corollary 3] for $d^{-1} \log L_F(1)$ read through the class-number formula, and $\log 2$, for the factor 2^d allowed for units in [32, Lemma 6]. The manuscript [23] removed the unit factor and sharpened Louboutin’s bound with Euler products over a fixed subfield. Here Proposition 5.2 accounts for the unit index $[\mathcal{O}_F^\times : N_{K/F} \mathcal{O}_K^\times]$ exactly, and the Kummer field gives $C = 0.04871285$, whereas $1 + \log \ell$ would exceed 2.73 even at our value of λ . Mixed signature costs $\theta \log \pi$ in this group, since each place of F carries one factor π in the class-number formula.

Points and region. Besides the term $-\delta H$, which both criteria share, Sawin’s packing count of points contributes $-2\delta \log(2R + e^{-H/2})$ to (1.3), which does not involve λ . Counting by covolume, as in [23] and here, contributes $\delta \ell - \delta \log 2$ to (1.4), because a larger discriminant makes the ideal lattice sparser. The term $2 \log(1 - R^{-1})$, which measures how much Sawin’s region overlaps its translates by elements of relative norm one, and the volume of that region become the functionals $J_{\mathbb{R}}$ and $J_{\mathbb{C}}$ of the profiles.

Signature. CM fields have $\theta = 0$. With the other data fixed, mixed signature adds $\theta(J_{\mathbb{C}} - 2J_{\mathbb{R}} - \log \pi)$ to the left side of (1.4). Section 8 proves $J_{\mathbb{C}} - 2J_{\mathbb{R}} - \log \pi > 0.6324$ (Proposition 8.5(h) and

Lemma 8.10), so with $\theta \geq \theta_*$ this term exceeds 0.316; at $\theta = 0$ the lower bound for the margin proved there would be negative (Remark 8.11).

Table 8 lists, rounded, the terms of the lower bound for the margin that Section 8 proves at $\delta = 0.04273$ and $\theta = \theta_*$; they sum to about $1.77 \cdot 10^{-4}$ (Proposition 8.5). With the same complex-place profile, the real-place profile adjusted to δ as in Definition 8.1, and shell weights re-optimized in the same way, the corresponding lower bound at $\delta = 0.0428$ is negative (Remark 8.12).

1.5. Organization. Section 2 constructs the tower over B and proves Theorem 2.42, which supplies the fields. Section 3 describes the Kummer field and its quadratic L -functions, and Section 4 proves the upper bound $d^{-1} \log L_F(1) < C$ for the relative zeta value (Theorem 4.2). Sections 5–7 carry out the geometric construction: the class-number formula for the units of relative norm one and the geometric transfer to planar sets, the shell profiles at the selected primes, and the archimedean profiles. These sections apply to any quadratic extension K/F satisfying the conditions (G1)–(G3) of Section 5. Section 8 proves the final inequality at $\delta = 0.04273$ and completes the proof of Theorem 1.1.

1.6. Computations and data. The proof uses finite computations: linear algebra over $\mathbb{F}_2$ for the tower, exact rational arithmetic for the Golod–Shafarevich function, rigorous evaluations of L -functions in the ball arithmetic of Arb, now part of FLINT [15, 38], and interval arithmetic with directed rounding for the margin [40]. PARI/GP [41] is used for the arithmetic of number fields and for independent checks. Each finite fact is verified by a supplementary program, named in the text where the fact is used. These computations concern exact arithmetic and rigorous inequalities, not the statistical accuracy of floating-point approximations.

The programs and their data are in the directory `papers/0.04273/certificates` of the public repository [24]. Some routines, for the degree-two approximate functional equations, the archimedean profiles and the shell profiles, are imported unchanged from the supplementary archive of an earlier, unpublished note of the author, superseded by the present paper, in the directory `papers/0.0418235/certificates` of the same repository, together with a manifest of the SHA-256 hashes of its members. A replay program runs every step and records its results. The computations were run with PARI/GP 2.17.2, python-flint 0.9.0 (FLINT 3.6.0) and mpmath 1.3.0.

A separate Lean 4 development [22], built on Mathlib [2, 39], proves the planar conclusion with the slightly smaller exponent 1.0427 from one explicit numerical inequality for the Dedekind zeta function of E (Remark 4.40). That inequality has not been proved in Lean, so the formalization is conditional, and it is not used as a substitute for the arguments here. The formalization is registered in the Palomar registry of machine-checked Lean proofs as PALOMAR-2026-10-01-000018, version 1 [22].

CONTENTS

1. Introduction	1
2. The Tower over $\mathbb{Q}(\sqrt{241})$	7
3. The Kummer Field and Its Quadratic L -Functions	23
4. The Relative Zeta Value and an Explicit Upper Bound	27
5. Units of Relative Norm One and Planar Point Sets	38
6. Shell Profiles at Split Finite Places	46
7. Archimedean Profiles	53
8. Proof of Theorem 1.1	59
References	64

2. THE TOWER OVER $\mathbb{Q}(\sqrt{241})$

This section constructs the number fields of Theorem 2.42 as finite subextensions of an infinite pro-2 extension of $B = \mathbb{Q}(\sqrt{241})$ with prescribed local Galois groups. Subsection 2.1 describes B and its $\{2, 3, 5\}$ -units. Subsection 2.2 recalls the local Galois groups involved and constructs the dyadic local field. Subsection 2.3 shows that the Galois group G_S of the maximal pro-2 extension of B unramified outside 2, 3, 5 has a presentation with eight generators and seven local relators (Lemma 2.17). Subsection 2.4 imposes the local conditions and defines the quotient G_B of G_S (Definition 2.20). Subsection 2.5 computes the first three graded pieces of the Zassenhaus filtration $(D_n G_B)_n$ of G_B , recalled below: the prescribed local groups inject into $G_B/D_3 G_B$, and the complex conjugation ι_1 (Definition 2.12) has 2^{15} conjugates in $G_B/D_4 G_B$ (Lemma 2.26). Subsections 2.6 and 2.7 prove that G_B is infinite, by a filtered Fox calculus and the Golod–Shafarevich method [10]: the Golod–Shafarevich function P_B of (2.37) takes a negative value (Lemma 2.38). Subsection 2.8 proves Theorem 2.42.

We use the following conventions. Subgroups of profinite groups are closed, generation is topological, and the normal closure of a set is the smallest closed normal subgroup containing it. The commutator is $[g, h] = g^{-1}h^{-1}gh$. The *generator rank* and the *relation rank* of a pro-2 group G are $\dim H^1(G, \mathbb{F}_2)$ and $\dim H^2(G, \mathbb{F}_2)$. For an extension M/A of local or global fields, $\mathfrak{D}_{M/A}$ denotes its different and $\mathfrak{d}_{M/A}$ its relative discriminant. For a finite 2-group Δ with augmentation ideal $\mathfrak{I} \subset \mathbb{F}_2[\Delta]$, the Zassenhaus filtration is $D_n \Delta = \{g : g - 1 \in \mathfrak{I}^n\}$; for a pro-2 group it is defined through finite quotients. Then $[D_m, D_n] \subset D_{m+n}$, $g^2 \in D_{2n}$ for $g \in D_n$, a surjection maps D_n onto D_n , and $\text{gr } \Delta = \bigoplus_{n \geq 1} \text{gr}_n \Delta$, with graded pieces $\text{gr}_n \Delta = D_n \Delta / D_{n+1} \Delta$, is a restricted Lie algebra over $\mathbb{F}_2$ whose bracket is induced by commutators and whose restricted square $v \mapsto v^{[2]}$ is induced by squaring [13, 31, 8]. By Lazard’s formula [8, Proposition 3.2], $D_n = \prod_{i, 2^j \geq n} \gamma_i^{2^j}$, where γ_i is the lower central series. In particular D_1 is the whole group, D_2 is the Frattini subgroup, and $D_3 = D_2^2[D_2, D_1]$. For a free pro-2 group $\mathcal{F}$ of rank n , $\text{gr } \mathcal{F}$ is the free restricted Lie algebra on $\mathcal{F}/D_2 \mathcal{F} \cong \mathbb{F}_2^n$ [31, 8]. We realize it inside the free associative algebra $\mathbb{F}_2\langle X_1, \dots, X_n \rangle$, with bracket $[a, b] = ab + ba$ and restricted square $a^{[2]} = a^2$; its graded pieces of degrees one, two and three have dimensions n , $n(n+1)/2$ and $(n^3 - n)/3$.

Definition 2.1. A *filtered space* is a finite-dimensional $\mathbb{F}_2$ -vector space M with subspaces $M = F^0 M \supseteq F^1 M \supseteq \dots$ such that $F^n M = 0$ for large n . Its *Hilbert polynomial* is $h_M(t) = \sum_{n \geq 0} \dim(F^n M / F^{n+1} M) t^n$. For a finite 2-group Δ we filter $\mathbb{F}_2[\Delta]$ by the powers $\mathfrak{I}^n$ of its augmentation ideal, so that $h_{\mathbb{F}_2[\Delta]}(t) = \sum_{n \geq 0} \dim(\mathfrak{I}^n / \mathfrak{I}^{n+1}) t^n$.

Theorem 2.2 (Jennings [13]; see also [31]). *Let Δ be a finite 2-group, and let $g_1, \dots, g_m \in \Delta$ be elements whose classes form a basis of $\text{gr } \Delta$ consisting of homogeneous elements, the class of g_i lying in $\text{gr}_{n_i} \Delta$. Then the products $(g_1 - 1)^{a_1} \dots (g_m - 1)^{a_m}$ with $a_i \in \{0, 1\}$, taken in this order, form a basis of $\mathbb{F}_2[\Delta]$, and those with $\sum_i a_i n_i \geq n$ form a basis of $\mathfrak{I}^n$. Consequently*

$$h_{\mathbb{F}_2[\Delta]}(t) = \prod_{n \geq 1} (1 + t^n)^{\dim \text{gr}_n \Delta}.$$

The form with the factors in an arbitrary fixed order follows from Quillen’s description of $\text{gr } \mathbb{F}_2[\Delta]$ as the restricted enveloping algebra of $\text{gr } \Delta$ [31] and the restricted Poincaré–Birkhoff–Witt theorem.

2.1. The Base Field. Let $B = \mathbb{Q}(\sqrt{241})$, with real places v_1 ($\sqrt{241} \mapsto +\sqrt{241}$) and v_2 ($\sqrt{241} \mapsto -\sqrt{241}$). Put

$$(2.3) \quad \begin{aligned} \alpha_0 &= -1, & \alpha_1 &= \varepsilon = -71011068 + 4574225\sqrt{241}, \\ \alpha_2 &= \frac{-6101-393\sqrt{241}}{2}, & \alpha_3 &= \frac{6101-393\sqrt{241}}{2}, \\ \alpha_4 &= 31 - 2\sqrt{241}, & \alpha_5 &= 31 + 2\sqrt{241}, & \alpha_6 &= 326 - 21\sqrt{241}, & \alpha_7 &= 326 + 21\sqrt{241}. \end{aligned}$$

Their norms $N_{B/\mathbb{Q}}(\alpha_i)$ are $1, -1, -2, -2, -3, -3, -5, -5$, and $\alpha_2\alpha_3 = 2$, $\alpha_4\alpha_5 = -3$, $\alpha_6\alpha_7 = -5$. For a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_B$ we write $N\mathfrak{a} = |\mathcal{O}_B/\mathfrak{a}|$ for its absolute norm.

Lemma 2.4. (a) $\mathcal{O}_B = \mathbb{Z}[(1 + \sqrt{241})/2]$, the discriminant of B is 241, and B has class number one.

(b) The unit ε has norm $N_{B/\mathbb{Q}}(\varepsilon) = -1$, and the classes of -1 and ε form a basis of $\mathcal{O}_B^\times/\mathcal{O}_B^{\times 2}$.

(c) In $\mathcal{O}_B$ we have $2 = \mathfrak{p}_1\mathfrak{p}_2$, $3 = \mathfrak{q}_1\mathfrak{q}_2$, $5 = \mathfrak{r}_1\mathfrak{r}_2$ and $29 = \mathfrak{t}_1\mathfrak{t}_2$, where

$$\mathfrak{p}_j = \alpha_{1+j}\mathcal{O}_B, \quad \mathfrak{q}_j = \alpha_{3+j}\mathcal{O}_B, \quad \mathfrak{r}_j = \alpha_{5+j}\mathcal{O}_B, \quad \mathfrak{t}_j = (-14127 \pm 910\sqrt{241})\mathcal{O}_B,$$

with the sign $+$ for $j = 1$. These eight primes are distinct and of degree one. The prime 7 is inert, and we write $\mathfrak{t}_0 = 7\mathcal{O}_B$, so that $N\mathfrak{t}_0 = 49$. The prime 241 ramifies. At each of the eight primes of degree one, above $p \in \{2, 3, 5, 29\}$, the completion of B is $\mathbb{Q}_p$, and $\sqrt{241}$ maps to the square root of 241 in $\mathbb{Z}_p$ given in Table 3.

(d) Let $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2\}$ and $V = \mathcal{O}_B[1/30]^\times/\mathcal{O}_B[1/30]^{\times 2}$. The classes of $\alpha_0, \dots, \alpha_7$ form a basis of V , and V is the subgroup of $B^\times/B^{\times 2}$ of classes with even valuation at every prime outside S . Moreover $\text{Pic}(\mathcal{O}_B[1/30]) = 0$.

(e) The residue field of $\mathfrak{t}_0$ is $\mathbb{F}_{49}$, and α_i is a square modulo $\mathfrak{t}_0$ exactly for $i = 0, 4, 5, 6, 7$.

Proof. (a) Since $241 \equiv 1 \pmod{4}$, the ring of integers and the discriminant are as stated. The Minkowski bound is $\sqrt{241}/2 < 8$, so every ideal class contains an integral ideal of norm at most 7, which is a product of primes of norm at most 7. By (c), these are the six primes above 2, 3, 5, and they are principal.

(b) A direct computation gives $71011068^2 - 241 \cdot 4574225^2 = -1$. By Dirichlet's theorem $\mathcal{O}_B^\times = \{\pm 1\} \times \eta^\mathbb{Z}$ for a fundamental unit η , and $\varepsilon = \pm \eta^k$. Since $N_{B/\mathbb{Q}}(\varepsilon) = -1$, the exponent k is odd, so -1 and ε generate $\mathcal{O}_B^\times$ modulo squares. Neither -1 nor $\pm \varepsilon$ is a square, because B is real and $N_{B/\mathbb{Q}}(\pm \varepsilon) = -1$.

(c) We have $241 \equiv 1 \pmod{8}$, $241 \equiv 1 \pmod{3}$, $241 \equiv 1 \pmod{5}$, $241 \equiv 9 \pmod{29}$ and $241 \equiv 3 \pmod{7}$, and 3 is not a square modulo 7. Hence 2, 3, 5, 29 split, 7 is inert and 241 ramifies. The listed generators have norms $\pm 2, \pm 3, \pm 5, 29$, so they generate primes of degree one, and the displayed products show that the two generators above each p generate the two distinct primes above p ; for 29 the product of the two generators is 29. A prime of degree one above p is the preimage of $p\mathbb{Z}_p$ under an embedding $B \rightarrow \mathbb{Q}_p$, which sends $\sqrt{241}$ to one of the two square roots of 241 in $\mathbb{Z}_p$; the completion there is $\mathbb{Q}_p$, and the prime contains the stated generator exactly for the square root in Table 3.

(d) Every S -unit u satisfies $u\mathcal{O}_B = \prod_{i \geq 2} (\alpha_i \mathcal{O}_B)^{a_i}$, so $u \prod_{i \geq 2} \alpha_i^{-a_i}$ is a unit, and by (b) the classes of $\alpha_0, \dots, \alpha_7$ generate V . If $\prod_i \alpha_i^{a_i}$ with $a_i \in \{0, 1\}$ is a square, the valuations at S give $a_i = 0$ for $i \geq 2$, and then (b) gives $a_0 = a_1 = 0$. If $b \in B^\times$ has even valuation outside S , then $b\mathcal{O}_B = \mathfrak{a}^2 \prod_{\mathfrak{p} \in S} \mathfrak{p}^{a_{\mathfrak{p}}}$ with $\mathfrak{a}$ principal by (a), so b is an S -unit times a square. Finally $\text{Pic}(\mathcal{O}_B[1/30])$ is a quotient of $\text{Pic}(\mathcal{O}_B) = 0$.

(e) By (c), $N\mathfrak{t}_0 = 49$. An element $a \in \mathcal{O}_B$ prime to $\mathfrak{t}_0$ is a square modulo $\mathfrak{t}_0$ exactly when $a^{24} \equiv 1$, that is, when the reduction of $N_{B/\mathbb{Q}}(a) \equiv a^8$ is a square in $\mathbb{F}_7$. By the norms listed after (2.3), this holds for α_i exactly when $i = 0, 4, 5, 6, 7$. $\square$

The classes in Table 3 follow from the residues of $\sqrt{241}$ given there; at $p = 2$ they need its image modulo 32. For example, at $\mathfrak{p}_1$ we have $4574225 \equiv 1$ and $-71011068 \equiv 4$ modulo 8, so $\varepsilon \equiv 4 + 7 \equiv 3 \equiv -5 \pmod{8}$. The classes modulo the inert prime $\mathfrak{t}_0$ are given by Lemma 2.4(e).

2.2. Local Galois Groups. For a prime p let $\mathcal{G}_{\mathbb{Q}_p}$ be the Galois group of the maximal pro-2 extension of $\mathbb{Q}_p$, and for a place ν of B let $\mathcal{G}_\nu$ be the Galois group of the maximal pro-2 extension of the completion B_ν ; for a real place, $\mathcal{G}_\nu = \text{Gal}(\mathbb{C}/\mathbb{R})$. We write $(\cdot, \cdot)$ for the Hilbert symbol of order two of a local field [19, Chapter III, Section 4]. For odd p and p -adic units u, w , and for 2-adic units

TABLE 3. The image of $\sqrt{241}$ in $\mathbb{Z}_p$ at each prime of degree one, given by its residue, and in $\mathbb{R}$ at the real places; the classes of $\alpha_0, \dots, \alpha_7$ in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ at these primes, and their signs at the real places. At $p = 2$ the classes are written as $\pm 1, \pm 5, \pm 2, \pm 10$; at odd p as $1, u, p, up$, where $u = -1, 2, 2$ is a nonsquare unit for $p = 3, 5, 29$.

place	$\sqrt{241} \mapsto$	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
$\mathfrak{p}_1$	7 mod 32	-1	-5	-10	-5	1	5	-5	1
$\mathfrak{p}_2$	25 mod 32	-1	5	5	10	5	1	1	-5
$\mathfrak{q}_1$	2 mod 3	-1	1	-1	1	3	-1	-1	-1
$\mathfrak{q}_2$	1 mod 3	-1	-1	-1	1	-1	3	-1	-1
$\mathfrak{r}_1$	1 mod 5	1	2	2	1	1	2	10	2
$\mathfrak{r}_2$	4 mod 5	1	2	1	2	2	1	2	10
$\mathfrak{t}_1$	3 mod 29	1	1	2	1	1	2	2	2
$\mathfrak{t}_2$	26 mod 29	1	1	1	2	2	1	2	2
v_1	$+\sqrt{241}$	-	+	-	-	-	+	-	+
v_2	$-\sqrt{241}$	-	-	+	+	+	-	+	-

u, w ,

$$(2.5) \quad (p^a u, p^b w)_p = (-1)^{ab(p-1)/2} \left(\frac{u}{p}\right)^b \left(\frac{w}{p}\right)^a, \quad (2^a u, 2^b w)_2 = (-1)^{\frac{u-1}{2} \frac{w-1}{2} + a \frac{w^2-1}{8} + b \frac{u^2-1}{8}}$$

[33, Chapter III, Theorem 1], [19, Chapter VIII, Section 5].

Definition 2.6. Let $g_1, \dots, g_k$ generate a pro-2 group G , and let $\mathcal{F}_k$ be the free pro-2 group on k letters, mapped onto G by sending the letters to $g_1, \dots, g_k$. A *defining relator* of G with respect to $g_1, \dots, g_k$ is an element of $\mathcal{F}_k$ whose normal closure is the kernel of $\mathcal{F}_k \rightarrow G$. If a defining relator r lies in $D_2 \mathcal{F}_k$, its *quadratic initial* is its class in $\text{gr}_2 \mathcal{F}_k$.

Lemma 2.7. (a) If ν is real, then $\mathcal{G}_\nu = \langle \iota \rangle \cong C_2$ with the single defining relator ι^2 , and $\iota(\sqrt{b}) = -\sqrt{b}$ exactly when $b < 0$.

(b) Let p be an odd prime and ϖ a uniformizer of $\mathbb{Q}_p$. Then $\mathcal{G}_{\mathbb{Q}_p}$ is generated by a generator τ of its inertia group and a Frobenius lift φ with $\varphi(\sqrt{\varpi}) = \sqrt{\varpi}$, with the single defining relator $\varphi\tau\varphi^{-1}\tau^{-p}$. For $b \in \mathbb{Q}_p^\times$, $\tau(\sqrt{b}) = -\sqrt{b}$ exactly when $\text{ord}_p(b)$ is odd; for a unit b , $\varphi(\sqrt{b}) = -\sqrt{b}$ exactly when b is not a square modulo p . The relator has quadratic initial $[\tau, \varphi] + \frac{p-1}{2}\tau^{[2]}$.

(c) Let $E_2 = \mathbb{Q}_2(\sqrt{-1}, \sqrt{2}, \sqrt{5})$, and let $x, y, z \in \mathcal{G}_{\mathbb{Q}_2}$ multiply the triple $(\sqrt{2}, \sqrt{-1}, \sqrt{5})$ by the signs $(-, +, +)$, by $(+, -, +)$ and by $(+, -, -)$. Then x, y, z generate $\mathcal{G}_{\mathbb{Q}_2}$. If $b \equiv (-1)^{a_1} 2^{a_2} 5^{a_3}$ modulo squares, they multiply $\sqrt{b}$ by $(-1)^{a_2}$, $(-1)^{a_1}$ and $(-1)^{a_1+a_3}$, that is, by the Hilbert symbols $(5, b)_2$, $(-1, b)_2$ and $(-2, b)_2$. The group $\mathcal{G}_{\mathbb{Q}_2}$ has a single defining relator r with respect to x, y, z , and every such r has quadratic initial $y^{[2]} + [x, y] + [x, z]$.

Proof. (a) is clear.

(b) By Iwasawa's theorem [26, Theorem 7.5.3], the Galois group of the maximal tamely ramified extension of $\mathbb{Q}_p$ is generated by a Frobenius lift φ' and a generator τ of tame inertia, with the single relation $\varphi'\tau\varphi'^{-1} = \tau^p$. Since p is odd, every 2-extension of $\mathbb{Q}_p$ is tamely ramified, so $\mathcal{G}_{\mathbb{Q}_p}$ is the pro-2 group with the same presentation. The extension $\mathbb{Q}_p(\sqrt{\varpi})$ is ramified, so τ moves $\sqrt{\varpi}$; replacing φ' by $\varphi'\tau$ if necessary gives φ . This substitution does not change the relator, since $(\varphi'\tau)\tau(\varphi'\tau)^{-1} = \varphi'\tau\varphi'^{-1}$. The actions on square roots hold because $\mathbb{Q}_p(\sqrt{b})$ is ramified exactly when $\text{ord}_p(b)$ is odd, and because φ acts on unramified extensions as the Frobenius. Modulo D_3 , the element $\varphi\tau\varphi^{-1}\tau^{-1}$ has class $[\varphi, \tau] = [\tau, \varphi]$, and τ^{1-p} has class $\frac{p-1}{2}\tau^{[2]}$.

(c) We first show that x, y, z generate $\mathcal{G}_{\mathbb{Q}_2}$, and then read off the quadratic initial of r from the cup-product pairing on $H^1(\mathcal{G}_{\mathbb{Q}_2}, \mathbb{F}_2)$, which is given by the Hilbert symbol. By Kummer theory the maximal elementary abelian quotient of $\mathcal{G}_{\mathbb{Q}_2}$ is $\text{Gal}(E_2/\mathbb{Q}_2)$, since $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ has basis $-1, 2, 5$. The images of x, y, z form a basis of it, so x, y, z generate [26, Proposition 3.9.1]. The action on $\sqrt{b}$ is read off from the actions on $\sqrt{-1}, \sqrt{2}, \sqrt{5}$, and it agrees with the stated Hilbert symbols by (2.5). By [26, Theorem 7.5.11], $\mathcal{G}_{\mathbb{Q}_2}$ is a Demuškin group of rank 3: it has a single defining relator r , and $H^2(\mathcal{G}_{\mathbb{Q}_2}, \mathbb{F}_2) \cong \mathbb{F}_2$. For $b \in \mathbb{Q}_2^\times$ let χ_b be the character with $g(\sqrt{b}) = (-1)^{\chi_b(g)}\sqrt{b}$. The characters dual to x, y, z are $\chi_2, \chi_{-5}, \chi_5$. Inflation identifies $H^2(\mathcal{G}_{\mathbb{Q}_2}, \mathbb{F}_2)$ with H^2 of the absolute Galois group of $\mathbb{Q}_2$ [26, Proposition 7.5.8], and there the invariant of $\chi_a \cup \chi_b$ is given by the Hilbert symbol $(a, b)_2$ [19, Chapter III, Section 4]. By (2.5), the matrix of the indicator of $(a, b)_2 = -1$ on $2, -5, 5$ is

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The evaluation tr_r of the transgression at r is an isomorphism $H^2(\mathcal{G}_{\mathbb{Q}_2}, \mathbb{F}_2) \rightarrow \mathbb{F}_2$ [26, Proposition 3.9.12(iii)], and so is the invariant, so the two coincide. We now apply the relation-cup identity [26, Proposition 3.9.13(ii)], see also [30, Proposition 3.2]. Write g_1, g_2, g_3 for x, y, z . The identity writes the relator as $r = \prod_j g_j^{q a_j} \prod_{k < l} [g_k, g_l]^{a_{kl}} r'$, with r' in the third term of the descending q -central series, and states that tr_r of the cup product of the characters dual to g_k and g_l is $-a_{kl}$ for $k < l$ and $-\binom{q}{2} a_k$ for $k = l$. Here q , the smallest elementary divisor of the abelianization of $\mathcal{G}_{\mathbb{Q}_2}$, is 2: by local class field theory this abelianization is the pro-2 completion of $\mathbb{Q}_2^\times$, which is $\mathbb{Z}_2^2 \times \mathbb{Z}/2$. The third term of the 2-central series is $(D_2)^2[D_2, D_1] = D_3$ by Lazard's formula, the class of g_j^2 in gr_2 is $g_j^{[2]}$, and the signs disappear modulo 2, with $\binom{2}{2} = 1$. Hence the off-diagonal entries of the matrix are the coefficients of $[x, y], [x, z], [y, z]$ in the quadratic initial of r , and the diagonal entries, which are the values of the cup squares $\chi \cup \chi$, are the coefficients of $x^{[2]}, y^{[2]}, z^{[2]}$. For $p = 2$ the cup square of a character is its Bockstein, so the diagonal coefficients are also given by [26, Proposition 3.9.14]. $\square$

We now construct the dyadic local field. Let U_4 be the unramified extension of $\mathbb{Q}_2$ of degree four, with Frobenius Fr ; let $i = \sqrt{-1}$, $k = \mathbb{Q}_2(i)$, $\alpha = 1 + 2i$, and

$$M_8 = \mathbb{Q}_2(i, \sqrt{5}, \sqrt{\alpha}), \quad M_{16} = M_8(\sqrt{2}), \quad L_2 = M_{16}U_4.$$

Since $\alpha\bar{\alpha} = 5$ with $\bar{\alpha} = 1 - 2i$, the field M_8 contains $\sqrt{\bar{\alpha}} = \sqrt{5}/\sqrt{\alpha}$. Let σ_y and σ_z be the automorphisms of M_8 given by

$$\sigma_y : i \mapsto -i, \sqrt{5} \mapsto \sqrt{5}, \sqrt{\alpha} \mapsto \sqrt{5}/\sqrt{\alpha}; \quad \sigma_z : i \mapsto -i, \sqrt{5} \mapsto -\sqrt{5}, \sqrt{\alpha} \mapsto \sqrt{5}/\sqrt{\alpha}.$$

Lemma 2.8. (a) *The extension $M_8/\mathbb{Q}_2$ is Galois of degree 8, and its Galois group $\langle \sigma_y, \sigma_z \rangle$ is dihedral.*

(b) *The extension $L_2/\mathbb{Q}_2$ is Galois of degree 32, with ramification index 8 and residue degree 4. There are unique $x, y, z \in \text{Gal}(L_2/\mathbb{Q}_2)$ such that x is trivial on M_8 and U_4 and negates $\sqrt{2}$; y restricts to σ_y on M_8 , fixes $\sqrt{2}$ and is trivial on U_4 ; and z restricts to σ_z on M_8 , fixes $\sqrt{2}$ and restricts to Fr on U_4 . They act on $E_2 \subset L_2$ as in Lemma 2.7(c), and the map sending the generators of*

$$D = \langle x, y, z \mid x^2, y^2, z^4, [y, z]^2, [x, y], [x, z], [[y, z], z] \rangle$$

to x, y, z is an isomorphism $D \cong \text{Gal}(L_2/\mathbb{Q}_2)$. The inertia group is $\langle x, y, [y, z] \rangle \cong C_2^3$.

(c) *The graded pieces of the Zassenhaus filtration of D are $\text{gr}_1 D = \langle \bar{x}, \bar{y}, \bar{z} \rangle \cong \mathbb{F}_2^3$ and $\text{gr}_2 D = \langle z^2, [y, z] \rangle \cong \mathbb{F}_2^2$, and $D_3(D) = 1$, so the Hilbert polynomial of $\mathbb{F}_2[D]$ (Definition 2.1) is $h_{\mathbb{F}_2[D]}(t) = (1+t)^3(1+t^2)^2$.*

- (d) The different $\mathfrak{D}_{L_2/\mathbb{Q}_2}$ has valuation 18 in L_2 ; equivalently, $\text{ord}_2(\mathfrak{D}_{L_2/\mathbb{Q}_2}) = 18/8 = 9/4$, where ord_2 is the valuation of L_2 normalized by $\text{ord}_2(2) = 1$.

Proof. Quadratic extensions of k . Let ord_k be the normalized valuation of k . Put $\varpi = 1 + i$, a uniformizer of k , so that $\text{ord}_k(2) = 2$, and for $b \in k^\times$ let $c(b)$ be the exponent of the conductor of $k(\sqrt{b})/k$, which for a quadratic extension equals the exponent of its discriminant. Then $c(5) = 0$, since $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified. Since $\alpha = 1 + \varpi^2$, the element $\varpi_\alpha = (\sqrt{\alpha} - 1 - \varpi)/\varpi$ is a root of the Eisenstein polynomial $X^2 + \frac{2(1+\varpi)}{\varpi}X + \frac{2}{\varpi}$; its derivative at ϖ_α is the sum of terms of valuations 5 and 2 in $k(\sqrt{\alpha})$, so $c(\alpha) = 2$. Next $2\alpha = \varpi^2\alpha'$ with $\alpha' = 2 - i$, and $\sqrt{\alpha'} - 1$ is a root of $X^2 + 2X + 1 - \alpha'$, which is Eisenstein since $\text{ord}_k(1 - \alpha') = 1$; its derivative $2\sqrt{\alpha'}$ has valuation 4, so $c(2\alpha) = 4$. Similarly $2 = -i\varpi^2$, $-i \equiv i$ modulo squares, and $\sqrt{i} - 1$ is a root of $X^2 + 2X + 1 - i$, so $c(2) = 4$. Finally $c(5b) = c(b)$ when $b \notin k^{\times 2} \cup 5k^{\times 2}$: the field $k(\sqrt{5}, \sqrt{b})$ is unramified over both $k(\sqrt{b})$ and $k(\sqrt{5b})$, so the two ways of computing its discriminant over k give $2c(b) = 2c(5b)$.

(a) Since $k(\sqrt{5})/k$ is unramified and $k(\sqrt{\alpha})/k$ is ramified, α is not a square in $k(\sqrt{5})$, so $[M_8 : \mathbb{Q}_2] = 8$. The field M_8 contains the conjugate $\sqrt{\alpha}$ of $\sqrt{\alpha}$, so it is Galois over $\mathbb{Q}_2$, and an automorphism is determined by the images $\pm i, \pm\sqrt{5}$ and a square root of the image of α ; in particular σ_y and σ_z exist. Now $\sigma_y^2 = 1$, σ_z^2 fixes $i, \sqrt{5}$ and negates $\sqrt{\alpha}$, σ_z has order four, and $\sigma_y\sigma_z\sigma_y = \sigma_z^{-1}$. So $\text{Gal}(M_8/\mathbb{Q}_2) = \langle \sigma_y, \sigma_z \rangle$ is dihedral of order eight, with center $\langle \sigma_z^2 \rangle$ and maximal abelian subextension $\mathbb{Q}_2(i, \sqrt{5})$.

(b) The quadratic subfields of M_8 are $\mathbb{Q}_2(\sqrt{b})$ for $b = -1, 5, -5$, so $\sqrt{2} \notin M_8$, and M_{16} has degree 16 and group $\text{Gal}(M_8/\mathbb{Q}_2) \times C_2$. This group has elementary abelian abelianization, so the maximal unramified subextension of M_{16} , which is cyclic over $\mathbb{Q}_2$ and contains $\mathbb{Q}_2(\sqrt{5})$, is $\mathbb{Q}_2(\sqrt{5})$. Hence M_{16} has ramification index 8, $M_{16} \cap U_4 = \mathbb{Q}_2(\sqrt{5})$, and $[L_2 : \mathbb{Q}_2] = 16 \cdot 4/2 = 32$. Since L_2 contains U_4 and has ramification index at least 8, its residue degree is 4 and its ramification index is 8. Restriction identifies $\text{Gal}(L_2/\mathbb{Q}_2)$ with the set of triples (σ, ϵ, μ) , where $\sigma \in \text{Gal}(M_8/\mathbb{Q}_2)$, $\epsilon = \pm 1$ is the sign by which the element multiplies $\sqrt{2}$, and $\mu \in \text{Gal}(U_4/\mathbb{Q}_2)$ agrees with σ on $\sqrt{5}$; both sets have 32 elements. Since Fr negates $\sqrt{5}$, the triples

$$x = (1, -1, 1), \quad y = (\sigma_y, 1, 1), \quad z = (\sigma_z, 1, \text{Fr}), \quad w = [y, z] = (\sigma_z^2, 1, 1)$$

exist and are the unique elements described in the statement. They act on E_2 as required. The elements x and w are central involutions, y is an involution, and z has order four. Hence the relations of D hold. Conversely, in D these relations make $w = [y, z]$ central: $w^y = w^{-1} = w$, and $[w, z] = 1$ is imposed. Since $zy = yzw$, every element of D is $x^{a_1}y^{a_2}z^{a_3}w^{a_4}$ with $a_1, a_2, a_4 \in \mathbb{F}_2$ and $a_3 \in \mathbb{Z}/4$, and

$$(a_1, a_2, a_3, a_4)(a'_1, a'_2, a'_3, a'_4) = (a_1 + a'_1, a_2 + a'_2, a_3 + a'_3, a_4 + a'_4 + a_3a'_2).$$

These 32 normal forms have distinct images in $\text{Gal}(L_2/\mathbb{Q}_2)$: the third component determines a_3 , the second a_1 , and $\sigma_y^{a_2}\sigma_z^{a_3+2a_4}$ determines a_2 and a_4 . So $D \cong \text{Gal}(L_2/\mathbb{Q}_2)$. The inertia group consists of the elements trivial on U_4 , namely $\langle x, y, w \rangle$.

(c) The Frattini subgroup of D is $\langle z^2, w \rangle$, which is central of exponent two, and D has exponent four. So Lazard's formula gives $D_3(D) = [[D, D], D][D, D]^2D^4 = 1$, and the Hilbert polynomial follows from Theorem 2.2.

(d) The extension M_{16}/k is abelian with group C_2^3 , generated by $\sqrt{5}, \sqrt{\alpha}, \sqrt{2}$. We apply the conductor–discriminant formula for abelian extensions [19, Chapter V, Theorem 3.27] to the extension $\mathbb{Q}(i)(\sqrt{5}, \sqrt{1+2i}, \sqrt{2})$ of $\mathbb{Q}(i)$, whose completion at the unique prime above $1+i$ is M_{16}/k . Taking $(1+i)$ -adic valuations gives

$$\text{ord}_k(\mathfrak{D}_{M_{16}/k}) = \sum_b c(b) = 0 + 0 + 2 + 2 + 4 + 4 + 4 + 4 = 20,$$

the sum over the classes $b = 1, 5, \alpha, 5\alpha, 2, 10, 2\alpha, 10\alpha$. Hence

$$\text{ord}_2(\mathfrak{d}_{M_{16}/\mathbb{Q}_2}) = [M_{16} : k] \text{ord}_2(\mathfrak{d}_{k/\mathbb{Q}_2}) + 20 = 8 \cdot 2 + 20 = 36.$$

Since M_{16} has residue degree two over $\mathbb{Q}_2$, its different has valuation $36/2 = 18$. The extension L_2/M_{16} is unramified, so the different of $L_2/\mathbb{Q}_2$ also has valuation 18, and $18/8 = 9/4$. $\square$

Remark 2.9. The field E_2 is the maximal elementary abelian subextension of L_2 , so $\text{Gal}(L_2/E_2)$ is the Frattini subgroup $\langle z^2, [y, z] \rangle$, which is central of exponent two. Hence any triple in $\text{Gal}(L_2/\mathbb{Q}_2)$ that acts on E_2 as x, y, z do differs from x, y, z by central elements of order at most two; it satisfies the relations of D and generates, so it also defines an isomorphism $D \cong \text{Gal}(L_2/\mathbb{Q}_2)$. The description of the inertia group, however, refers to the triple of Lemma 2.8(b).

2.3. The Global Group and Its Complete Presentation. Let B_S be the maximal pro-2 extension of B , in a fixed algebraic closure, that is unramified at every finite prime outside S ; no condition is imposed at v_1, v_2 . Let $G_S = \text{Gal}(B_S/B)$, and let $E = B(\sqrt{\alpha_0}, \dots, \sqrt{\alpha_7}) = B(\sqrt{V})$ be the *Kummer field*.

Lemma 2.10. *The field E is the maximal elementary abelian extension of B contained in B_S , and $[E : B] = 256$. Hence $G_S/D_2G_S = \text{Gal}(E/B)$.*

Proof. Every prime above 2 lies in S , so a quadratic extension $B(\sqrt{b})$ lies in B_S exactly when b has even valuation outside S . By Lemma 2.4(d), E is the maximal elementary abelian extension of B in B_S , and $[E : B] = 256$. Since D_2G_S is the Frattini subgroup of G_S , its fixed field is this maximal elementary abelian extension. $\square$

Definition 2.11. Let $M \subseteq B_S$ be a Galois extension of B containing E , for example $M = B_S$. The *elementary image* of $g \in \text{Gal}(M/B)$ is the vector $\bar{g} \in \mathbb{F}_2^8$ with $g(\sqrt{\alpha_i}) = (-1)^{\bar{g}_i} \sqrt{\alpha_i}$ for $0 \leq i \leq 7$. For $a \in V$, the *Kummer character* χ_a is defined by $g(\sqrt{a}) = (-1)^{\chi_a(g)} \sqrt{a}$; its values lie in $\mathbb{F}_2$.

By Lemmas 2.4(d) and 2.10, $g \mapsto \bar{g}$ identifies $G_S/D_2G_S = \text{Gal}(E/B)$ with $\mathbb{F}_2^8$, and $a \mapsto \chi_a$ identifies V with the dual of $\mathbb{F}_2^8$, with $\chi_{\alpha_i}(g) = \bar{g}_i$. We write vectors in $\mathbb{F}_2^8$ as strings $c_0c_1 \cdots c_7$ of their coordinates.

For a place ν of B , a choice of a place of B_S above ν gives a homomorphism $\mathcal{G}_\nu \rightarrow G_S$, the *local map* at ν ; another choice changes it by an inner automorphism of G_S . For a finite place $\nu \notin S$, the local map kills inertia, and its image is generated by a Frobenius element Frob_ν . Let $\Sigma = S \cup \{v_1, v_2\}$.

Definition 2.12. Fix a place of B_S above each place of B , and use it to define the local maps. For $\nu \in \Sigma$ we fix generators of $\mathcal{G}_\nu$ as follows, and use the same names for their images in G_S : ι_j at v_j (Lemma 2.7(a)), so that ι_1, ι_2 are complex conjugations; τ_ν, φ_ν at $\nu \in \{q_1, q_2, \mathfrak{r}_1, \mathfrak{r}_2\}$, with the generator α_i of ν as uniformizer ϖ in Lemma 2.7(b); and x_j, y_j, z_j at $\mathfrak{p}_j$, the images of one fixed triple $x, y, z \in \mathcal{G}_{\mathbb{Q}_2} = \mathcal{G}_{\mathfrak{p}_j}$ lifting the elements x, y, z of Lemma 2.8(b). We also write $\text{Frob}_{\mathfrak{t}_k}$ for $k = 0, 1, 2$. These elements are the *local generators*: those at $\nu \in \Sigma$ are the generators just fixed, and the local generator at $\mathfrak{t}_k$ is $\text{Frob}_{\mathfrak{t}_k}$.

The triple x, y, z satisfies the hypothesis of Lemma 2.7(c).

Table 4 lists the elementary images. They follow from Lemma 2.7, Table 3 and Lemma 2.4(e). For example, at the places above 3 and 5 the vector of τ_ν marks the odd valuations, and that of φ_ν marks the units that are not squares modulo ν , with a zero at the generator of ν . The columns headed “action” express the same actions as Hilbert symbols, that is, as local Artin symbols [19, Chapter III, Remark 4.5]. The supplementary program `kummer241.gp` checks the norms of the α_i , the generators of the primes in Lemma 2.4(c) and the residues of $\sqrt{241}$ in Table 3, and recomputes Table 4 from these Hilbert symbols.

Fix a minimal presentation $1 \rightarrow R \rightarrow \mathcal{F} \rightarrow G_S \rightarrow 1$, where $\mathcal{F}$ is a free pro-2 group of rank 8. Minimality means $R \subset D_2\mathcal{F}$, so $\mathcal{F}/D_2\mathcal{F} = \mathbb{F}_2^8$ with the coordinates above. Put $\mathfrak{L} = \text{gr } \mathcal{F}$, so that

TABLE 4. Elementary images in $\mathbb{F}_2^8$ of the local generators. Entry i is 1 exactly when the element negates $\sqrt{\alpha_i}$. The third and sixth columns give the action on $\sqrt{b}$ for b in the completion.

element	image	action	element	image	action
ι_1	10111010	sign at v_1	ι_2	11000101	sign at v_2
x_1	00100000	$(5, b)_{\mathfrak{p}_1}$	x_2	00010000	$(5, b)_{\mathfrak{p}_2}$
y_1	11110010	$(-1, b)_{\mathfrak{p}_1}$	y_2	10000001	$(-1, b)_{\mathfrak{p}_2}$
z_1	10000100	$(-2, b)_{\mathfrak{p}_1}$	z_2	11111000	$(-2, b)_{\mathfrak{p}_2}$
$\tau_{\mathfrak{q}_1}$	00001000	$(-1, b)_{\mathfrak{q}_1}$	$\varphi_{\mathfrak{q}_1}$	10100111	$(-\alpha_4, b)_{\mathfrak{q}_1}$
$\tau_{\mathfrak{q}_2}$	00000100	$(-1, b)_{\mathfrak{q}_2}$	$\varphi_{\mathfrak{q}_2}$	11101011	$(-\alpha_5, b)_{\mathfrak{q}_2}$
$\tau_{\mathfrak{r}_1}$	00000010	$(2, b)_{\mathfrak{r}_1}$	$\varphi_{\mathfrak{r}_1}$	01100101	$(-\alpha_6, b)_{\mathfrak{r}_1}$
$\tau_{\mathfrak{r}_2}$	00000001	$(2, b)_{\mathfrak{r}_2}$	$\varphi_{\mathfrak{r}_2}$	01011010	$(-\alpha_7, b)_{\mathfrak{r}_2}$
$\text{Frob}_{\mathfrak{t}_1}$	00100111	$(29, b)_{\mathfrak{t}_1}$	$\text{Frob}_{\mathfrak{t}_2}$	00011011	$(29, b)_{\mathfrak{t}_2}$
$\text{Frob}_{\mathfrak{t}_0}$	01110000	$(7, b)_{\mathfrak{t}_0}$			

$\dim \mathfrak{L}_1 = 8$, $\dim \mathfrak{L}_2 = 36$ and $\dim \mathfrak{L}_3 = 168$. For $v, w \in \mathfrak{L}_1$ we have $(v + w)^{[2]} = v^{[2]} + w^{[2]} + [v, w]$, and the square of an element of $\mathcal{F}$ with image v has class $v^{[2]}$. For each local generator g above choose a lift $\hat{g} \in \mathcal{F}$, and define the local relators

$$(2.13) \quad \rho_{v_j} = \hat{l}_j^2, \quad \rho_\nu = \hat{\varphi}_\nu \hat{\tau}_\nu \hat{\varphi}_\nu^{-1} \hat{\tau}_\nu^{-p} \quad (\nu \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2\}), \quad \rho_{\mathfrak{p}_j} = r(\hat{x}_j, \hat{y}_j, \hat{z}_j),$$

where $p \in \{3, 5\}$ is the rational prime below ν , and r is a defining relator of $\mathcal{G}_{\mathbb{Q}_2}$ with respect to the fixed triple x, y, z , the same for $j = 1, 2$. They lie in R , because each local relation holds in $\mathcal{G}_\nu$. Their classes in $\mathfrak{L}_2$ are obtained by substituting elementary images into the quadratic initials of Lemma 2.7:

$$(2.14) \quad \bar{l}_j^{[2]}, \quad [\bar{\tau}_\nu, \bar{\varphi}_\nu] + \frac{p-1}{2} \bar{\tau}_\nu^{[2]}, \quad \bar{y}_j^{[2]} + [\bar{x}_j, \bar{y}_j] + [\bar{x}_j, \bar{z}_j].$$

The results below hold for every minimal presentation and every choice of lifts.

The classes (2.14) have an arithmetic meaning. As in the conventions, we realize $\mathfrak{L}$ inside the free associative algebra $\mathbb{F}_2\langle X_0, \dots, X_7 \rangle$, where $X_0, \dots, X_7$ is the standard basis of $\mathfrak{L}_1 = \mathbb{F}_2^8$. The elements $X_i^{[2]} = X_i^2$ and $[X_i, X_j] = X_i X_j + X_j X_i$ ($i < j$) form a basis of $\mathfrak{L}_2$, so there is a linear isomorphism β from $\mathfrak{L}_2$ onto the space of symmetric bilinear forms on V with

$$\beta(v^{[2]})(a, b) = \chi_a(v) \chi_b(v), \quad \beta([v, w])(a, b) = \chi_a(v) \chi_b(w) + \chi_a(w) \chi_b(v) \quad (v, w \in \mathfrak{L}_1).$$

It is defined by these formulas for basis vectors v, w , which send the basis of $\mathfrak{L}_2$ to a basis of the symmetric bilinear forms. The formulas then hold for all v, w , because the bracket is bilinear, $(v + w)^{[2]} = v^{[2]} + w^{[2]} + [v, w]$, and squaring is the identity on $\mathbb{F}_2$. Equivalently, if $\xi \in \mathfrak{L}_2$ is written in the free algebra as $\sum_{i,j} n_{ij} X_i X_j$, then $\beta(\xi)(\alpha_i, \alpha_j) = n_{ij}$.

Definition 2.15. For $\nu \in \Sigma$, the *local Hilbert form* H_ν is the symmetric bilinear form on V with $H_\nu(a, b) = 1$ if $(a, b)_\nu = -1$ and $H_\nu(a, b) = 0$ otherwise.

Lemma 2.16. For every $\nu \in \Sigma$, β maps the class of ρ_ν to H_ν . The eight classes (2.14), one for each $\nu \in \Sigma$, sum to zero, and the seven classes with $\nu \neq \mathfrak{p}_1$ are linearly independent.

Proof. For a local generator g at ν , $\chi_a(\bar{g})$ is the value at g of the local Kummer character of the image of a in B_ν . Hence β of the class of ρ_ν is the pullback to V of a symmetric bilinear form on $B_\nu^\times / B_\nu^{\times 2}$, as is H_ν , and it suffices to compare the two on a basis of $B_\nu^\times / B_\nu^{\times 2}$. At a real place the only class is -1 , and both forms take the value 1 on $(-1, -1)$. At ν above $p \in \{3, 5\}$, take the basis ϖ, u with ϖ the generator of ν and u a nonsquare unit. By Lemma 2.7(b), $\chi_\varpi(\tau) = \chi_u(\varphi) = 1$ and $\chi_\varpi(\varphi) = \chi_u(\tau) = 0$, so the form of $[\tau, \varphi] + \frac{p-1}{2} \tau^{[2]}$ takes the values $\frac{p-1}{2}, 1, 0$ on $(\varpi, \varpi), (\varpi, u),$

(u, u) ; by (2.5) these are the indicators of $(\varpi, \varpi)_p = (-1)^{(p-1)/2}$, $(\varpi, u)_p = -1$ and $(u, u)_p = 1$. At $\mathfrak{p}_j$ the characters $\chi_2, \chi_{-5}, \chi_5$ are dual to x, y, z , as in the proof of Lemma 2.7(c). So $y^{[2]}$ contributes the entry at $(-5, -5)$, $[x, y]$ the entries at $(2, -5)$ and $(-5, 2)$, and $[x, z]$ those at $(2, 5)$ and $(5, 2)$: the form of $y^{[2]} + [x, y] + [x, z]$ on the basis $2, -5, 5$ is the matrix of the Hilbert symbol displayed in that proof, from which this initial was obtained.

For $a, b \in V$ and a place $\nu' \notin \Sigma$, the place ν' is finite and not above 2, and a, b are units at ν' , so $(a, b)_{\nu'} = 1$ [19, Chapter VIII, 5.8]. By the product formula for the Hilbert symbol [19, Chapter V, Example 5.4], $\sum_{\nu \in \Sigma} H_\nu = 0$, so the eight classes sum to zero.

Finally, by Table 3 and (2.5), the seven pairs

$$(-1, \alpha_2), (-1, \varepsilon), (-1, \alpha_7), (-1, \alpha_4), (-1, \alpha_5), (\alpha_2, \alpha_6), (\varepsilon, \alpha_7)$$

have Hilbert symbol -1 exactly at $\{\mathfrak{p}_1, v_1\}$, $\{\mathfrak{p}_1, v_2\}$, $\{\mathfrak{p}_2, v_2\}$, $\{\mathfrak{q}_1, v_1\}$, $\{\mathfrak{q}_2, v_2\}$, $\{\mathfrak{r}_1, v_1\}$ and $\{\mathfrak{r}_2, v_2\}$; the supplementary program `cup241.gp` recomputes these symbols. Evaluating a relation $\sum_{\nu \neq \mathfrak{p}_1} n_\nu H_\nu = 0$, with $n_\nu \in \mathbb{F}_2$, at the first two pairs gives $n_{v_1} = n_{v_2} = 0$, and then at the other five pairs gives $n_{\mathfrak{p}_2} = n_{\mathfrak{q}_1} = n_{\mathfrak{q}_2} = n_{\mathfrak{r}_1} = n_{\mathfrak{r}_2} = 0$. $\square$

Lemma 2.17. *The group G_S has generator rank 8 and relation rank 7. The seven relators ρ_ν with $\nu \in \Sigma \setminus \{\mathfrak{p}_1\}$ form a minimal system of defining relations: their normal closure in $\mathcal{F}$ is R . In particular the dyadic local relator $\rho_{\mathfrak{p}_1}$ lies in the normal closure of the other seven.*

Proof. The generator rank is $\dim H^1(G_S, \mathbb{F}_2) = 8$, by Lemma 2.10 and [26, Proposition 3.9.1].

Next we bound H^2 . Let $X = \text{Spec } \mathcal{O}_B[1/30]$. Since 2 is invertible on X , the sheaf μ_2 is the constant sheaf $\mathbb{F}_2$. The finite subextensions of B_S/B correspond to the connected finite étale Galois 2-covers $Y \rightarrow X$, and the Hochschild–Serre spectral sequence of this system of covers [17, Theorem 14.9 and Remark 14.10] gives an exact sequence

$$0 \rightarrow H^1(G_S, \mathbb{F}_2) \rightarrow H^1(X, \mathbb{F}_2) \rightarrow \left(\varinjlim_Y H^1(Y, \mathbb{F}_2) \right)^{G_S} \rightarrow H^2(G_S, \mathbb{F}_2) \rightarrow H^2(X, \mathbb{F}_2).$$

A class in $H^1(Y, \mathbb{F}_2)$ is an étale double cover of Y . Its Galois closure over X is a finite étale Galois cover whose group embeds in the wreath product of $\text{Gal}(Y/X)$ with C_2 , hence a 2-cover in this system, over which the class vanishes. So the direct limit is zero, and $H^2(G_S, \mathbb{F}_2)$ injects into $H^2(X, \mu_2)$. The Kummer sequence and $\text{Pic}(X) = 0$ identify $H^2(X, \mu_2)$ with $\text{Br}(X)[2]$, where $\text{Br}(X) = H^2(X, \mathbb{G}_m)$. By [29, Theorem 6.8.3 and Example 6.9.4], $\text{Br}(X)$ is the kernel of the sum of the local invariants $\bigoplus_{\nu \in \Sigma} \text{Br}(B_\nu) \rightarrow \mathbb{Q}/\mathbb{Z}$. Each of the eight groups $\text{Br}(B_\nu)[2]$ has order two, and the sum of the invariants maps their direct sum onto $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, so $\dim \text{Br}(X)[2] = 7$. We use only the resulting bound $\dim H^2(G_S, \mathbb{F}_2) \leq \dim \text{Br}(X)[2] \leq 7$.

By Lemma 2.16, the classes in $\mathfrak{L}_2$ of the seven relators ρ_ν , $\nu \neq \mathfrak{p}_1$, are linearly independent. Since $R \subset D_2\mathcal{F}$, we have $R^2[R, \mathcal{F}] \subset D_3\mathcal{F}$, so the classes of these seven relators in $R/R^2[R, \mathcal{F}]$ are independent. On the other hand $\dim R/R^2[R, \mathcal{F}] = \dim H^2(G_S, \mathbb{F}_2) \leq 7$ by the five-term exact sequence of the presentation [26, Proposition 3.9.5], [30, (3.3)–(3.4)]. Hence the seven classes form a basis, the relation rank is 7, and by the pro-2 Nakayama lemma [26, Corollary 3.9.3] the seven relators generate R as a normal subgroup. Finally $\rho_{\mathfrak{p}_1} \in R$. $\square$

Corollary 2.18. *Any seven of the eight local relators ρ_ν , $\nu \in \Sigma$, generate R as a normal subgroup.*

Proof. By Lemma 2.16, the only linear relation among the eight classes (2.14) is that their sum vanishes, and this relation is Hilbert reciprocity. Hence any seven of the eight classes are linearly independent, and the proof of Lemma 2.17 applies to any seven of the eight local relators. $\square$

We omit the dyadic relator at $\mathfrak{p}_1$.

Remark 2.19. By Lemma 2.17, the bound $\dim H^2(G_S, \mathbb{F}_2) \leq \dim \text{Br}(X)[2] = 7$ is attained, so $H^2(G_S, \mathbb{F}_2) \rightarrow \text{Br}(X)[2]$ is an isomorphism. This can also be seen directly: the cup product $\chi_a \cup \chi_b$

maps to the class of the quaternion algebra (a, b) , whose invariant at ν is given by $(a, b)_\nu$ [19, Chapter III, Remark 4.7], and the seven pairs in the proof of Lemma 2.16 give seven classes with independent invariant vectors. The supplementary program `cup241.gp` computes the invariant vectors at the eight places of Σ of all 36 algebras (α_i, α_j) .

2.4. The Prescribed Local Groups. We now cut G_S down to prescribed local groups. At the dyadic places we use the restriction $\mathcal{G}_{\mathfrak{p}_j} = \mathcal{G}_{\mathbb{Q}_2} \rightarrow \text{Gal}(L_2/\mathbb{Q}_2) = D$ of Lemma 2.8. At a place ν above $p \in \{3, 5\}$, the maximal elementary abelian quotient of $\mathcal{G}_\nu$ is $\text{Gal}(\mathbb{Q}_p(\sqrt{u}, \sqrt{p})/\mathbb{Q}_p) \cong C_2 \times C_2$ for a nonsquare unit u ; this quotient has ramification index and residue degree two. At $\mathfrak{t}_1, \mathfrak{t}_2$, whose completions are $\mathbb{Q}_{29}$, and at $\mathfrak{t}_0$, whose residue field is $\mathbb{F}_{49}$, we bound the order of the Frobenius by four.

Definition 2.20. Let N be the normal closure in G_S of the images of $\ker(\mathcal{G}_{\mathfrak{p}_j} \rightarrow D)$ for $j = 1, 2$, of the Frattini subgroups $D_2\mathcal{G}_\nu$ for $\nu \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2\}$, and of $\text{Frob}_{\mathfrak{t}_k}^4$ for $k = 0, 1, 2$. Put $G_B = G_S/N$ and $\overline{G}_B = G_B/D_4G_B$, and let $B_G \subset B_S$ be the fixed field of N , so that $\text{Gal}(B_G/B) = G_B$. We call the extension B_G/B the *tower*.

This does not depend on the choice of places of B_S above each ν : another choice changes each local map by an inner automorphism of G_S , which replaces the images above by conjugates and does not change their normal closure N .

Lemma 2.21. (a) *The image of $\mathcal{G}_{\mathfrak{p}_j}$ in G_B is a quotient of D , the image of $\mathcal{G}_\nu$ for ν above 3 or 5 is a quotient of $C_2 \times C_2$ in which inertia maps to the image of τ_ν , and $\text{Frob}_{\mathfrak{t}_k}$ has order dividing four in G_B .*

(b) *$N \subseteq D_2G_S$. Hence $G_B/D_2G_B = \text{Gal}(E/B)$, and $E \subseteq B_G$ is the fixed field of D_2G_B .*

Proof. (a) By Definition 2.20, the maps $\mathcal{G}_{\mathfrak{p}_j} \rightarrow G_B$ and $\mathcal{G}_\nu \rightarrow G_B$ kill $\ker(\mathcal{G}_{\mathfrak{p}_j} \rightarrow D)$ and $D_2\mathcal{G}_\nu$, and $\text{Frob}_{\mathfrak{t}_k}^4 \in N$. For ν above 3 or 5, $\mathcal{G}_\nu/D_2\mathcal{G}_\nu \cong C_2 \times C_2$, and the inertia group of $\mathcal{G}_\nu$ is generated by τ_ν (Lemma 2.7(b)).

(b) Since D and $\mathcal{G}_{\mathbb{Q}_2}$ both have generator rank three, $\ker(\mathcal{G}_{\mathfrak{p}_j} \rightarrow D)$ lies in the Frattini subgroup of $\mathcal{G}_{\mathfrak{p}_j}$. The images of the Frattini subgroups of the local groups, and the fourth powers $\text{Frob}_{\mathfrak{t}_k}^4$, lie in D_2G_S . Hence $N \subseteq D_2G_S$, and $G_B/D_2G_B = G_S/D_2G_S = \text{Gal}(E/B)$ by Lemma 2.10. $\square$

By Lemma 2.26(b) below, the quotients in Lemma 2.21(a) are D and $C_2 \times C_2$, and $\text{Frob}_{\mathfrak{t}_k}$ has order exactly four in G_B .

Lemma 2.22. *The kernel N_B of $\mathcal{F} \rightarrow G_S \rightarrow G_B$ is the normal closure of the following thirty elements:*

- (i) *the seven relators ρ_ν , $\nu \in \Sigma \setminus \{\mathfrak{p}_1\}$;*
- (ii) *for $j = 1, 2$: $\hat{x}_j^2$, $[\hat{x}_j, \hat{y}_j]$, $[\hat{x}_j, \hat{z}_j]$, $[[\hat{y}_j, \hat{z}_j], \hat{z}_j]$, $\hat{z}_j^4$, $[\hat{y}_j, \hat{z}_j]^2$;*
- (iii) *for $\nu \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2\}$: $\hat{\tau}_\nu^2$ and $\hat{\varphi}_\nu^2$;*
- (iv) *for $k = 0, 1, 2$: $\hat{F}_k^4$, where $\hat{F}_k$ is the chosen lift of $\text{Frob}_{\mathfrak{t}_k}$.*

Moreover $N_B \subset D_2\mathcal{F}$, and $\rho_{\mathfrak{p}_1} \in N_B$.

Proof. By Lemma 2.17, it suffices to show that the images in G_S of the elements (ii)–(iv) generate N as a normal subgroup. Let $\mathcal{F}_3$ be free on x, y, z , and let N_D be the normal closure of the seven relators of D in Lemma 2.8, so that $\mathcal{F}_3/N_D = D$. The relator r maps to 1 in D , so $r \in N_D$, and $\ker(\mathcal{G}_{\mathbb{Q}_2} \rightarrow D)$ is the image of N_D . Since $N_D \subset D_2\mathcal{F}_3$, we have $N_D^2[N_D, \mathcal{F}_3] \subset D_3\mathcal{F}_3$. The seven relators of D span $N_D/N_D^2[N_D, \mathcal{F}_3]$ [26, Corollary 3.9.3]; write the class of r as a combination of them. The classes in $\text{gr}_2\mathcal{F}_3$ of $x^2, y^2, [x, y], [x, z]$ are independent, the relators $z^4, [y, z]^2$ and $[[y, z], z]$ lie in $D_3\mathcal{F}_3$, and r has class $y^{[2]} + [x, y] + [x, z]$; so y^2 has coefficient one. Replacing y^2 by r therefore still gives a spanning set, and by [26, Corollary 3.9.3] the elements $r, x^2, [x, y], [x, z], [[y, z], z], z^4, [y, z]^2$ generate N_D as a normal subgroup. Since $r = 1$ in $\mathcal{G}_{\mathbb{Q}_2}$, the other six generate $\ker(\mathcal{G}_{\mathbb{Q}_2} \rightarrow D)$.

For ν above $p \in \{3, 5\}$, the quotient of $\mathcal{G}_\nu$ by the normal closure of τ^2, φ^2 is generated by two involutions which commute, because $\varphi\tau\varphi^{-1} = \tau^p = \tau$ there; so that normal closure is $D_2\mathcal{G}_\nu$. Finally $N \subseteq D_2G_S$ (Lemma 2.21(b)) and $R \subset D_2\mathcal{F}$ give $N_B \subset D_2\mathcal{F}$, and $\rho_{\mathbf{p}_1} \in R \subset N_B$. $\square$

2.5. The Quotient G_B/D_4G_B .

Definition 2.23. For $n \geq 1$, the *relation space* $R_n \subseteq \mathfrak{L}_n$ of G_B in degree n is the image of $N_B \cap D_n\mathcal{F}$.

Since $N_B \subset D_2\mathcal{F}$ and D_nG_B is the image of $D_n\mathcal{F}$,

$$\mathrm{gr}_1 G_B = \mathbb{F}_2^8, \quad \mathrm{gr}_n G_B \cong \mathfrak{L}_n/R_n.$$

Consider the following 22 elements of $\mathfrak{L}_2$, written with the vectors of Table 4:

$$(2.24) \quad \begin{aligned} & \bar{\iota}_1^{[2]}, \bar{\iota}_2^{[2]}; \quad [\bar{\tau}_\nu, \bar{\varphi}_\nu] + \bar{\tau}_\nu^{[2]} \quad (\nu = \mathbf{q}_1, \mathbf{q}_2), \quad [\bar{\tau}_\nu, \bar{\varphi}_\nu] \quad (\nu = \mathbf{r}_1, \mathbf{r}_2); \\ & \bar{y}_j^{[2]} + [\bar{x}_j, \bar{y}_j] + [\bar{x}_j, \bar{z}_j], \quad \bar{x}_j^{[2]}, \quad [\bar{x}_j, \bar{y}_j], \quad [\bar{x}_j, \bar{z}_j] \quad (j = 1, 2); \\ & \bar{\tau}_\nu^{[2]}, \bar{\varphi}_\nu^{[2]} \quad (\nu = \mathbf{q}_1, \mathbf{q}_2, \mathbf{r}_1, \mathbf{r}_2). \end{aligned}$$

They are the classes of the eight local relators (2.14) and of the fourteen quadratic elements $\hat{x}_j^2$, $[\hat{x}_j, \hat{y}_j]$, $[\hat{x}_j, \hat{z}_j]$, $\hat{\tau}_\nu^2$, $\hat{\varphi}_\nu^2$ of Lemma 2.22.

Lemma 2.25. *The space R_2 is spanned by the 22 elements (2.24), and $\dim R_2 = 21$; their only linear relation is that the eight classes of local relators sum to zero. Hence $\dim \mathrm{gr}_2 G_B = 15$. Consequently, if $g \in G_B$ has nonzero elementary image v , then g has order at least four in G_B/D_3G_B exactly when $v^{[2]} \notin R_2$; otherwise g has order two there.*

Proof. Conjugates of an element of $D_2\mathcal{F}$ have the same class modulo $D_3\mathcal{F}$, classes of products add, and $\mathfrak{L}_2$ is finite. Hence, by Lemma 2.22, R_2 is spanned by the classes of the thirty generators of N_B . Those in (i) have the classes (2.14), and the quadratic elements of (ii) and (iii) have the classes $\bar{x}_j^{[2]}$, $[\bar{x}_j, \bar{y}_j]$, $[\bar{x}_j, \bar{z}_j]$, $\bar{\tau}_\nu^{[2]}$, $\bar{\varphi}_\nu^{[2]}$. The remaining generators, $[[\hat{y}_j, \hat{z}_j], \hat{z}_j]$, $\hat{z}_j^4$, $[\hat{y}_j, \hat{z}_j]^2$ and the fourth powers in (iv), lie in $D_3\mathcal{F}$. The class of $\rho_{\mathbf{p}_1}$ also lies in R_2 , since $\rho_{\mathbf{p}_1} \in N_B$. The supplementary program `lie241.py` computes the rank of the 22 elements in the 36-dimensional space $\mathfrak{L}_2$: it is 21. The sum of the eight local classes vanishes by Lemma 2.16, that is, by Hilbert reciprocity, so this is the only relation; none of the fourteen quadratic elements of (ii) and (iii) is involved in it. For the last statement, $g^2 \in D_2G_B$ has class $v^{[2]}$ in $\mathrm{gr}_2 G_B = \mathfrak{L}_2/R_2$, so $g^2 \in D_3G_B$ exactly when $v^{[2]} \in R_2$. $\square$

Lemma 2.26. (a) $\dim \mathrm{gr}_3 G_B = 26$, so $|\overline{G}_B| = 2^{8+15+26} = 2^{49}$.

- (b) For $j = 1, 2$, the local map induces an injection $D \rightarrow G_B/D_3G_B$, and $\mathrm{gr}_n D \rightarrow \mathrm{gr}_n G_B$ is injective for $n = 1, 2$. For ν above 3 or 5, the image of $\mathcal{G}_\nu$ in G_B is $\langle \tau_\nu \rangle \times \langle \varphi_\nu \rangle \cong C_2 \times C_2$, and it injects into G_B/D_2G_B . For $k = 0, 1, 2$, $\mathrm{Frob}_{\mathbf{t}_k}$ has order exactly four in G_B and in G_B/D_3G_B . For $j = 1, 2$, ι_j has order two in G_B/D_2G_B .
- (c) The conjugacy class of ι_1 in $\overline{G}_B$ has 2^{15} elements.
- (d) We have $\bar{\iota}_1 \neq \bar{\iota}_2$. For each $\nu \in \{\mathbf{p}_1, \mathbf{p}_2, \mathbf{q}_1, \mathbf{q}_2, \mathbf{r}_1, \mathbf{r}_2, \mathbf{t}_0, \mathbf{t}_1, \mathbf{t}_2\}$, neither $\bar{\iota}_1$ nor $\bar{\iota}_2$ lies in the span of the elementary images of the local generators at ν .

Proof. (a) Work in $\mathcal{F}/D_4\mathcal{F}$, in which $D_2\mathcal{F}/D_4\mathcal{F}$ is elementary abelian and $D_3\mathcal{F}/D_4\mathcal{F}$ is central. Let $\rho_1, \dots, \rho_{21}$ be the generators of N_B listed in (i), the first three elements of (ii) for each j , and (iii) of Lemma 2.22. They lie in $D_2\mathcal{F}$, and their classes in $\mathfrak{L}_2$ are the elements of (2.24) other than the class of $\rho_{\mathbf{p}_1}$, which are independent by Lemma 2.25. The generators $\omega_j = [[\hat{y}_j, \hat{z}_j], \hat{z}_j]$ lie in $D_3\mathcal{F}$, and the remaining generators of N_B lie in $D_4\mathcal{F}$. For $\rho \in D_2\mathcal{F}$ and $g \in \mathcal{F}$ we have $g^{-1}\rho g = \rho[\rho, g]$, and modulo $D_4\mathcal{F}$ the commutator $[\rho, g]$ is central and depends only, and linearly, on the classes of ρ in $\mathfrak{L}_2$ and of g in $\mathfrak{L}_1$. Hence the image of N_B in $\mathcal{F}/D_4\mathcal{F}$ is the subgroup generated by the ρ_i , the $[\rho_i, f]$ for f in a basis of $\mathcal{F}$, and the ω_j . An element $\prod_i \rho_i^{a_i}$ times an element of $D_3\mathcal{F}$ lies in $D_3\mathcal{F}$ only

if all $a_i = 0$. Therefore R_3 is spanned by the brackets $[\bar{\rho}_i, \xi]$, for ξ in a basis of $\mathfrak{L}_1$, and by $[[\bar{y}_j, \bar{z}_j], \bar{z}_j]$. The supplementary program `lie241c.py` computes these elements in the free associative algebra, where $[a, \xi] = a\xi + \xi a$: they span a space of dimension 142 in the 168-dimensional space $\mathfrak{L}_3$. So $\dim \text{gr}_3 G_B = 26$.

(b) The local map $\mathcal{G}_{\mathfrak{p}_j} \rightarrow G_B$ factors through D by Definition 2.20, and the induced map $D \rightarrow G_B$ preserves the Zassenhaus filtrations. It is injective on gr_1 because $\bar{x}_j, \bar{y}_j, \bar{z}_j$ are independent, and on gr_2 because $\bar{z}_j^{[2]}$ and $[\bar{y}_j, \bar{z}_j]$, the images of $\bar{z}^2$ and $[\bar{y}, \bar{z}]$, are independent modulo R_2 ; the program `lie241.py` checks both facts. If $1 \neq g \in D$, let $n \leq 2$ be maximal with $g \in D_n(D)$; then the image of g is nonzero in $\text{gr}_n G_B$, so it is not in $D_3 G_B$. For ν above 3 or 5, the vectors $\bar{\tau}_\nu$ and $\bar{\varphi}_\nu$ are independent, and the image of $\mathcal{G}_\nu$ is a quotient of $C_2 \times C_2$. For the Frobenius elements, `lie241.py` checks that $\overline{\text{Frob}}_{t_k}^{[2]} \notin R_2$, so Lemma 2.25 gives order at least four in $G_B/D_3 G_B$, while Definition 2.20 gives order at most four in G_B . Finally $\bar{t}_j \neq 0$.

(c) Write $\bar{G} = \bar{G}_B$ and $\iota = \iota_1$. The map $\mathfrak{L}_1 \rightarrow \text{gr}_2 \bar{G}$, $v \mapsto [\bar{v}, v]$, has rank 7 by `lie241.py`, so its kernel is the line through $\bar{v}$. The map $\text{gr}_2 \bar{G} \rightarrow \text{gr}_3 \bar{G}$, $u \mapsto [u, \bar{v}]$, has rank 8 by `lie241c.py`. Since $D_2 \bar{G}$ is abelian and $D_3 \bar{G}$ is central in $\bar{G}$, the map $h \mapsto [h, \bar{v}]$ is a homomorphism $D_2 \bar{G} \rightarrow D_3 \bar{G}$; it factors through $\text{gr}_2 \bar{G}$ and equals the second map. Its kernel $C_{\bar{G}}(\iota) \cap D_2 \bar{G}$ therefore has order $2^{15+26-8} = 2^{33}$. If $g \in C_{\bar{G}}(\iota)$, then $[\bar{v}, g] = 0$ in $\text{gr}_2 \bar{G}$, so $g \in \{0, \bar{v}\}$; conversely $\iota \in C_{\bar{G}}(\iota)$. Hence $|C_{\bar{G}}(\iota)| = 2^{34}$, and the class of ι has $2^{49-34} = 2^{15}$ elements.

(d) This is a finite check on Table 4, carried out by `lie241.py`. $\square$

2.6. Filtered Fox Calculus. This subsection and the next prove that G_B is infinite (Proposition 2.39) by the Golod–Shafarevich method. Suppose that G_B is finite, and let $\Lambda = \mathbb{F}_2[G_B]$. The rows (Definition 2.30) of the relators of G_B in a presentation with eight generators (Lemma 2.22) span a Λ -module $\mathcal{M}$ whose Hilbert polynomial is $1 - (1 - 8t)h_\Lambda$ (Lemma 2.32). The module $\mathcal{M}$ is also the sum of the modules spanned by the rows of the relations of the eleven local groups Γ , each isomorphic to C_2 , $C_2 \times C_2$, C_4 or D ; for $0 < t < 1$ the Hilbert polynomial of each of these modules is at most $\psi_\Gamma(t)h_\Lambda(t)$, with ψ_Γ as in Definition 2.33 (Lemma 2.34). The row of the dyadic relator $\rho_{\mathfrak{p}_1}$ of (2.13) lies both in the module of $\mathfrak{p}_1$ and in the sum of the other ten, and the module it generates has Hilbert polynomial $s_D h_\Lambda$, with s_D as in Lemma 2.35. Comparing these bounds gives $1 \leq h_\Lambda(t)P_B(t)$ for $0 < t < 1$, with P_B as in (2.37); this fails at $t = 34/117$ (Lemma 2.38).

Let Δ be a finite 2-group, $\Lambda = \mathbb{F}_2[\Delta]$, and $\mathfrak{I}$ its augmentation ideal. We use the filtered spaces and Hilbert polynomials of Definition 2.1; in particular $F^n \Lambda = \mathfrak{I}^n$. For $m \geq 1$, $\Lambda^m(-1)$ denotes Λ^m with $F^n = (\mathfrak{I}^{n-1})^m$ for $n \geq 1$, so that $h_{\Lambda^m(-1)} = m t h_\Lambda$. Subspaces carry the induced filtration unless stated otherwise. For $0 < t < 1$,

$$(2.27) \quad h_M(t) = (1 - t) \sum_{n \geq 1} \dim(M/F^n M) t^{n-1}.$$

Lemma 2.28. *Let $0 < t < 1$.*

- (h1) *If $f: M \rightarrow M'$ is surjective with $f(F^n M) \subset F^n M'$, then $h_{M'}(t) \leq h_M(t)$.*
- (h2) *If $U_1 \subset U_2$ are subspaces of the same filtered space, then $h_{U_1}(t) \leq h_{U_2}(t)$.*
- (h3) *If f is surjective and strict, $f(F^n M) = F^n M'$, then $h_M = h_{\ker f} + h_{M'}$.*
- (h4) *For subspaces U_1, U_2 of a filtered space,*

$$(2.29) \quad h_{U_1+U_2}(t) \leq h_{U_1}(t) + h_{U_2}(t) - h_{U_1 \cap U_2}(t).$$

Proof. Statements (h1)–(h3) follow from the definitions and (2.27). For (h4), apply (h3) to $U_1 \oplus U_2 \rightarrow U_1 + U_2$, $(u_1, u_2) \mapsto u_1 + u_2$, whose kernel is $U_1 \cap U_2$, with the image filtration $F^n U_1 + F^n U_2$ on $U_1 + U_2$; this filtration is contained in the induced one, and (h1) applies to the identity map. $\square$

Definition 2.30. Let $\mathcal{F}$ be a free pro-2 group with basis $f_1, \dots, f_n$ and $\pi: \mathcal{F} \rightarrow \Delta$ a surjection. Since $\Lambda^n \rtimes \Delta$, with Δ acting by left multiplication, is a finite 2-group, there is a unique homomorphism

$\mathcal{F} \rightarrow \Lambda^n \rtimes \Delta$ sending f_i to $(e_i, \pi(f_i))$, where $e_1, \dots, e_n$ is the standard basis of Λ^n . We write it as $w \mapsto (\partial w, \pi(w))$ and call $\partial w = (\partial_1 w, \dots, \partial_n w) \in \Lambda^n$ the row of w .

For w in the discrete free group on the f_i , the row $\partial w \in \Lambda^n$ is the image of the vector of free derivatives of w [9, Section 2].

Lemma 2.31. (F1) $\partial(ww') = \partial w + \pi(w)\partial w'$.

(F2) $\sum_i \partial_i w (\pi(f_i) - 1) = \pi(w) - 1$.

(F3) If $\pi(\rho) = 1$, then $\partial(u\rho u^{-1}) = \pi(u)\partial\rho$; and ∂ restricts to a continuous homomorphism on $\ker \pi$.

(F4) If $\mathcal{F}'$ is free on $f'_1, \dots, f'_m, u_1, \dots, u_m \in \mathcal{F}$, and ∂' denotes the rows for the map $\mathcal{F}' \rightarrow \Delta$, $f'_l \mapsto \pi(u_l)$, then $\partial(W(u_1, \dots, u_m)) = \sum_l \partial'_l W \cdot \partial u_l$ for $W \in \mathcal{F}'$.

Proof. (F1) is the multiplication of the semidirect product. For (F2), the pairs (a, g) with $\sum a_i(\pi(f_i) - 1) = g - 1$ form a subgroup containing the images of the f_i . (F3) follows from (F1). For (F4), both sides are the first components of homomorphisms $\mathcal{F}' \rightarrow \Lambda^n \rtimes \Delta$ that agree on the basis. $\square$

Lemma 2.32. Let $\mathcal{M} = \{a \in \Lambda^n : \sum_i a_i(\pi(f_i) - 1) = 0\}$, with the filtration induced from $\Lambda^n(-1)$. Then $h_{\mathcal{M}} = 1 - (1 - nt)h_{\Lambda}$ and $\mathcal{M} = \partial(\ker \pi)$. If ρ lies in the normal closure of a set $Y \subset \ker \pi$, then $\partial\rho$ lies in the Λ -span of ∂Y . In particular, $\mathcal{M}$ is the Λ -span of the rows of any set of normal generators of $\ker \pi$.

Proof. Since the $\pi(f_i)$ generate Δ , we have $\mathfrak{I} = \sum_i \Lambda(\pi(f_i) - 1) \subset \sum_i \mathbb{F}_2(\pi(f_i) - 1) + \mathfrak{I}^2$, hence $\mathfrak{I}^m = \sum_i \mathfrak{I}^{m-1}(\pi(f_i) - 1)$ for all $m \geq 1$, by induction and because $\mathfrak{I}$ is nilpotent. So $\Lambda^n(-1) \rightarrow \mathfrak{I}$, $a \mapsto \sum a_i(\pi(f_i) - 1)$, is strict and surjective with kernel $\mathcal{M}$, and (h3) gives $h_{\mathcal{M}} = nt h_{\Lambda} - (h_{\Lambda} - 1)$.

By (F2), $\partial(\ker \pi) \subset \mathcal{M}$. Conversely, let $\mathcal{F}^\circ \subset \mathcal{F}$ be the dense subgroup generated by the f_i , which is a free group on them. Then $\pi(\mathcal{F}^\circ) = \Delta$, and the kernel of $\mathbb{F}_2[\mathcal{F}^\circ] \rightarrow \Lambda$ is $\mathbb{F}_2[\mathcal{F}^\circ] (\mathcal{F}^\circ \cap \ker \pi - 1)$. Lift $a \in \mathcal{M}$ to $\tilde{a} \in \mathbb{F}_2[\mathcal{F}^\circ]^n$. Then $\sum_i \tilde{a}_i(f_i - 1) = \sum_l \zeta_l(n_l - 1)$ with $n_l \in \mathcal{F}^\circ \cap \ker \pi$ and $\zeta_l \in \mathbb{F}_2[\mathcal{F}^\circ]$. By Fox's fundamental formula $n_l - 1 = \sum_i (\partial n_l / \partial f_i)(f_i - 1)$, where the $\partial / \partial f_i$ are the free derivatives [9, Section 2], and the coefficients of the $f_i - 1$ are unique, because $\partial / \partial f_j$ maps $\sum_i \zeta'_i(f_i - 1)$ to ζ'_j . So $\tilde{a}_i = \sum_l \zeta_l \partial n_l / \partial f_i$. On $\mathcal{F}^\circ$ the rows are the images of the vectors of free derivatives, so $a = \sum_l \zeta_l \partial n_l$ lies in $\Lambda \partial(\ker \pi)$, which equals $\partial(\ker \pi)$ by (F3). For the remaining statements, let M_Y be the Λ -span of ∂Y . By (F3), the elements $n \in \ker \pi$ with $\partial n \in M_Y$ form a closed normal subgroup of $\mathcal{F}$ containing Y . $\square$

The next lemma bounds, in terms of the function ψ_Γ below, the Hilbert polynomial of the Λ -module spanned by the rows of all relations of one local group Γ . The groups Γ below are C_2 , $C_2 \times C_2$, C_4 and D , with standard generators ι ; τ, φ ; a generator; and x, y, z . Let k be the number of standard generators, so $k = 1, 2, 1, 3$. The Hilbert polynomials $h_{\mathbb{F}_2[\Gamma]}$ are $1 + t$, $(1 + t)^2$, $(1 + t)(1 + t^2)$ and $h_{\mathbb{F}_2[D]}$ (Theorem 2.2), and $D_3(\Gamma) = 1$ in each case.

Definition 2.33. For each of these groups Γ , put

$$\psi_\Gamma(t) = kt - 1 + h_{\mathbb{F}_2[\Gamma]}(t)^{-1}.$$

Lemma 2.34. Let $\Gamma \leq \Delta$ be a subgroup isomorphic to one of these groups, with $g_1, \dots, g_k \in \Gamma$ corresponding to its standard generators, and suppose that $\text{gr}_n \Gamma \rightarrow \text{gr}_n \Delta$ is injective for $n = 1, 2$. Let $\Lambda_\Gamma = \mathbb{F}_2[\Gamma] \subset \Lambda$, with augmentation ideal $\mathfrak{I}_\Gamma$, and let $\mathcal{M}_\Gamma \subset \Lambda_\Gamma^k(-1)$ be the kernel of $b \mapsto \sum_l b_l(g_l - 1)$.

- (a) There are elements $\eta_j \in \Lambda$ and integers $w_j \geq 0$ such that $\Lambda = \bigoplus_j \eta_j \Lambda_\Gamma$ and $\mathfrak{I}^m = \bigoplus_j \eta_j \mathfrak{I}_\Gamma^{m-w_j}$ for every m , where $\mathfrak{I}_\Gamma^{m'} = \Lambda_\Gamma$ for $m' \leq 0$; moreover $\sum_j t^{w_j} = h_\Lambda / h_{\mathbb{F}_2[\Gamma]}$.
- (b) The Λ -module $\Lambda \mathcal{M}_\Gamma \subset \Lambda^k(-1)$ has $h_{\Lambda \mathcal{M}_\Gamma} = \psi_\Gamma h_\Lambda$.
- (c) Let $\mathcal{F}$ and π be as above, let $u_1, \dots, u_k \in \mathcal{F}$ with $\pi(u_l) = g_l$, and let $\mathcal{F}_k$ be free on k letters, mapping to Γ by the standard generators. Let $U \subset \Lambda^n(-1)$ be the Λ -span of the rows $\partial W(u_1, \dots, u_k)$ for all W in the kernel of $\mathcal{F}_k \rightarrow \Gamma$. Then $h_U(t) \leq \psi_\Gamma(t) h_\Lambda(t)$ for $0 < t < 1$.

Proof. (a) Since $D_3(\Gamma) = 1$ and $\text{gr } \Gamma \rightarrow \text{gr } \Delta$ is injective, $\Gamma \cap D_m \Delta = D_m(\Gamma)$ for all m . Choose elements of Γ whose classes form a homogeneous basis of $\text{gr } \Gamma$, and extend them by elements of Δ to a family whose classes form a homogeneous basis of $\text{gr } \Delta$. By Theorem 2.2, the ordered products of the elements $g - 1$ of this family, each used at most once and with the elements of Γ last, form a basis of Λ , and those of weight at least m form a basis of $\mathfrak{I}^m$; here the weight of a product is the sum of the degrees of the classes of its factors. The same holds for Λ_Γ and the elements of Γ alone. Let the η_j be the ordered products of the other elements, and w_j the weight of η_j . The empty product $\eta_j = 1$ has weight 0, so $\mathfrak{I}^m \cap \Lambda_\Gamma = \mathfrak{I}_\Gamma^m$: the filtration of Λ_Γ induced from Λ is its augmentation filtration, with Hilbert polynomial $h_{\mathbb{F}_2[\Gamma]}$. Comparing Hilbert polynomials gives the last assertion.

(b) As in the proof of Lemma 2.32, the map $\Lambda_\Gamma^k(-1) \rightarrow \mathfrak{I}_\Gamma$ is strict and surjective, so $h_{\mathcal{M}_\Gamma} = kt h_{\mathbb{F}_2[\Gamma]} - (h_{\mathbb{F}_2[\Gamma]} - 1)$. By (a), $\Lambda^k(-1) = \bigoplus_j \eta_j \Lambda_\Gamma^k(-1)$ with $F^m = \bigoplus_j \eta_j F^{m-w_j}$, and $\Lambda \mathcal{M}_\Gamma = \bigoplus_j \eta_j \mathcal{M}_\Gamma$. Hence $h_{\Lambda \mathcal{M}_\Gamma} = (h_\Lambda / h_{\mathbb{F}_2[\Gamma]}) h_{\mathcal{M}_\Gamma} = \psi_\Gamma h_\Lambda$.

(c) For W in the kernel, the local row $\partial' W \in \Lambda_\Gamma^k$ lies in $\mathcal{M}_\Gamma$ by (F2), and by (F4) $\partial W(u) = \sum_l \partial'_l W \partial u_l$. Thus U is contained in the image of $\Lambda \mathcal{M}_\Gamma$ under the map $T_u: \Lambda^k(-1) \rightarrow \Lambda^n(-1)$, $a \mapsto \sum_l a_l \partial u_l$, which preserves filtrations because $\partial u_l \in \Lambda^n = F^0$. By (h2), (h1) and (b), $h_U \leq h_{T_u(\Lambda \mathcal{M}_\Gamma)} \leq h_{\Lambda \mathcal{M}_\Gamma} = \psi_\Gamma h_\Lambda$. $\square$

In the proof of Proposition 2.39, the row of the dyadic relator $\rho_{\mathfrak{p}_1}$ lies both in the module spanned by the rows of the relations at $\mathfrak{p}_1$ and in the module spanned by the rows of the relations at the other ten places. The next lemma computes the Hilbert polynomial of the module generated by this row.

Lemma 2.35. *In the situation of Lemma 2.34 with $\Gamma = D$, suppose that u_1, u_2, u_3 are the basis elements f_1, f_2, f_3 of $\mathcal{F}$. Let $r \in \mathcal{F}_3$ map to 1 in D , with class $y^{[2]} + [x, y] + [x, z]$ in $\text{gr}_2 \mathcal{F}_3$, and let $\rho = r(f_1, f_2, f_3)$. Then*

$$h_{\Lambda \partial \rho} = s_D h_\Lambda, \quad s_D(t) = t^2 \left(1 - \frac{t^7}{h_{\mathbb{F}_2[D]}(t)} \right).$$

Proof. By (F4), $\partial \rho = (\partial' r, 0, \dots, 0)$, where $\partial' r \in \Lambda_D^3$ is the local row, so $\Lambda \partial \rho$ is the module $\Lambda \partial' r \subset \Lambda^3(-1)$ placed in the first three coordinates. By Lemma 2.34(a), $\Lambda^3 = \bigoplus_j \eta_j \Lambda_D^3$ with $F^n(\Lambda^3(-1)) = \bigoplus_j \eta_j F^{n-w_j}(\Lambda_D^3(-1))$, and $b \mapsto \eta_j b$ is injective on Λ_D^3 . The submodule $\Lambda \partial' r = \bigoplus_j \eta_j \Lambda_D \partial' r$ decomposes in the same way, so $F^n(\Lambda \partial' r) = \bigoplus_j \eta_j F^{n-w_j}(\Lambda_D \partial' r)$ for the induced filtrations, and $h_{\Lambda \partial \rho} = (h_\Lambda / h_{\mathbb{F}_2[D]}) h_{\Lambda_D \partial' r}$. It therefore suffices to show that $h_{\Lambda_D \partial' r} = t^2(h_{\mathbb{F}_2[D]} - t^7)$, for the filtration induced from $\Lambda_D^3(-1)$. Write $\mathfrak{I}_D$ for the augmentation ideal of $\Lambda_D = \mathbb{F}_2[D]$, and X_1, X_2, X_3, X_4 for $x - 1, y - 1, z - 1, w - 1$, where $w = [y, z]$.

The linear part of $\partial' r$. Here π also denotes the map $\mathcal{F}_3 \rightarrow D$. For $g, h \in \mathcal{F}_3$, (F1) gives $\partial'(g^2) = (1 + \pi(g))\partial' g$ and $\partial'[g, h] = \pi(g)^{-1}(\pi(h)^{-1} - 1)\partial' g + \pi(g)^{-1}\pi(h)^{-1}(\pi(g) - 1)\partial' h$. Moreover $\partial' g$ is congruent modulo $\mathfrak{I}_D$ to the image $\bar{g} \in \mathbb{F}_2^3$ of g in $\mathcal{F}_3/D_2\mathcal{F}_3$, and $\pi(g) - 1 \equiv \sum_l \bar{g}_l X_l$ modulo $\mathfrak{I}_D^2$ by (F2). Hence, for $q \in D_2\mathcal{F}_3$, the row $\partial' q$ has entries in $\mathfrak{I}_D$, and modulo $\mathfrak{I}_D^2$ it is additive in q , because $\pi(q) - 1 \in \mathfrak{I}_D^2$. It vanishes modulo $\mathfrak{I}_D^2$ on $D_3\mathcal{F}_3 = (D_2\mathcal{F}_3)^2[D_2\mathcal{F}_3, \mathcal{F}_3]$ (Lazard's formula): for $q \in D_2\mathcal{F}_3$ the formulas above give $\partial'(q^2), \partial'[q, h] \in \mathfrak{I}_D^2$, since $\bar{q} = 0$ and $\pi(q) - 1 \in \mathfrak{I}_D^2$. So the row modulo $\mathfrak{I}_D^2$ depends only on the class of q in $\text{gr}_2 \mathcal{F}_3$, the classes $v^{[2]}$ and $[v, v']$ giving the rows with l -th entries $v_l \sum_m v_m X_m$ and $v_l \sum_m v'_m X_m + v'_l \sum_m v_m X_m$. For the class $y^{[2]} + [x, y] + [x, z]$ this gives

$$\partial' r \equiv (X_2 + X_3, X_2 + X_1, X_1) \pmod{\mathfrak{I}_D^2}.$$

Three facts about Λ_D . Let $A = \bigoplus_m \mathfrak{I}_D^m / \mathfrak{I}_D^{m+1}$, and write X, Y, Z and W for the classes of X_1, X_2, X_3 in degree one and of X_4 in degree two. By Theorem 2.2 and Lemma 2.8(c), the products $X_1^{a_1} X_2^{a_2} X_3^{a_3} X_4^{a_4}$ with $a_1, a_2, a_4 \in \{0, 1\}$ and $0 \leq a_3 \leq 3$, of weight $a_1 + a_2 + a_3 + 2a_4 \geq m$, form a basis of $\mathfrak{I}_D^m$; here $X_3^2 = z^2 - 1$. Hence the monomials $X^{a_1} Y^{a_2} Z^{a_3} W^{a_4}$ form a basis of A , and, since

the coefficients of $h_{\mathbb{F}_2[D]}$ are 1, 3, 5, 7, 7, 5, 3, 1,

$$\dim \mathfrak{J}_D^m = 32, 31, 28, 23, 16, 9, 4, 1, 0 \quad (m = 0, \dots, 8).$$

Because x and w are central and $x^2 = y^2 = w^2 = z^4 = 1$, the elements X and W are central in A and $X^2 = Y^2 = W^2 = Z^4 = 0$. Moreover $ZY = YZ + W$, because $X_3X_2 + X_2X_3 = zy + yz = zy(w-1) \equiv X_4 \pmod{\mathfrak{J}_D^3}$; by induction $Z^jY = YZ^j + jZ^{j-1}W$ for $j \geq 1$.

First, $\mathfrak{J}_D^7 = \mathbb{F}_2\Omega_D$, where $\Omega_D = \sum_{g \in D} g$: $\mathfrak{J}_D^7$ is one-dimensional and $(g-1)\mathfrak{J}_D^7 \subset \mathfrak{J}_D^8 = 0$, so its nonzero element is invariant under left multiplication by D , and hence equal to Ω_D .

Second, for $m < 7$ the map $A_m \rightarrow A_{m+1}^3$, $\xi \mapsto (\xi X, \xi Y, \xi Z)$, is injective. Let $\xi = \sum_{\mu} b_{\mu}\mu$ over the basis monomials $\mu = X^{a_1}Y^{a_2}Z^{a_3}W^{a_4}$ of degree m . Right multiplication by X maps the monomials with $a_1 = 0$ to distinct basis monomials and kills the others, and right multiplication by Z maps those with $a_3 \leq 2$ to distinct basis monomials and kills those with $a_3 = 3$. So $\xi X = \xi Z = 0$ forces $\xi = \sum_{a_2, a_4} b_{a_2 a_4} X Y^{a_2} Z^3 W^{a_4}$. Then

$$\xi Y = b_{00}(XYZ^3 + XZ^2W) + b_{01}XYZ^3W + b_{10}XYZ^2W,$$

a combination of distinct basis monomials, so $\xi Y = 0$ forces $\xi = b_{11}XYZ^3W$, which has degree 7. Hence $\xi = 0$ when $m < 7$.

Third, the same holds for $\xi \mapsto (\xi(Y+Z), \xi(Y+X), \xi X)$, because this triple is obtained from (X, Y, Z) by the invertible matrix

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

This is the coefficient matrix of $y^{[2]} + [x, y] + [x, z]$, that is, the matrix of the 2-adic Hilbert symbol on 2, -5, 5 in the proof of Lemma 2.7(c). So the injectivity used here, and with it the correction term s_D , comes from the nondegeneracy of the local Hilbert pairing, that is, from local duality. The supplementary program `dyadic241.py` confirms these three facts by direct computation in Λ_D .

The filtration. If $\xi \in \mathfrak{J}_D^m \setminus \mathfrak{J}_D^{m+1}$ with $m < 7$, then by the third fact $\xi \partial' r$ lies in F^{m+2} but not in F^{m+3} , whereas $\Omega_D \partial' r = 0$ because $\Omega_D \mathfrak{J}_D = 0$. Now let $\xi \in \Lambda_D$ with $\xi \partial' r \in F^{m+2}$, and suppose that $\xi \notin \mathfrak{J}_D^m + \mathbb{F}_2\Omega_D$. Let $m' < m$ be maximal with $\xi \in \mathfrak{J}_D^{m'} + \mathbb{F}_2\Omega_D$, and write $\xi = \xi' + a\Omega_D$ with $\xi' \in \mathfrak{J}_D^{m'}$ and $a \in \mathbb{F}_2$. Then $\xi' \notin \mathfrak{J}_D^{m'+1}$, and $m' < 7$ because $\mathfrak{J}_D^7 = \mathbb{F}_2\Omega_D$; so $\xi \partial' r = \xi' \partial' r$ is not in $F^{m'+3} \supset F^{m+2}$, a contradiction. Therefore $F^{m+2}(\Lambda_D \partial' r) = \mathfrak{J}_D^m \partial' r$ for every $m \geq 0$, the map $\xi \mapsto \xi \partial' r$ has kernel $\mathbb{F}_2\Omega_D$, and $h_{\Lambda_D \partial' r} = \sum_{m < 7} \dim(\mathfrak{J}_D^m / \mathfrak{J}_D^{m+1}) t^{m+2} = t^2(h_{\mathbb{F}_2[D]} - t^7)$. $\square$

2.7. Infinitude. By Definition 2.33 and the Hilbert polynomials listed before it,

$$(2.36) \quad \begin{aligned} \psi_{C_2}(t) &= \frac{t^2}{1+t}, & \psi_{C_2 \times C_2}(t) &= 2t - 1 + \frac{1}{(1+t)^2}, \\ \psi_{C_4}(t) &= \frac{t^4}{(1+t)(1+t^2)}, & \psi_D(t) &= 3t - 1 + \frac{1}{h_{\mathbb{F}_2[D]}(t)}. \end{aligned}$$

With s_D as in Lemma 2.35, the *Golod–Shafarevich function* of G_B is

$$(2.37) \quad P_B(t) = 1 - 8t + 2\psi_{C_2}(t) + 4\psi_{C_2 \times C_2}(t) + 2\psi_D(t) - s_D(t) + 3\psi_{C_4}(t).$$

In the proof of Proposition 2.39, the term $-8t$ comes from the eight generators of a free group mapping onto G_B ; the terms in ψ_{C_2} , $\psi_{C_2 \times C_2}$, ψ_D and ψ_{C_4} come from the local relations at the two real places, the four places above 3 and 5, the two dyadic places and the three places $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$; and $-s_D$ comes from the row of the dyadic relator $\rho_{\mathfrak{p}_1}$, which lies both in the module of $\mathfrak{p}_1$ and in the sum of the modules of the other places.

Lemma 2.38.

$$P_B\left(\frac{34}{117}\right) = -\frac{187433948535241}{88772225460489675} < 0.$$

Proof. By (2.36), (2.37), the formula for s_D in Lemma 2.35 and $h_{\mathbb{F}_2[D]}(t) = (1+t)^3(1+t^2)^2$ (Lemma 2.8(c)), P_B is a rational function with rational coefficients. Exact rational arithmetic, carried out by the supplementary program `gs241.py`, gives the stated value. $\square$

Proposition 2.39. *The group G_B is infinite.*

Proof. Suppose that G_B is finite, and put $\Delta = G_B$ and $\Lambda = \mathbb{F}_2[\Delta]$. By Table 4, $\bar{x}_1, \bar{y}_1, \bar{z}_1$ are independent; choose $g_4, \dots, g_8 \in G_S$ such that $\bar{x}_1, \bar{y}_1, \bar{z}_1, \bar{g}_4, \dots, \bar{g}_8$ is a basis of $\mathbb{F}_2^8$. Let $\mathcal{F}$ be free on $f_1, \dots, f_8$, and send f_1, f_2, f_3 to x_1, y_1, z_1 and f_l to g_l for $4 \leq l \leq 8$. This is a minimal presentation of G_S ; we take the lifts $\hat{x}_1 = f_1$, $\hat{y}_1 = f_2$, $\hat{z}_1 = f_3$, and arbitrary lifts of the other local generators. Let $\pi: \mathcal{F} \rightarrow \Delta$ be the composite and $\mathcal{M}$ as in Lemma 2.32, so that $h_{\mathcal{M}} = 1 - (1 - 8t)h_{\Lambda}$.

By Lemma 2.26(b), the image in Δ of each local group is the prescribed group Γ , and $\text{gr}_n \Gamma \rightarrow \text{gr}_n \Delta$ is injective for $n = 1, 2$; this is the hypothesis of Lemma 2.34. Indeed, for $\Gamma = D$ this is stated in Lemma 2.26(b). For $\Gamma = C_2$ and $\Gamma = C_2 \times C_2$ we have $\text{gr}_2 \Gamma = 0$, and $\text{gr}_1 \Gamma = \Gamma$ injects into G_B/D_2G_B because $\bar{t}_j \neq 0$, respectively because the image of $\mathcal{G}_{\nu}$ injects into G_B/D_2G_B . For $\Gamma = C_4$ generated by Frob_{t_k} , which has order four in G_B/D_3G_B , we have $\text{Frob}_{t_k} \notin D_2G_B$, since otherwise its square would lie in $D_4G_B \subseteq D_3G_B$, and $\text{Frob}_{t_k}^2 \notin D_3G_B$; this is the injectivity on $\text{gr}_1 \Gamma$ and on $\text{gr}_2 \Gamma = \langle \text{Frob}_{t_k}^2 \rangle$. We use eleven places: the real places v_1, v_2 , with $\Gamma = C_2$; the four places above 3 and 5, with $\Gamma = C_2 \times C_2$; the dyadic places $\mathfrak{p}_1, \mathfrak{p}_2$, with $\Gamma = D$; and $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$, with $\Gamma = C_4$ generated by the Frobenius. For each of these places ν , let U_{ν} be the module U of Lemma 2.34(c) for this Γ , formed with the lifts of the local generators at ν . Every generator of N_B in Lemma 2.22 is of the form $W(u_1, \dots, u_k)$ for one of these places and some W in the kernel of $\mathcal{F}_k \rightarrow \Gamma$, and conversely every such element lies in N_B . By Lemma 2.32, $\mathcal{M} = \sum_{\nu} U_{\nu}$. Let U' be the sum of the U_{ν} over the ten places $\nu \neq \mathfrak{p}_1$. The row of $\rho_{\mathfrak{p}_1}$ lies in $U_{\mathfrak{p}_1}$. Since $\rho_{\mathfrak{p}_1}$ lies in the normal closure of the relators (i) of Lemma 2.22, its row also lies in the Λ -span of their rows (Lemma 2.32), which is contained in U' . Hence $\Lambda \partial \rho_{\mathfrak{p}_1} \subset U_{\mathfrak{p}_1} \cap U'$. By Lemma 2.28(h4) and (h2), Lemma 2.34(c) and Lemma 2.35, for $0 < t < 1$,

$$\begin{aligned} 1 - (1 - 8t)h_{\Lambda}(t) &= h_{\mathcal{M}}(t) \leq h_{U_{\mathfrak{p}_1}}(t) + \sum_{\nu \neq \mathfrak{p}_1} h_{U_{\nu}}(t) - h_{\Lambda \partial \rho_{\mathfrak{p}_1}}(t) \\ &\leq (2\psi_{C_2} + 4\psi_{C_2 \times C_2} + 2\psi_D + 3\psi_{C_4} - s_D)(t) h_{\Lambda}(t), \end{aligned}$$

that is, $1 \leq h_{\Lambda}(t)P_B(t)$. Since $h_{\Lambda}(t) > 0$, this contradicts $P_B(34/117) < 0$ (Lemma 2.38). $\square$

2.8. The Fields.

Definition 2.40. The *root discriminant* of a number field M with discriminant Δ_M is $\text{rd}(M) = |\Delta_M|^{1/[M:\mathbb{Q}]}$.

Definition 2.41. For a number field M and a prime $\mathfrak{P}$ of M above a rational prime p , the *absolute type* of $\mathfrak{P}$ is the pair (e, f) of its ramification index and residue degree over p . For a Galois extension M/A of number fields, all primes of M above a prime $\mathfrak{p}$ of A have the same ramification index e and residue degree f in M/A ; the pair (e, f) is the *type* of $\mathfrak{p}$ in M/A .

As in the introduction, let $\lambda = 2^{9/4}\sqrt{3615}$, where $3615 = 3 \cdot 5 \cdot 241$.

Theorem 2.42. *For every power of two $m \geq 2^{49}$ there is a finite Galois extension K/B of degree m , contained in B_G , such that $G_B \rightarrow \bar{G}_B$ factors through $\text{Gal}(K/B)$. In particular K contains the fixed field of D_4G_B , hence the fixed field of D_3G_B and the Kummer field E . Every such K is totally imaginary. Let ι_1 also denote complex conjugation at any place of K above v_1 ; these complex conjugations are conjugate in $\text{Gal}(K/B)$, one of them is the image of the element ι_1 of Definition 2.12, and the statements below do not depend on the choice. Let $F = K^{\langle \iota_1 \rangle}$ and $d = [F:\mathbb{Q}] = m$, let (b, c) be the signature of F and $\theta = c/d$, and put $\theta_* = 65535/131072 = 1/2 - 2^{-17}$. Then F has a real*

place,

$$\text{rd}(K) = \text{rd}(F) = \lambda, \quad \theta_* \leq \theta < \frac{1}{2},$$

and $b/d = 1/(2N_\iota)$, where $N_\iota \geq 2^{15}$ is the number of conjugates of ι_1 in $\text{Gal}(K/B)$. The extension K/F is quadratic and unramified at every finite place. For $r \in \{2, 3, 5, 7, 29\}$, every prime of F above r splits in K , and the primes of K and of F above r have the absolute type (e_r, f_r) of Table 5; that is, K/F has uniform local types $(e_r, f_r)_{r \in \{2, 3, 5, 7, 29\}}$ in the sense of Definition 5.4. The completions of K at the primes above 2, 3, 5, 7 and 29 are the local extensions listed in Table 5.

TABLE 5. Absolute types of the places of K and F above 2, 3, 5, 7 and 29, the corresponding local extensions of the completions of B , and the contributions of these primes to $\text{rd}(K)$. The last row is the prime 241, which ramifies in B ; K/B is unramified above it.

r	(e_r, f_r)	local extension over B	factor of $\text{rd}(K)$
2	(8, 4)	$L_2/\mathbb{Q}_2$, group D	$2^{9/4}$
3	(2, 2)	$\mathbb{Q}_3(\sqrt{-1}, \sqrt{3})/\mathbb{Q}_3$, group $C_2 \times C_2$	$3^{1/2}$
5	(2, 2)	$\mathbb{Q}_5(\sqrt{2}, \sqrt{5})/\mathbb{Q}_5$, group $C_2 \times C_2$	$5^{1/2}$
7	(1, 8)	unramified of degree 4 over B_{t_0}	1
29	(1, 4)	unramified of degree 4 over $\mathbb{Q}_{29}$	1
241	$e = 2$	unramified	$241^{1/2}$

Proof. Existence. By Proposition 2.39, G_B has open normal subgroups of arbitrarily large index, and D_4G_B is open because G_B is finitely generated. Given m , choose an open normal subgroup $\mathcal{U}' \subset D_4G_B$ of G_B of index at least m , and put $N' = D_4G_B/\mathcal{U}'$. A nontrivial normal subgroup of a finite 2-group meets its center, so N' contains normal subgroups of $G_B/\mathcal{U}'$ of every order dividing $|N'|$. Take one of order $[G_B : \mathcal{U}']/m$, which divides $|N'| = [G_B : \mathcal{U}']/2^{49}$. Its preimage $\mathcal{U}$ is open and normal in G_B , contained in D_4G_B , and of index m . Let K be its fixed field in B_G . Conversely, every K as in the statement is the fixed field of an open normal subgroup $\mathcal{U} \subset D_4G_B$. We fix such a K and put $H = \text{Gal}(K/B) = G_B/\mathcal{U}$.

Complex places. Since $\sqrt{-1} = \sqrt{\alpha_0} \in E \subset K$, the field K is totally imaginary, and $[K : F] = 2$. Let $j \in \{1, 2\}$. The group H permutes the places of K above v_j transitively. If an embedding $\sigma : K \rightarrow \mathbb{C}$ induces such a place and $\iota_\sigma \in H$ is its complex conjugation, so that $\bar{\sigma} = \sigma \circ \iota_\sigma$, then for $h \in H$ we have $\overline{\sigma \circ h} = (\sigma \circ h) \circ (h^{-1}\iota_\sigma h)$, so the complex conjugation at the place of $\sigma \circ h$ is $h^{-1}\iota_\sigma h$. By the definition of the local map at v_j , the image of ι_j in H is the complex conjugation at the place of K below the place of B_S fixed in Definition 2.12. Hence every complex conjugation at a place of K above v_j is conjugate in H to the image of ι_j , and has elementary image $\bar{\iota}_j$, since conjugation preserves elementary images. In particular, two choices of ι_1 in the statement are conjugate in H , so an element of H maps the field F of one choice onto that of the other, and the statements of the theorem hold for both choices or for neither.

Let $\sigma_1 : K \rightarrow \mathbb{C}$ induce the chosen place, so that $\bar{\sigma}_1 = \sigma_1 \circ \iota_1$ and $\sigma_1(F) \subset \mathbb{R}$. The embeddings above v_1 are $\sigma_1 \circ h$ with $h \in H$, and two of them agree on F exactly when they differ by right multiplication by an element of $\langle \iota_1 \rangle$. The restriction of $\sigma_1 \circ h$ to F is real exactly when $\sigma_1 \circ \iota_1 h$ and $\sigma_1 \circ h$ agree on F , that is, when $h^{-1}\iota_1 h \in \langle \iota_1 \rangle$, that is, when $h \in C_H(\iota_1)$. Similarly, if ι' is complex conjugation for an embedding σ_2 above v_2 , the restriction of $\sigma_2 \circ h$ to F is real exactly when $h^{-1}\iota' h = \iota_1$. This never happens, because conjugation preserves elementary images and $\bar{\iota}' = \bar{\iota}_2 \neq \bar{\iota}_1$ (Lemma 2.26(d)). Hence $b = |C_H(\iota_1)|/2 \geq 1$, so F has a real place and $\theta = (1 - b/d)/2 < 1/2$. Moreover $d = |H|$, so $b/d = |C_H(\iota_1)|/(2|H|)$ is half the reciprocal of the size N_ι of the conjugacy

class of ι_1 in H , that is, $b/d = 1/(2N_\iota)$. This class maps onto the class in $\overline{G}_B$ of the element ι_1 of Definition 2.12, which has 2^{15} elements by Lemma 2.26(c). Hence $N_\iota \geq 2^{15}$, $b/d \leq 2^{-16}$ and $\theta \geq (1 - 2^{-16})/2 = \theta_*$.

Local structure and splitting. Let $\mathfrak{P}$ be a prime of K above $\mathfrak{p} \in S \cup \{\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2\}$. Its decomposition group in H is conjugate to the image of the local map at $\mathfrak{p}$. Since $\mathcal{U} \subset D_3 G_B$, Lemma 2.26(b) shows that this image is D , $C_2 \times C_2$ or C_4 , the last one cyclic on the Frobenius, and that the prescribed local group injects into H . Therefore the completion $K_{\mathfrak{P}}$ is L_2 over $B_{\mathfrak{p}_j} = \mathbb{Q}_2$, the field $\mathbb{Q}_p(\sqrt{u}, \sqrt{p})$ over $B_{\mathfrak{p}} = \mathbb{Q}_p$ for $p = 3, 5$, and the unramified extension of degree four of $B_{\mathfrak{t}_k}$. Since $B_{\mathfrak{t}_0}$ is unramified of degree two over $\mathbb{Q}_7$ and $B_{\mathfrak{t}_1} = B_{\mathfrak{t}_2} = \mathbb{Q}_{29}$, the places of K above 2, 3, 5, 7 and 29 have the absolute types of Table 5. Every element of the decomposition group has elementary image in the span of the images of the local generators at $\mathfrak{p}$, whereas every conjugate of ι_1 has elementary image $\bar{\iota}_1$. By Lemma 2.26(d), ι_1 lies in no decomposition group of a prime above $S \cup \{\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2\}$, so the decomposition group of $\mathfrak{P}$ in $\text{Gal}(K/F) = \langle \iota_1 \rangle$ is trivial. Hence the places of F above 2, 3, 5, 7, 29 split in K , and they have the same absolute types.

Ramification and root discriminant. The extension K/B , and hence K/F , is unramified at every prime outside S , in particular at $(\sqrt{241})$. At primes above S the inertia group of K/F is trivial, because it lies in the decomposition group. So K/F is unramified at every finite place, its relative discriminant is trivial, $|\Delta_K| = |\Delta_F|^2$, and $\text{rd}(K) = \text{rd}(F)$. To compute $\text{rd}(K)$ we use $|\Delta_K| = 241^{[K:B]} N \mathfrak{d}_{K/B}$. Since K/B is Galois, for $\mathfrak{p} \in S$ all primes $\mathfrak{P}$ above $\mathfrak{p}$ have the same ramification index e , residue degree and different exponent $\text{ord}_{\mathfrak{P}}(\mathfrak{D}_{K/B})$, where $\text{ord}_{\mathfrak{P}}$ and $\text{ord}_{\mathfrak{p}}$ are the normalized valuations at $\mathfrak{P}$ and $\mathfrak{p}$, and $\text{ord}_{\mathfrak{p}}(\mathfrak{D}_{K/B}) = [K : B] \text{ord}_{\mathfrak{P}}(\mathfrak{D}_{K/B})/e$. For $\mathfrak{p}$ above 3 or 5 we have $e = 2$ and $\text{ord}_{\mathfrak{P}}(\mathfrak{D}_{K/B}) = 1$, since over the unramified extension $\mathbb{Q}_p(\sqrt{u})$ the different of $\mathbb{Q}_p(\sqrt{u}, \sqrt{p})$ is generated by $2\sqrt{p}$. For $\mathfrak{p}_1, \mathfrak{p}_2$, Lemma 2.8(d) gives $\text{ord}_{\mathfrak{P}}(\mathfrak{D}_{K/B})/e = 9/4$. Since $[K : \mathbb{Q}] = 2[K : B]$, the base contributes $241^{1/2}$, each of the two primes above 3 contributes $3^{1/4}$, each of the two above 5 contributes $5^{1/4}$, and each dyadic prime contributes $2^{9/8}$. Hence $\text{rd}(K) = 2^{9/4} 3^{1/2} 5^{1/2} 241^{1/2} = \lambda$. $\square$

Remark 2.43. The Lean development [22] formalizes a version of this construction; Remark 4.40 states what it proves and the numerical hypothesis it assumes.

3. THE KUMMER FIELD AND ITS QUADRATIC L -FUNCTIONS

The analytic estimate of Section 4 compares every field of Theorem 2.42 with one fixed subfield, the Kummer field

$$E = B(\sqrt{\alpha_0}, \dots, \sqrt{\alpha_7}) = B(\sqrt{V})$$

of Subsection 2.3, with $\alpha_0, \dots, \alpha_7$ as in (2.3) and V as in Lemma 2.4(d). It is the maximal elementary abelian 2-extension of B unramified at the finite primes outside S , that is, the fixed field of the Frattini subgroup of G_B (Lemma 3.2). The Lean formalization calls E the genus field; we do not use that name here. This section shows that E lies in every field of Theorem 2.42. It then writes ζ_E as the product of ζ_B and 255 quadratic Hecke L -functions of B , and determines their conductors, gamma factors, root numbers and Euler factors.

For $v, e \in \mathbb{F}_2^8$ put $\langle v, e \rangle = \sum_{i=0}^7 v_i e_i \in \mathbb{F}_2$; as in Section 2, vectors are written as strings of their coordinates. For a nonzero ideal $\mathfrak{a}$ of a number field, $N\mathfrak{a}$ denotes its absolute norm. The number of positive divisors of an integer $n \geq 1$ is $\tau(n)$.

3.1. The Characters of the Kummer Field. By Lemma 2.10, $[E : B] = 256$, and the elementary image $\bar{g} \in \mathbb{F}_2^8$ of Definition 2.11, given by $g(\sqrt{\alpha_i}) = (-1)^{\bar{g}_i} \sqrt{\alpha_i}$, identifies $\text{Gal}(E/B)$ with $\mathbb{F}_2^8$.

Definition 3.1. For $e \in \mathbb{F}_2^8$ put

$$\alpha_e = \prod_{i=0}^7 \alpha_i^{e_i}, \quad B_e = B(\sqrt{\alpha_e}),$$

and let χ_e be the character $g \mapsto (-1)^{\langle \bar{g}, e \rangle}$ of $\text{Gal}(E/B)$.

The character χ_e takes the values ± 1 ; in the additive notation of Definition 2.11, $\chi_e(g) = (-1)^{\chi_{\alpha_e}(g)}$. Since $g(\sqrt{\alpha_e}) = \chi_e(g)\sqrt{\alpha_e}$, the character χ_e cuts out B_e , and the 256 characters χ_e are all the characters of $\text{Gal}(E/B)$. For $e \neq 0$ the extension B_e/B is quadratic, because the classes of $\alpha_0, \dots, \alpha_7$ are independent in $B^\times/B^{\times 2}$ (Lemma 2.4(d)).

Lemma 3.2. *The fixed field of the Frattini subgroup D_2G_B of G_B is E . Consequently E is contained in every field K of Theorem 2.42.*

Proof. Let G_S be the group of Subsection 2.3, so that $G_S/D_2G_S = \text{Gal}(E/B)$ (Lemma 2.10), and let $G_B = G_S/N$ as in Definition 2.20. By Lemma 2.21(b), $N \subseteq D_2G_S$, so $G_B/D_2G_B = G_S/D_2G_S = \text{Gal}(E/B)$. A field K of Theorem 2.42 contains the fixed field of $D_4G_B \subseteq D_2G_B$, and hence contains E . $\square$

3.2. Local Data.

Definition 3.3. For a prime $\mathfrak{p} \notin S$ of B , the *Frobenius vector* $\overline{\text{Frob}}_{\mathfrak{p}} \in \mathbb{F}_2^8$ is the elementary image of the Frobenius of $\mathfrak{p}$ in $\text{Gal}(E/B)$, that is, of the Frobenius element $\text{Frob}_{\mathfrak{p}}$ of Subsection 2.3.

For $\mathfrak{p} = \mathfrak{t}_k$ it is the vector of $\text{Frob}_{\mathfrak{t}_k}$ in Table 4. By Euler's criterion, $(\overline{\text{Frob}}_{\mathfrak{p}})_i = 1$ exactly when α_i is not a square in $\mathcal{O}_B/\mathfrak{p}$. For a place $\mathfrak{p}$ of B we write $(\cdot, \cdot)_{\mathfrak{p}}$ for the quadratic Hilbert symbol of $B_{\mathfrak{p}}$.

Proposition 3.4. *Let $e \in \mathbb{F}_2^8 \setminus \{0\}$. For a prime $\mathfrak{p}$ of B let $c_{\mathfrak{p}}(e)$ be the exponent of $\mathfrak{p}$ in the conductor of χ_e , and if $c_{\mathfrak{p}}(e) = 0$, let $\chi_e(\mathfrak{p}) \in \{\pm 1\}$ be the value of χ_e at the Frobenius of $\mathfrak{p}$.*

- (1) *If $\mathfrak{p} \notin S$, then $c_{\mathfrak{p}}(e) = 0$ and $\chi_e(\mathfrak{p}) = (-1)^{\langle \overline{\text{Frob}}_{\mathfrak{p}}, e \rangle}$. Let p be the rational prime below $\mathfrak{p}$. If p splits in B , then $\mathfrak{p} = (p, \sqrt{241} - r)$ with $r^2 \equiv 241 \pmod{p}$, and $(\overline{\text{Frob}}_{\mathfrak{p}})_i = 1$ exactly when the image of α_i under $\sqrt{241} \mapsto r$ is a quadratic nonresidue modulo p . If p is inert, then $(\overline{\text{Frob}}_{\mathfrak{p}})_i = 1$ exactly when $N_{B/\mathbb{Q}}(\alpha_i)$ is a quadratic nonresidue modulo p . If $p = 241$, the same holds with $\sqrt{241} \mapsto 0$.*
- (2) *Let $\mathfrak{p}$ lie above $p \in \{3, 5\}$, let $u = -1$ if $p = 3$ and $u = 2$ if $p = 5$, and let α_i be the generator of $\mathfrak{p}$. If $(u, \alpha_e)_{\mathfrak{p}} = -1$, then $c_{\mathfrak{p}}(e) = 1$. Otherwise $c_{\mathfrak{p}}(e) = 0$ and $\chi_e(\mathfrak{p}) = (-\alpha_i, \alpha_e)_{\mathfrak{p}}$. The Frobenius generator $\varphi_{\mathfrak{p}}$ of Definition 2.12, which fixes $\sqrt{\alpha_i}$, acts on square roots by $(-\alpha_i, \cdot)_{\mathfrak{p}}$ (Table 4).*
- (3) *Let $\mathfrak{p} = \mathfrak{p}_j$. If $(5, \alpha_e)_{\mathfrak{p}} = -1$, then $c_{\mathfrak{p}}(e) = 3$. If $(5, \alpha_e)_{\mathfrak{p}} = 1$ and $(-1, \alpha_e)_{\mathfrak{p}} = -1$, then $c_{\mathfrak{p}}(e) = 2$. Otherwise $c_{\mathfrak{p}}(e) = 0$ and $\chi_e(\mathfrak{p}) = (-2, \alpha_e)_{\mathfrak{p}}$.*
- (4) *The real place v_k becomes complex in B_e , that is, χ_e is nontrivial at v_k , exactly when $\alpha_e < 0$ at v_k .*

Proof. For (1), $\mathfrak{p}$ is odd and α_e is a unit at $\mathfrak{p}$, so $\mathfrak{p}$ is unramified in B_e . By Euler's criterion the Frobenius multiplies $\sqrt{\alpha_e}$ by the quadratic residue symbol of α_e modulo $\mathfrak{p}$, which is $\prod_i (\alpha_i/\mathfrak{p})^{e_i}$. For a split prime, $\mathcal{O}_B/\mathfrak{p} \cong \mathbb{F}_p$ via $\sqrt{241} \mapsto r$. For an inert prime, $\mathcal{O}_B/\mathfrak{p} \cong \mathbb{F}_{p^2}$ and the conjugation of B induces the Frobenius $x \mapsto x^p$ of the residue field, so the residue of $N_{B/\mathbb{Q}}(\alpha)$ is $\bar{\alpha}^{p+1}$. An element of $\mathbb{F}_{p^2}^\times$ is a square exactly when $\bar{\alpha}^{(p^2-1)/2} = (\bar{\alpha}^{p+1})^{(p-1)/2}$ equals 1, that is, when its norm is a square in $\mathbb{F}_p$. The prime above 241 has residue field $\mathbb{F}_{241}$ and $\sqrt{241} \mapsto 0$.

For (2) and (3) we use local class field theory for $B_{\mathfrak{p}} = \mathbb{Q}_p$. The local Artin map sends $b \in \mathbb{Q}_p^\times$ to the automorphism multiplying $\sqrt{\alpha_e}$ by $(b, \alpha_e)_{\mathfrak{p}}$. Units map onto inertia, a uniformizer maps to a Frobenius, and the conductor exponent is the least $n \geq 0$ such that $b \mapsto (b, \alpha_e)_{\mathfrak{p}}$ is trivial on $U^{(n)}$, where $U^{(0)} = \mathbb{Z}_p^\times$ and $U^{(n)} = 1 + p^n \mathbb{Z}_p$ [19].

For $p = 3, 5$, the unit group modulo squares is $\{1, u\}$, and $U^{(1)}$ consists of squares by Hensel's lemma. Hence $c_{\mathfrak{p}}(e) \leq 1$, with equality exactly when $(u, \alpha_e)_{\mathfrak{p}} = -1$. In the unramified case the Frobenius is the image of any uniformizer, such as $-\alpha_i$.

For $p = 2$, the squares of $\mathbb{Z}_2^\times$ form $U^{(3)}$. Moreover $U^{(2)} = U^{(3)} \cup 5U^{(3)}$ and $U^{(0)} = U^{(1)} = \{\pm 1, \pm 5\}U^{(3)}$. The character is thus trivial on $U^{(3)}$. It is trivial on $U^{(2)}$ exactly when $(5, \alpha_e) = 1$, and on $U^{(0)}$ exactly when also $(-1, \alpha_e) = 1$. This gives the stated exponents; the exponent 1 cannot occur since $U^{(0)} = U^{(1)}$. In the unramified case the Frobenius is the image of the uniformizer -2 .

For (4), the real place v_k splits in B_e exactly when $\alpha_e > 0$ at v_k . $\square$

Each condition in the proposition is linear in e :

Lemma 3.5. *Let $e \in \mathbb{F}_2^8$. Then $(5, \alpha_e)_{\mathfrak{p}_j} = (-1)^{\langle \bar{x}_j, e \rangle}$, $(-1, \alpha_e)_{\mathfrak{p}_j} = (-1)^{\langle \bar{y}_j, e \rangle}$ and $(-2, \alpha_e)_{\mathfrak{p}_j} = (-1)^{\langle \bar{z}_j, e \rangle}$. For a prime $\mathfrak{p}$ above 3 or 5, with u as in Proposition 3.4(2) and α_i the generator of $\mathfrak{p}$, $(u, \alpha_e)_{\mathfrak{p}} = (-1)^{\langle \bar{u}, e \rangle}$ and $(-\alpha_i, \alpha_e)_{\mathfrak{p}} = (-1)^{\langle \bar{\alpha}_i, e \rangle}$. Finally, $\alpha_e < 0$ at v_k exactly when $\langle \bar{v}_k, e \rangle = 1$.*

Proof. In each case $(b, \alpha_e)_{\mathfrak{p}} = (-1)^{\langle w, e \rangle}$, where w is the elementary image of the local generator that acts on square roots by $(b, \cdot)_{\mathfrak{p}}$ in Table 4: at $\mathfrak{p}_j$ the vectors $\bar{x}_j, \bar{y}_j, \bar{z}_j$ belong to $b = 5, -1, -2$, and above 3 and 5 the images of the inertia and Frobenius generators belong to $b = u$ and $b = -\alpha_i$. Likewise the complex conjugation ι_k negates $\sqrt{\alpha_e}$ exactly when $\alpha_e < 0$ at v_k (Lemma 2.7(a)), and it multiplies $\sqrt{\alpha_e}$ by $(-1)^{\langle \bar{v}_k, e \rangle}$. $\square$

We put $\nu_k(e) = \langle \bar{v}_k, e \rangle \in \{0, 1\}$ for $k = 1, 2$. By Proposition 3.4, the conductor of χ_e is $f_e = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{c_{\mathfrak{p}}(e)}$.

Corollary 3.6. *The type (Definition 2.41) of a prime $\mathfrak{p}$ of B in E/B is $(4, 2)$ at $\mathfrak{p}_1, \mathfrak{p}_2$; $(2, 2)$ at $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2$; and $(1, 1)$ or $(1, 2)$ at $\mathfrak{p} \notin S$, according as $\overline{\text{Frob}}_{\mathfrak{p}} = 0$ or not. In particular $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$ have type $(1, 2)$ in E/B .*

Proof. For $\mathfrak{p} \in S$, local class field theory identifies the decomposition group of $\mathfrak{p}$ in $\text{Gal}(E/B) = \mathbb{F}_2^8$ with the image of $\mathbb{Q}_p^\times$ under the local Artin map, and the inertia group with the image of the units. By Lemma 3.5, at $\mathfrak{p}_j$ these are spanned by $\bar{x}_j, \bar{y}_j, \bar{z}_j$ and by $\bar{x}_j, \bar{y}_j$; the three vectors are independent (Table 4), so the decomposition group has order 8 and inertia has order 4. Above 3 and 5 the two elementary images are independent, which gives $(2, 2)$. For $\mathfrak{p} \notin S$ the decomposition group is generated by $\overline{\text{Frob}}_{\mathfrak{p}}$. The Frobenius vectors of $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$ are nonzero (Table 4). $\square$

3.3. The Zeta Function of the Kummer Field. Let χ_B be the Dirichlet character $n \mapsto (n/241)$.

Proposition 3.7. *For $\text{Re } s > 1$,*

$$\zeta_E(s) = \zeta_B(s) \prod_{e \in \mathbb{F}_2^8 \setminus \{0\}} L(s, \chi_e), \quad \zeta_B(s) = \zeta(s) L(s, \chi_B),$$

where $L(s, \chi_e) = \zeta_{B_e}(s)/\zeta_B(s)$ is the Hecke L -function of χ_e .

Proof. Compare Euler factors at a prime $\mathfrak{p}$ of B . Let $T_{\mathfrak{p}} \subseteq Z_{\mathfrak{p}} \subseteq G = \text{Gal}(E/B)$ be its inertia and decomposition groups, and put $f_{\mathfrak{p}} = |Z_{\mathfrak{p}}/T_{\mathfrak{p}}|$ and $g_{\mathfrak{p}} = |G/Z_{\mathfrak{p}}|$. The Euler factor of ζ_E at $\mathfrak{p}$ is $(1 - X^{f_{\mathfrak{p}}})^{-g_{\mathfrak{p}}}$ with $X = N\mathfrak{p}^{-s}$. A character nontrivial on $T_{\mathfrak{p}}$ contributes the factor 1. The characters trivial on $T_{\mathfrak{p}}$ are those of $G/T_{\mathfrak{p}}$; they restrict onto the $f_{\mathfrak{p}}$ characters of the cyclic group $Z_{\mathfrak{p}}/T_{\mathfrak{p}}$, each with $g_{\mathfrak{p}}$ extensions. Hence their factors multiply to $\prod_{\zeta^{f_{\mathfrak{p}}}=1} (1 - \zeta X)^{-g_{\mathfrak{p}}} = (1 - X^{f_{\mathfrak{p}}})^{-g_{\mathfrak{p}}}$. The same identity for B_e/B identifies $L(s, \chi_e)$ with ζ_{B_e}/ζ_B . The second identity is the case of $B/\mathbb{Q}$. Since $241 \equiv 1 \pmod{8}$, the prime 2 splits in B , and quadratic reciprocity shows that the character of $B/\mathbb{Q}$ is χ_B . $\square$

Put $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2)$ and $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s)$, so that $\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s+1)$ by the duplication formula. For a number field M with discriminant Δ_M and signature $(r_1(M), r_2(M))$, the completed Dedekind zeta function is

$$\Lambda_M(s) = |\Delta_M|^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1(M)} \Gamma_{\mathbb{C}}(s)^{r_2(M)} \zeta_M(s).$$

Proposition 3.8. *Let $e \neq 0$, write $L(s, \chi_e) = \sum_{n \geq 1} a_n(e) n^{-s}$, and put*

$$Q_e = 241 \text{Nf}_e, \quad \Lambda(s, \chi_e) = Q_e^{s/2} \Gamma_{\mathbb{R}}(s + \nu_1(e)) \Gamma_{\mathbb{R}}(s + \nu_2(e)) L(s, \chi_e).$$

- (1) *The coefficients $a_n(e)$ are integers with $|a_n(e)| \leq \tau(n)$. The Euler factor at a rational prime p is $\prod_{\mathfrak{p}|p} (1 - \chi_e(\mathfrak{p}) \text{N}\mathfrak{p}^{-s})^{-1}$, with $\chi_e(\mathfrak{p}) = 0$ when $c_{\mathfrak{p}}(e) > 0$.*
- (2) *The function $\Lambda(s, \chi_e)$ equals $\Lambda_{B_e}(s)/\Lambda_B(s)$. It is entire of order at most one and satisfies $\Lambda(s, \chi_e) = \Lambda(1-s, \chi_e)$; that is, the root number of $L(s, \chi_e)$ is 1.*
- (3) *Exactly 63 of the characters have $\nu_1(e) = \nu_2(e) = 0$, exactly 64 have $\nu_1(e) = \nu_2(e) = 1$, and 128 have $\nu_1(e) \neq \nu_2(e)$.*

Proof. The Euler factor in (1) is Proposition 3.7 applied prime by prime. Above a rational prime there are at most two primes of B . So the local factor is either a product of at most two factors $(1 - cp^{-s})^{-1}$, or a single factor $(1 - cp^{-2s})^{-1}$, with $c \in \{0, \pm 1\}$. In both cases the coefficient of p^{-ks} has modulus at most $k+1 = \tau(p^k)$. Multiplicativity gives (1).

For (2), the completed Dedekind zeta functions satisfy $\Lambda_M(1-s) = \Lambda_M(s)$, and $L(s, \chi_e)$ extends to an entire function because χ_e is nontrivial [12, 37]. The discriminants satisfy $|\Delta_{B_e}| = |\Delta_B|^2 \text{N}\mathfrak{d}_{B_e/B}$, where $\mathfrak{d}_{B_e/B}$ is the relative discriminant, and the conductor–discriminant formula gives $\mathfrak{d}_{B_e/B} = \mathfrak{f}_e$ for the quadratic extension B_e/B . Hence $|\Delta_{B_e}|/|\Delta_B| = 241 \text{Nf}_e = Q_e$. If $\nu_k(e) = 0$, the place v_k splits into two real places of B_e and contributes $\Gamma_{\mathbb{R}}(s)^2/\Gamma_{\mathbb{R}}(s) = \Gamma_{\mathbb{R}}(s)$. If $\nu_k(e) = 1$, it becomes one complex place and contributes $\Gamma_{\mathbb{C}}(s)/\Gamma_{\mathbb{R}}(s) = \Gamma_{\mathbb{R}}(s+1)$. Thus $\Lambda_{B_e}/\Lambda_B = \Lambda(s, \chi_e)$. It is the completed Hecke L -function of χ_e , which is entire of order at most one [12, 37].

For (3), the vectors $\bar{t}_1, \bar{t}_2$ are linearly independent. So $e \mapsto (\nu_1(e), \nu_2(e))$ maps $\mathbb{F}_2^8$ onto $\mathbb{F}_2^2$ with fibers of size 64. Removing $e = 0$ from the fiber over $(0, 0)$ gives the counts. $\square$

Definition 3.9. Let $e \neq 0$. The gamma factor of χ_e is *pure* if $\nu_1(e) = \nu_2(e) = \nu$, and then it equals $\Gamma_{\mathbb{R}}(s + \nu)^2$; otherwise it is *mixed*, and then it equals $\Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s + 1) = \Gamma_{\mathbb{C}}(s)$.

Corollary 3.10. *For $e \neq 0$, $Q_e = 241 \cdot 2^i \cdot m$, where $2^i = 2^{c_{\mathfrak{p}_1}(e) + c_{\mathfrak{p}_2}(e)} \in \{1, 4, 8, 16, 32, 64\}$ and $m = 3^{c_{\mathfrak{q}_1}(e) + c_{\mathfrak{q}_2}(e)} 5^{c_{\mathfrak{r}_1}(e) + c_{\mathfrak{r}_2}(e)}$ divides 225. The number of characters χ_e with given 2^i and m is given by the table*

$2^i \backslash m$	1	3	5	9	15	25	45	75	225	total
1	0	2	2	1	4	1	2	2	1	15
4	2	4	4	2	8	2	4	4	2	32
8	4	8	8	4	16	4	8	8	4	64
16	1	2	2	1	4	1	2	2	1	16
32	4	8	8	4	16	4	8	8	4	64
64	4	8	8	4	16	4	8	8	4	64
total	15	32	32	16	64	16	32	32	16	255

In particular $723 \leq Q_e \leq 241 \cdot 14400 = 3470400$.

Proof. Only the primes of S divide the conductors, so $Q_e = 241 \text{Nf}_e$ with

$$\text{Nf}_e = 2^{c_{\mathfrak{p}_1}(e) + c_{\mathfrak{p}_2}(e)} 3^{c_{\mathfrak{q}_1}(e) + c_{\mathfrak{q}_2}(e)} 5^{c_{\mathfrak{r}_1}(e) + c_{\mathfrak{r}_2}(e)}.$$

By Proposition 3.4, $c_{\mathfrak{p}_j}(e) \in \{0, 2, 3\}$ and $c_{\mathfrak{q}_j}(e), c_{\mathfrak{r}_j}(e) \in \{0, 1\}$, and by Lemma 3.5 these exponents are determined by the vectors of Table 4; counting the 255 vectors $e \neq 0$ gives the table, which the supplementary program `check255.gp` also prints (Remark 3.12). No nontrivial character has $\text{Nf}_e = 1$, since B has class number one and a unit of norm -1 (Lemma 2.4(a),(b)), so that its narrow class number is one. The range of Q_e can be read off from the table. $\square$

Remark 3.12. The supplementary program `lfun241.py` computes, for each $e \neq 0$, the integer Q_e , the pair $(\nu_1(e), \nu_2(e))$ and the coefficients $a_n(e)$ for $n \leq N_e = 4\lfloor \sqrt{Q_e} \rfloor + 1$, the truncation point used in Subsection 4.6, from Propositions 3.4 and 3.8(1); these are the data used in Section 4.

The supplementary program `check255.gp` compares all 255 of them with PARI/GP's own number fields and L -functions [41]. For each e it computes the maximal order of B_e , checks $|\Delta_{B_e}| = 241 Q_e$ and the pair $(\nu_1(e), \nu_2(e))$ against the signature of B_e , and checks every coefficient $a_n(e)$ with $n \leq N_e$ against the Dirichlet series of ζ_{B_e}/ζ_B . All agree. It also prints the table (3.11), the counts of Proposition 3.8(3) and the range of Q_e . These comparisons check the implementation; the identification of the L -functions rests on Propositions 3.4 and 3.8.

4. THE RELATIVE ZETA VALUE AND AN EXPLICIT UPPER BOUND

We bound the relative zeta value $L_F(1)$ needed in the geometric construction. Logarithms of Dedekind zeta functions are normalized by the degree: for a number field A we work with $[A : \mathbb{Q}]^{-1} \log \zeta_A(s)$.

Definition 4.1. Let $\mathcal{K}$ be the set of all finite Galois extensions K/B contained in B_G , of degree a power of two at least 2^{49} , such that $G_B \rightarrow \overline{G}_B$ factors through $\text{Gal}(K/B)$ (notation of Definition 2.20). These are the fields K of Theorem 2.42.

For $K \in \mathcal{K}$ we use the notation of Theorem 2.42: ι_1 is a complex conjugation at a place of K above v_1 , $F = K^{\langle \iota_1 \rangle}$, $d = [F : \mathbb{Q}]$, so that $[K : \mathbb{Q}] = 2d$, (b, c) is the signature of F , $\theta = c/d$, and $\lambda = 2^{9/4} \sqrt{3615}$ is the root discriminant of both K and F . Put

$$\ell = \log \lambda = \frac{9}{4} \log 2 + \frac{1}{2} \log 3615 = 5.65600472355 \dots$$

Different choices of ι_1 are conjugate in $\text{Gal}(K/B)$ and give conjugate fields F ; hence b, c, θ and the function $L_F(s) = \zeta_K(s)/\zeta_F(s)$ depend only on K . The extension K/F is quadratic and unramified at every finite place, K is totally imaginary, and $b \geq 1$. Let γ be Euler's constant. For a prime $\mathfrak{p}$ of B , let $e_K(\mathfrak{p})$ and $f_K(\mathfrak{p})$ be its ramification index and residue degree in the Galois extension K/B , so that $(e_K(\mathfrak{p}), f_K(\mathfrak{p}))$ is the type of $\mathfrak{p}$ in K/B (Definition 2.41).

Theorem 4.2. *There is an m_0 such that every $K \in \mathcal{K}$ with $[K : B] \geq m_0$ satisfies*

$$\frac{1}{d} \log L_F(1) < C := 0.04871285.$$

The proof assumes neither the generalized Riemann hypothesis nor a Brauer–Siegel type asymptotic formula, and it does not give an effective value of m_0 . It has three steps. Monotonicity of the completion of L_F reduces the value at $s = 1$ to ζ_K at a real point $\sigma > 1$ (Subsection 4.1). The Tsfasman–Vlăduț inequality bounds the error of this shift (Subsection 4.2, Proposition 4.13). Finally, $\zeta_K(\sigma)$ is bounded prime by prime by $\zeta_E(\sigma)$, for the Kummer field E of Section 3, minus corrections at the primes above 2, 7 and 29, whose types in K/B are known, and at the primes of $\mathcal{P}_4$ (Definition 4.15), whose residue degree in K/B is at least 4 (Proposition 4.19); $\zeta_E(\sigma)$ is evaluated rigorously in Subsections 4.4–4.6 (Proposition 4.29). Subsection 4.7 computes these corrections and the lower bounds for the types in K/B that Proposition 4.13 uses, and the last subsection combines the steps. Throughout, σ denotes a real number greater than 1 and $\varepsilon = \sigma - 1$; in this section ε is this positive number, not the unit α_1 of (2.3).

4.1. Reduction to $s > 1$. For a number field A , write h_A , Reg_A , w_A and Δ_A for its class number, regulator, number of roots of unity and discriminant. The residue of ζ_A at $s = 1$ is $2^{r_1(A)} (2\pi)^{r_2(A)} h_A \text{Reg}_A / (w_A |\Delta_A|^{1/2})$. Since K/F is unramified at the finite places, $|\Delta_K| = |\Delta_F|^2$. Hence

$$(4.3) \quad L_F(1) = \lim_{s \rightarrow 1} \frac{\zeta_K(s)}{\zeta_F(s)} = 2^c \pi^{d-c} \lambda^{-d/2} \frac{h_K \text{Reg}_K w_F}{h_F \text{Reg}_F w_K} > 0.$$

Let $s > 1$ be real. At a prime of F of norm q , the Euler factor of L_F is $(1 - q^{-s})^{-1}$ if the prime splits in K and $(1 + q^{-s})^{-1}$ if it is inert. Its square is at most the Euler factor of ζ_K , which is

$(1 - q^{-s})^{-2}$, respectively $(1 - q^{-2s})^{-1}$. Consequently

$$(4.4) \quad \frac{\log L_F(s)}{d} \leq \frac{\log \zeta_K(s)}{2d} = \frac{\log \zeta_K(s)}{[K : \mathbb{Q}]}.$$

The function L_F is the Hecke L -function of the quadratic character of K/F . This character is unramified at every finite place and nontrivial at every real place of F , since K is totally imaginary. With $\Gamma_{\mathbb{R}}$, $\Gamma_{\mathbb{C}}$ and Λ_A as in Section 3, put

$$(4.5) \quad \mathcal{L}_F(s) = \frac{\Lambda_K(s)}{\Lambda_F(s)} = \lambda^{ds/2} \Gamma_{\mathbb{R}}(s+1)^b \Gamma_{\mathbb{C}}(s)^c L_F(s).$$

By Hecke's theorem [12, 37], $\mathcal{L}_F$ is entire of order at most one, and it satisfies $\mathcal{L}_F(s) = \mathcal{L}_F(1-s)$ because both completed Dedekind zeta functions do.

Lemma 4.6. *The function $\mathcal{L}_F(s)$ is positive and nondecreasing on $[1, \infty)$.*

Proof. The Euler product shows that $\mathcal{L}_F$ has no zeros with $\operatorname{Re} s > 1$, and the functional equation excludes $\operatorname{Re} s < 0$. So every zero ρ satisfies $0 \leq \operatorname{Re} \rho \leq 1$. There is no zero on $[1, \infty)$, by the Euler product and by (4.3). As $\mathcal{L}_F(s) > 0$ for large real s , it is positive on $[1, \infty)$.

Put $\Xi(z) = \mathcal{L}_F(\frac{1}{2} + z)$. It is entire of order at most one, even, and real on the real axis. Its zeros $z = \rho - \frac{1}{2}$ satisfy $|\operatorname{Re} z| \leq \frac{1}{2}$, and $\sum_{z \neq 0} |z|^{-2} < \infty$. Group the nonzero zeros into pairs $\{z_0, -z_0\}$, and let $m \geq 0$ be the order of Ξ at 0. By Hadamard's theorem for functions of order at most one,

$$\frac{\Xi'}{\Xi}(z) - \frac{m}{z} - \sum_{\{z_0, -z_0\}} \frac{2z}{z^2 - z_0^2}$$

is constant, where the series converges absolutely and locally uniformly away from the zeros. Since Ξ is even, Ξ'/Ξ is odd, so the constant is zero. For real $x \geq \frac{1}{2}$ the logarithmic derivative is real, so it equals the sum of the real parts. If $z_0 = a + iy$, then

$$\operatorname{Re} \frac{2x}{x^2 - z_0^2} = \frac{2x(x^2 - a^2 + y^2)}{(x^2 - a^2 + y^2)^2 + 4a^2y^2} \geq 0,$$

because $|a| \leq \frac{1}{2} \leq x$. Since also $m/x \geq 0$, the logarithmic derivative is nonnegative, and $\log \Xi$ is nondecreasing on $[\frac{1}{2}, \infty)$. $\square$

For $0 < \varepsilon \leq 1$ and $0 \leq \theta \leq \frac{1}{2}$ put

$$(4.7) \quad \Upsilon(\varepsilon, \theta) = \frac{\varepsilon}{2}(\ell - \log \pi) - \varepsilon\theta \log 2 + (1 - 2\theta) \log \Gamma\left(1 + \frac{\varepsilon}{2}\right) + \theta \log \Gamma(1 + \varepsilon).$$

Lemma 4.8. *Let $K \in \mathcal{K}$ and $0 < \varepsilon \leq 1$. Then*

$$(4.9) \quad \frac{\log L_F(1)}{d} \leq \frac{\log \zeta_K(1 + \varepsilon)}{[K : \mathbb{Q}]} + \Upsilon(\varepsilon, \theta).$$

Moreover $\Upsilon(\varepsilon, \theta) \rightarrow 0$ as $\varepsilon \downarrow 0$, uniformly for $0 \leq \theta \leq \frac{1}{2}$.

Proof. By Lemma 4.6, $\mathcal{L}_F(1) \leq \mathcal{L}_F(1 + \varepsilon)$. In (4.5) the gamma factors change by

$$\frac{\Gamma_{\mathbb{R}}(2 + \varepsilon)}{\Gamma_{\mathbb{R}}(2)} = \pi^{-\varepsilon/2} \Gamma\left(1 + \frac{\varepsilon}{2}\right), \quad \frac{\Gamma_{\mathbb{C}}(1 + \varepsilon)}{\Gamma_{\mathbb{C}}(1)} = (2\pi)^{-\varepsilon} \Gamma(1 + \varepsilon).$$

Taking logarithms, dividing by d , and using $b/d = 1 - 2\theta$, $c/d = \theta$ and (4.4), we obtain (4.9). Since Υ is affine in θ , $\Upsilon(\varepsilon, \theta) \rightarrow 0$ as $\varepsilon \downarrow 0$, uniformly for $0 \leq \theta \leq \frac{1}{2}$. $\square$

The term Υ does not appear in the final estimate. With the value $\varepsilon = 1/300$ used in the proof of Theorem 4.2, (4.9) would add $\Upsilon(1/300, \theta) \approx 0.0054$ for θ near $\frac{1}{2}$. Instead, the proof of Proposition 4.13 applies (4.9) with $s - 1$ in place of ε for each fixed $s \in (1, 2]$, passes to the limit along a sequence of fields, and then lets $s \downarrow 1$, so that Υ vanishes in the limit; the Tsfasman-Vlăduț

inequality then bounds the change from $1 + \varepsilon$ to 1 by the term $\varepsilon(\kappa_\infty + \mathcal{D})$ of that proposition, which is about 0.00215 in the proof of Theorem 4.2. This limit is also the reason why m_0 is not effective.

4.2. The Tsfasman–Vlăduț Inequality over B . For $q > 1$ and $s \geq 1$ put $g_s(q) = -\log(1 - q^{-s})$.

Lemma 4.10. *Let M be a finite Galois extension of B and $s > 1$. For a prime $\mathfrak{p}$ of B let $e_M(\mathfrak{p})$ and $f_M(\mathfrak{p})$ be its ramification index and residue degree in M/B . Then*

$$(4.11) \quad \frac{\log \zeta_M(s)}{[M : \mathbb{Q}]} = \sum_{\mathfrak{p}} \frac{g_s(\mathbf{N}\mathfrak{p}^{f_M(\mathfrak{p})})}{2e_M(\mathfrak{p})f_M(\mathfrak{p})},$$

$$(4.12) \quad -\frac{1}{[M : \mathbb{Q}]} \frac{\zeta'_M}{\zeta_M}(2) = \frac{1}{[M : \mathbb{Q}]} \sum_{\mathfrak{p}} \frac{\log \mathbf{N}\mathfrak{p}}{\mathbf{N}\mathfrak{p}^2 - 1} = \sum_{\mathfrak{p}} \frac{\log \mathbf{N}\mathfrak{p}}{2e_M(\mathfrak{p})(\mathbf{N}\mathfrak{p}^{2f_M(\mathfrak{p})} - 1)},$$

where $\mathfrak{p}$ runs over the primes of M . Each summand on the right does not increase when $e_M(\mathfrak{p})$ or $f_M(\mathfrak{p})$ is replaced by a larger real number. If $M \subseteq M'$ are both Galois over B , then $e_M(\mathfrak{p}) \mid e_{M'}(\mathfrak{p})$ and $f_M(\mathfrak{p}) \mid f_{M'}(\mathfrak{p})$.

Proof. Above $\mathfrak{p}$ there are $[M : B]/(ef)$ primes of M , each of norm $\mathbf{N}\mathfrak{p}^f$, and $[M : \mathbb{Q}] = 2[M : B]$. This gives both formulas. The first equality in (4.12) follows from $-\zeta'_M/\zeta_M(s) = \sum_{\mathfrak{p}} \log \mathbf{N}\mathfrak{p}/(\mathbf{N}\mathfrak{p}^s - 1)$. For monotonicity in f , write $g_s(x^f)/f = \sum_{j \geq 1} x^{-fjs}/(fj)$ for $x > 1$; each term decreases in f . The divisibilities hold because ramification indices and residue degrees are multiplicative in towers. $\square$

Put

$$\kappa_\infty = \frac{\ell - \gamma - \log(4\pi)}{4}, \quad w(q) = 2 \log q \sum_{m \geq 1} \frac{1}{q^m + 1}.$$

Here $2\kappa_\infty$ is the right side, and $w(q)$ the weight of the prime power q , in the Tsfasman–Vlăduț inequality (4.14) below.

Proposition 4.13. *Let $\sigma = 1 + \varepsilon$ with $0 < \varepsilon \leq 1$, and let Y_* be a real number with $[K : \mathbb{Q}]^{-1} \log \zeta_K(\sigma) \leq Y_*$ for every $K \in \mathcal{K}$. For each prime $\mathfrak{p}$ of B , let $e_{\mathfrak{p}}^0, f_{\mathfrak{p}}^0 \geq 1$ be integers with $e_K(\mathfrak{p}) \geq e_{\mathfrak{p}}^0$ and $f_K(\mathfrak{p}) \geq f_{\mathfrak{p}}^0$ for every $K \in \mathcal{K}$, that is, lower bounds for the type of $\mathfrak{p}$ in K/B , and let*

$$\mathcal{D} \geq \sum_{\mathfrak{p}} \frac{\log \mathbf{N}\mathfrak{p}}{2e_{\mathfrak{p}}^0(\mathbf{N}\mathfrak{p}^{2f_{\mathfrak{p}}^0} - 1)}.$$

Then every $C' > Y_ + \varepsilon(\kappa_\infty + \mathcal{D})$ has the following property: there is an m_0 such that $d^{-1} \log L_F(1) < C'$ for every $K \in \mathcal{K}$ with $[K : B] \geq m_0$.*

Proof. A limiting sequence. Suppose not. Then there are fields $K^{(j)} \in \mathcal{K}$ of strictly increasing degree, hence pairwise non-isomorphic, with $d_j^{-1} \log L_{F^{(j)}}(1) \geq C'$, where $[K^{(j)} : \mathbb{Q}] = 2d_j$. For a prime power q let $N_q(K)$ be the number of primes of K of norm q . If $q = p^f$, then $N_q(K) \leq [K : \mathbb{Q}]/f$, since the local degrees above p add up to $[K : \mathbb{Q}]$. By a diagonal argument we may assume that $\beta_q = \lim_j N_q(K^{(j)})/(2d_j)$ exists for every q .

The Tsfasman–Vlăduț inequality. Tsfasman and Vlăduț call a sequence (A_i) of pairwise non-isomorphic number fields asymptotically exact if its genus $\mathfrak{g}(A_i) = \log |\Delta_{A_i}|^{1/2}$ tends to infinity and the limits $\phi_q = \lim N_q(A_i)/\mathfrak{g}(A_i)$, $\phi_{\mathbb{R}} = \lim r_1(A_i)/\mathfrak{g}(A_i)$ and $\phi_{\mathbb{C}} = \lim r_2(A_i)/\mathfrak{g}(A_i)$ exist. Their unconditional Basic Inequality' [42, Section 3.2, Proposition 3.1] states that every such sequence satisfies

$$2 \sum_q \phi_q \log q \sum_{m \geq 1} \frac{1}{q^m + 1} + \phi_{\mathbb{R}} \left(\frac{\gamma}{2} + \frac{1}{2} + \log 2\sqrt{\pi} \right) + \phi_{\mathbb{C}} (\gamma + \log 4\pi) \leq 1.$$

For our sequence $\mathbf{g}(K^{(j)}) = d_j \ell$ and $K^{(j)}$ is totally imaginary, so $\phi_q = 2\beta_q/\ell$, $\phi_{\mathbb{R}} = 0$ and $\phi_{\mathbb{C}} = 1/\ell$, and the inequality becomes

$$(4.14) \quad \sum_q \beta_q w(q) \leq \frac{\ell - \gamma - \log(4\pi)}{2} = 2\kappa_{\infty}.$$

The value at 1. Put $Z(s) = \sum_q \beta_q g_s(q)$ for $s \geq 1$. Since $g_1(q) \leq 1/(q-1)$ and $w(q) \geq 2 \log q/(q+1)$, we have $g_1(q) \leq 3w(q)/(2 \log 2)$, so $Z(1)$ is finite. For fixed real $s > 1$, $(2d_j)^{-1} \log \zeta_{K^{(j)}}(s) = \sum_q (N_q(K^{(j)})/2d_j) g_s(q)$ tends to $Z(s)$ by dominated convergence: for $q = p^f$ the terms are at most $g_s(q)/f \leq 2q^{-s}$, and $\sum_q q^{-s} < \infty$. By Lemma 4.8 with $s-1$ in place of ε , for $1 < s \leq 2$,

$$C' \leq \limsup_j \frac{\log L_{F^{(j)}}(1)}{d_j} \leq Z(s) + \sup_{0 \leq \theta \leq 1/2} \Upsilon(s-1, \theta).$$

As $s \downarrow 1$, $Z(s)$ increases to $Z(1)$ and the supremum tends to zero. Hence $C' \leq Z(1)$.

From $1 + \varepsilon$ to 1. For every prime power q ,

$$\begin{aligned} g_1(q) - g_{1+\varepsilon}(q) &= \int_1^{1+\varepsilon} \frac{\log q}{q^u - 1} du \leq \frac{\varepsilon \log q}{q - 1}, \\ \frac{\log q}{q - 1} - \frac{w(q)}{2} &= \log q \sum_{m \geq 1} \frac{1}{q^m (q^m + 1)} \leq \frac{\log q}{q^2 - 1}. \end{aligned}$$

With (4.14) these give

$$Z(1) \leq Z(1 + \varepsilon) + \varepsilon \left(\kappa_{\infty} + \sum_q \beta_q \frac{\log q}{q^2 - 1} \right).$$

By Fatou's lemma, (4.12) for $M = K^{(j)}$, and the monotonicity in Lemma 4.10,

$$\sum_q \beta_q \frac{\log q}{q^2 - 1} \leq \liminf_j \sum_{\mathfrak{p}} \frac{\log N_{\mathfrak{p}}}{2e_{K^{(j)}}(\mathfrak{p})(N_{\mathfrak{p}}^{2f_{K^{(j)}}(\mathfrak{p})} - 1)} \leq \mathcal{D}.$$

Finally $Z(1 + \varepsilon) = \lim_j (2d_j)^{-1} \log \zeta_{K^{(j)}}(1 + \varepsilon) \leq Y_*$. Thus $C' \leq Z(1) \leq Y_* + \varepsilon(\kappa_{\infty} + \mathcal{D})$, a contradiction. $\square$

4.3. Comparison with the Kummer Field. We use the set S of the six primes of B above 2, 3 and 5 and the primes $\mathfrak{t}_0 = 7\mathcal{O}_B$ and $\mathfrak{t}_1, \mathfrak{t}_2$ above 29 (Lemma 2.4), the group G_B of Definition 2.20 and its Zassenhaus filtration $D_n G_B$, the relation space R_2 in degree two (Definition 2.23), which Lemma 2.25 computes, the restricted square $v^{[2]}$ of a vector $v \in \mathbb{F}_2^8$ as in Section 2, and the Frobenius vectors $\overline{\text{Frob}}_{\mathfrak{p}}$ of Definition 3.3.

Definition 4.15. Let $\Sigma_2 = \{v \in \mathbb{F}_2^8 : v^{[2]} \in R_2\}$, and let $\mathcal{P}_4$ be the set of primes $\mathfrak{p} \notin S \cup \{\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2\}$ of B with $N_{\mathfrak{p}} \leq 10^6$ and $\overline{\text{Frob}}_{\mathfrak{p}} \notin \Sigma_2$.

Lemma 4.16. *Let $K \in \mathcal{K}$, and let $\mathfrak{p} \notin S$ be a prime of B with $\overline{\text{Frob}}_{\mathfrak{p}} \notin \Sigma_2$. Then $e_K(\mathfrak{p}) = 1$ and $f_K(\mathfrak{p}) \geq 4$.*

Proof. The field K is unramified over B outside S , so $e_K(\mathfrak{p}) = 1$, and a prime $\mathfrak{P}$ of K above $\mathfrak{p}$ has a Frobenius $\text{Frob}_{\mathfrak{P}} \in \text{Gal}(K/B)$ of order $f_K(\mathfrak{p})$. Choose $g \in G_B$ mapping to $\text{Frob}_{\mathfrak{P}}$. Its image in $G_B/D_2 G_B = \text{Gal}(E/B)$ is the Frobenius of $\mathfrak{p}$ in E (Lemma 3.2), whose elementary image is $\overline{\text{Frob}}_{\mathfrak{p}}$; it is nonzero, since $0 \in \Sigma_2$. By Lemma 2.25, which uses the complete list of generators of N_B in Lemma 2.22, and since $\overline{\text{Frob}}_{\mathfrak{p}}^{[2]} \notin R_2$, g has order at least 4 in $G_B/D_3 G_B$. The projection $G_B \rightarrow G_B/D_3 G_B$ factors through $\text{Gal}(K/B)$, because K contains the fixed field of $D_4 G_B \subseteq D_3 G_B$. So $\text{Frob}_{\mathfrak{P}}$ has order at least 4. $\square$

The next proposition compares $\zeta_K(\sigma)$ with $\zeta_E(\sigma)$ and subtracts two corrections. The first concerns the primes $\mathfrak{p}_1, \mathfrak{p}_2$ above 2 and $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$ above 7 and 29, whose types in K/B are known; the second concerns the primes of $\mathcal{P}_4$, which are found in Subsection 4.7. Put

$$(4.17) \quad \Delta_{2,7,29}(\sigma) = 2\left(\frac{g_\sigma(2^2)}{16} - \frac{g_\sigma(2^4)}{64}\right) + 2\left(\frac{g_\sigma(29^2)}{4} - \frac{g_\sigma(29^4)}{8}\right) + \frac{g_\sigma(7^4)}{4} - \frac{g_\sigma(7^8)}{8},$$

$$(4.18) \quad \Delta_{\mathcal{P}_4}(\sigma) = \sum_{\mathfrak{p} \in \mathcal{P}_4} \left(\frac{g_\sigma(N\mathfrak{p}^2)}{4} - \frac{g_\sigma(N\mathfrak{p}^4)}{8} \right).$$

Every term of both sums is nonnegative, since $g_\sigma(x^2) \leq g_\sigma(x)$.

Proposition 4.19. *Every $K \in \mathcal{K}$ satisfies*

$$\frac{\log \zeta_K(\sigma)}{[K : \mathbb{Q}]} \leq \frac{\log \zeta_E(\sigma)}{512} - \Delta_{2,7,29}(\sigma) - \Delta_{\mathcal{P}_4}(\sigma).$$

Proof. By Lemma 3.2, $E \subseteq K$, and both are Galois over B . Apply (4.11) to $M = E$ and $M = K$. By Lemma 4.10, each term for K is at most the corresponding term for E . For the primes listed below we bound the term for K from above using what is known about the type in K/B , and subtract the difference between the term for E and this upper bound.

The types in E/B are given by Corollary 3.6: $(4, 2)$ at $\mathfrak{p}_1, \mathfrak{p}_2$, and $(1, 2)$ at $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$ and at the primes of $\mathcal{P}_4$. By Theorem 2.42, the primes of K above 2, 29 and 7 have absolute types $(8, 4)$, $(1, 4)$ and $(1, 8)$. The primes $\mathfrak{p}_j$, $\mathfrak{t}_1$ and $\mathfrak{t}_2$ have residue degree one over $\mathbb{Q}$, and $\mathfrak{t}_0$ has residue degree two. So the types in K/B are $(8, 4)$ at $\mathfrak{p}_j$ and $(1, 4)$ at $\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2$. By Lemma 4.16, the primes of $\mathcal{P}_4$ have $e_K = 1$ and $f_K \geq 4$. The differences of the terms of E and the upper bounds for the terms of K are exactly the summands of (4.17) and (4.18). For example, at $\mathfrak{p}_j$ the term of E is $g_\sigma(2^2)/(2 \cdot 4 \cdot 2)$ and that of K is $g_\sigma(2^4)/(2 \cdot 8 \cdot 4)$. $\square$

4.4. An Approximate Functional Equation for Two Gamma Factors. We evaluate $\zeta_E(\sigma)$ through Proposition 3.7. The factors $L(\sigma, \chi_e)$ are computed from an approximate functional equation. For real μ and $x, y > 0$ define the incomplete gamma and Bessel integrals

$$H_\mu(x) = \int_1^\infty u^{\mu-1} e^{-xu} du, \quad I_\mu(y) = \int_1^\infty u^\mu K_0(yu) du,$$

where K_0 is the modified Bessel function of the second kind of order zero, and their envelopes (upper bounds, by Lemma 4.21(2))

$$\mathcal{V}_1(x) = \frac{e^{-x}}{x} \left(1 + \frac{1}{x}\right), \quad \mathcal{V}_2(y) = \sqrt{\frac{\pi}{2}} \frac{e^{-y}}{y^{3/2}} \left(1 + \frac{1}{y}\right).$$

Numerical evaluation of L -functions from their functional equations is developed in [3]. Part (1) of the next lemma treats mixed gamma factors, and part (2), for pure gamma factors, uses the Bessel function K_0 . We prove both.

Lemma 4.20. *Let a_n be real numbers with $|a_n| \leq \tau(n)$, let $Q > 0$ and $\nu_1, \nu_2 \in \{0, 1\}$ (integers, not places), and let $L(s) = \sum_{n \geq 1} a_n n^{-s}$. Suppose that $\Lambda(s) = Q^{s/2} \Gamma_{\mathbb{R}}(s + \nu_1) \Gamma_{\mathbb{R}}(s + \nu_2) L(s)$ extends to an entire function of order at most one with $\Lambda(1-s) = \Lambda(s)$. Put $t = 2\pi/\sqrt{Q}$ and let $\sigma > 1$ be real.*

(1) *If $\nu_1 \neq \nu_2$, then*

$$L(\sigma) = \frac{t^\sigma}{\Gamma(\sigma)} \sum_{n \geq 1} a_n (H_\sigma(tn) + H_{1-\sigma}(tn)).$$

(2) *If $\nu_1 = \nu_2 = \nu$, then*

$$L(\sigma) = \frac{4(t/2)^{\sigma+\nu}}{\Gamma((\sigma+\nu)/2)^2} \sum_{n \geq 1} a_n n^\nu (I_{\sigma+\nu-1}(tn) + I_{\nu-\sigma}(tn)).$$

The series converge absolutely.

Proof. In case (1) put $k(x) = e^{-x}$ and $\nu = 0$, and in case (2) put $k(x) = K_0(x)$. Their Mellin transforms are $\Gamma(w)$ and $2^{w-2}\Gamma(w/2)^2$ for $\operatorname{Re} w > 0$ [25, 10.43.19]. Let $\Theta(u) = \sum_n a_n n^\nu k(tnu)$ for $u > 0$. For $\operatorname{Re} w > 1 + \nu$, termwise integration gives

$$\tilde{\Theta}(w) = \int_0^\infty \Theta(u) u^{w-1} du = \begin{cases} t^{-w} \Gamma(w) L(w) = \frac{1}{2} \Lambda(w) & \text{in case (1),} \\ 2^{w-2} t^{-w} \Gamma(w/2)^2 L(w - \nu) = \frac{1}{4} Q^{\nu/2} \Lambda(w - \nu) & \text{in case (2).} \end{cases}$$

In case (1) we used $\Gamma_{\mathbb{R}}(w)\Gamma_{\mathbb{R}}(w+1) = \Gamma_{\mathbb{C}}(w)$ and $Q^{w/2}(2\pi)^{-w} = t^{-w}$. In both cases $\tilde{\Theta}$ is entire and $\tilde{\Theta}(w) = \tilde{\Theta}(1 + 2\nu - w)$.

The function $L = \Lambda/(Q^{s/2}\Gamma_{\mathbb{R}}(s + \nu_1)\Gamma_{\mathbb{R}}(s + \nu_2))$ of the complex variable s is entire of finite order. Fix $\eta > 0$. The function L is bounded on $\operatorname{Re} s = 1 + \eta$, and, by the functional equation and Stirling's formula, of polynomial growth on $\operatorname{Re} s = -\eta$. By the Phragmén–Lindelöf principle it has polynomial growth in $|\operatorname{Im} s|$ on every vertical strip. With Stirling's formula this shows that $\tilde{\Theta}(w)$ decays exponentially in $|\operatorname{Im} w|$, uniformly on vertical strips. Mellin inversion on a line $\operatorname{Re} w = c > 1 + \nu$ and a shift to $\operatorname{Re} w = 1 + 2\nu - c$ are therefore justified, and no residues occur. With the functional equation of $\tilde{\Theta}$ they give

$$\Theta(u) = u^{-1-2\nu} \Theta(1/u) \quad (u > 0).$$

In particular $\Theta(u)$ decays rapidly as $u \downarrow 0$. Splitting the Mellin integral at $u = 1$ and substituting $u \mapsto 1/u$ below 1 gives

$$\tilde{\Theta}(\sigma + \nu) = \int_1^\infty \Theta(u) (u^{\sigma+\nu-1} + u^{\nu-\sigma}) du.$$

Termwise integration, justified by the exponential decay of k , turns the right side into $\sum_n a_n n^\nu$ times $H_\sigma(tn) + H_{1-\sigma}(tn)$ in case (1), and times $I_{\sigma+\nu-1}(tn) + I_{\nu-\sigma}(tn)$ in case (2). On the left, $\tilde{\Theta}(\sigma) = t^{-\sigma} \Gamma(\sigma) L(\sigma)$ in case (1), and $\tilde{\Theta}(\sigma + \nu) = 2^{\sigma+\nu-2} t^{-\sigma-\nu} \Gamma((\sigma + \nu)/2)^2 L(\sigma)$ in case (2). $\square$

Lemma 4.21. *Let $\mu \in \mathbb{R}$.*

- (1) *The functions H_μ and I_μ are Laplace transforms of positive measures on $[1, \infty)$. They are completely monotone on $(0, \infty)$, extend holomorphically to $\operatorname{Re} z > 0$, and satisfy $|H(z)| \leq H(\operatorname{Re} z)$ there, for $H = H_\mu$ or $H = I_\mu$.*
- (2) *If $\mu \leq 2$, then $H_\mu \leq \mathcal{V}_1$. If $\mu \leq 3/2$, then $I_\mu \leq \mathcal{V}_2$.*
- (3) *They satisfy*

$$xH'_\mu(x) + \mu H_\mu(x) = -e^{-x}, \quad yI'_\mu(y) + (\mu + 1)I_\mu(y) = -K_0(y),$$

and K_0 satisfies $y^2 K_0'' + yK_0' - y^2 K_0 = 0$ and $K_0' = -K_1$, where K_1 is the modified Bessel function of the second kind of order one.

Proof. The definition exhibits H_μ as the Laplace transform of $u^{\mu-1} du$ on $[1, \infty)$. Taking the order 0 in [25, 10.32.9] and substituting $v = \cosh r$ in its integral gives $K_0(x) = \int_1^\infty e^{-xv} (v^2 - 1)^{-1/2} dv$. Substituting this into I_μ , and then $v = r/u$ in the inner integral, shows

$$I_\mu(y) = \int_1^\infty e^{-yr} \left(\int_1^r u^\mu (r^2 - u^2)^{-1/2} du \right) dr,$$

with a nonnegative inner integral. Differentiation under the integral gives complete monotonicity. Since the measures are positive and $|e^{-zr}| = e^{-r \operatorname{Re} z}$, we get $|H(z)| \leq H(\operatorname{Re} z)$ for $\operatorname{Re} z > 0$, which proves (1).

For (2), $u^{\mu-1} \leq u$ for $u \geq 1$ and $\mu \leq 2$, and $\int_1^\infty u e^{-xu} du = \mathcal{V}_1(x)$. For I_μ we use $K_0(x) \leq K_{1/2}(x) = \sqrt{\pi/(2x)} e^{-x}$ [25, 10.39.2]. It holds because the modified Bessel function of order $\eta \geq 0$

is $\int_0^\infty e^{-x \cosh r} \cosh(\eta r) dr$ [25, 10.32.9], which increases with η . Since $u^{\mu-1/2} \leq u$ for $\mu \leq 3/2$,

$$I_\mu(y) \leq \sqrt{\frac{\pi}{2y}} \int_1^\infty u^{\mu-1/2} e^{-yu} du \leq \mathcal{V}_2(y).$$

For (3), differentiate under the integral and integrate by parts: $xH'_\mu(x) = -\int_1^\infty u^\mu x e^{-xu} du = -e^{-x} - \mu H_\mu(x)$, and $yI'_\mu(y) = \int_1^\infty u^{\mu+1} \frac{d}{du} K_0(yu) du = -K_0(y) - (\mu+1)I_\mu(y)$. The last two identities are Bessel's equation and a standard derivative [25, 10.25.1, 10.29.3]. $\square$

In the application $\sigma = 301/300$, so $1 < \sigma \leq 3/2$. The four exponents σ , $1 - \sigma$, $\sigma + \nu - 1$ and $\nu - \sigma$ in Lemma 4.20 are then covered by the envelopes: $\mathcal{V}_1$ bounds H_σ and $H_{1-\sigma}$, and $\mathcal{V}_2$ bounds $I_{\sigma+\nu-1}$ and $I_{\nu-\sigma}$.

Lemma 4.22. *Let $1 < \sigma \leq 3/2$, let $|a_n| \leq \tau(n)$, let $t > 0$, $N \geq 1$ and $\omega > 1$.*

(1) *If $t(N+1) \geq \omega - 1$, then for $\mu \in \{\sigma, 1 - \sigma\}$*

$$\sum_{n>N} |a_n| H_\mu(tn) \leq \zeta(\omega)^2 (N+1)^\omega \mathcal{V}_1(t(N+1)).$$

(2) *If $\nu \in \{0, 1\}$ and $t(N+1) \geq \omega + \nu - \frac{3}{2}$, then for $\mu \in \{\sigma + \nu - 1, \nu - \sigma\}$*

$$\sum_{n>N} |a_n| n^\nu I_\mu(tn) \leq \zeta(\omega)^2 (N+1)^{\omega+\nu} \mathcal{V}_2(t(N+1)).$$

Proof. The logarithmic derivative of $x^\omega \mathcal{V}_1(x) = x^{\omega-1} e^{-x} (1+1/x)$ is $(\omega-1)/x - 1 - 1/(x(x+1)) < 0$ for $x \geq \omega - 1$. So $n^\omega \mathcal{V}_1(tn) \leq (N+1)^\omega \mathcal{V}_1(t(N+1))$ for $n > N$. By Lemma 4.21(2),

$$\sum_{n>N} |a_n| H_\mu(tn) \leq \sum_{n>N} \frac{\tau(n)}{n^\omega} n^\omega \mathcal{V}_1(tn) \leq (N+1)^\omega \mathcal{V}_1(t(N+1)) \sum_{n \geq 1} \frac{\tau(n)}{n^\omega},$$

and the last sum is $\zeta(\omega)^2$. Part (2) is the same, since $y^{\omega+\nu} \mathcal{V}_2(y)$ is a multiple of $y^{\omega+\nu-3/2} e^{-y} (1+1/y)$, which decreases for $y \geq \omega + \nu - \frac{3}{2}$. $\square$

4.5. Enclosures of H_μ and I_μ , and Finite Sums. An *enclosure* of a real number is an interval that contains it. We enclose H_μ and I_μ on a geometric grid. Let H be H_μ or I_μ with μ as in Lemma 4.22, and let $\mathcal{V}$ be its envelope, $\mathcal{V}_1$ or $\mathcal{V}_2$. For $J \geq 0$ and $\xi > 0$ put

$$\rho_J(\xi) = \mathcal{V}(\xi/2) \frac{16^{-J-1}}{1 - 1/16}.$$

Lemma 4.23. *Let $\xi > 0$ and let $h_j = H^{(j)}(\xi)/j!$ be the Taylor coefficients of H at ξ .*

(1) *$(-1)^j h_j \geq 0$ and $|h_j| \leq \mathcal{V}(\xi/2) (2/\xi)^j$ for all $j \geq 0$.*

(2) *For $|x - \xi| \leq \xi/32$, $|H(x) - \sum_{j=0}^J h_j (x - \xi)^j| \leq \rho_J(\xi)$. For $x = 31\xi/32$ the difference lies in $[0, \rho_J(\xi)]$.*

(3) *Let k_j be the Taylor coefficients at ξ of e^{-x} if $H = H_\mu$, and of K_0 if $H = I_\mu$. If $H = H_\mu$, then $(j+1)\xi h_{j+1} = -k_j - (j+\mu)h_j$, and $k_j = (-1)^j e^{-\xi}/j!$. If $H = I_\mu$, then $(j+1)\xi h_{j+1} = -k_j - (j+\mu+1)h_j$, where $k_0 = K_0(\xi)$, $k_1 = -K_1(\xi)$, and*

$$(j+1)(j+2)\xi^2 k_{j+2} = -(j+1)(2j+1)\xi k_{j+1} - (j^2 - \xi^2)k_j + 2\xi k_{j-1} + k_{j-2},$$

with $k_{-1} = k_{-2} = 0$.

Proof. Complete monotonicity gives the signs in (1). The disc $|z - \xi| \leq \xi/2$ lies in $\operatorname{Re} z \geq \xi/2$, where $|H(z)| \leq H(\xi/2) \leq \mathcal{V}(\xi/2)$ by Lemma 4.21. Cauchy's estimate gives the bound on h_j . For $|x - \xi| \leq \xi/32$, the omitted terms have modulus at most $\mathcal{V}(\xi/2) 16^{-j}$, and their sum over $j > J$ is at most $\rho_J(\xi)$. For $x < \xi$ every term $h_j (x - \xi)^j$ is nonnegative by (1), so the remainder is nonnegative. Part (3) follows by comparing coefficients of $(x - \xi)^j$ in the differential equations of Lemma 4.21(3), written at $x = \xi + (x - \xi)$. $\square$

The grid points are $\xi_i = 64(31/32)^i$ for $0 \leq i \leq i_1$, where $i_1 = 1878$ is the least index with $\xi_{i_1} \leq 2^{-80}$. Taylor polynomials are formed at $\xi_0, \dots, \xi_{i_1-1}$. The initial values $e^{-\xi_i}$, $K_0(\xi_i)$ and $K_1(\xi_i)$ of part (3) of Lemma 4.23 are enclosed with the rigorous exponential and Bessel functions of Arb [15], which is now part of FLINT [38] and is called through its Python interface.

Lemma 4.24. *Let $J \geq 0$, and suppose that enclosures of $e^{-\xi_i}$, $K_0(\xi_i)$ and $K_1(\xi_i)$ are given for $0 \leq i < i_1$. Start from the enclosure $[0, \mathcal{V}(64)]$ of $H(\xi_0)$. For $i = 0, 1, \dots, i_1 - 1$, compute from the enclosure of $H(\xi_i)$ enclosures of $h_0, \dots, h_J$ at ξ_i by the recurrences of Lemma 4.23(3), and take*

$$\sum_{j=0}^J h_j(-\xi_i/32)^j + [0, \rho_J(\xi_i)],$$

evaluated in interval arithmetic, as the enclosure of $H(\xi_{i+1})$. Then every interval so obtained contains the corresponding true value.

Proof. By Lemma 4.21, $H(\xi_0) \in [0, \mathcal{V}(64)]$. Suppose that the enclosure of $H(\xi_i)$ contains $H(\xi_i)$. The true Taylor coefficients at ξ_i are obtained from the true value $H(\xi_i)$ by the same recurrence, so their enclosures contain them. Since $\xi_{i+1} = 31\xi_i/32$, Lemma 4.23(2) shows that the enclosure of $H(\xi_{i+1})$ contains $H(\xi_{i+1})$. Induction on i proves the lemma. $\square$

Now let $t > 0$, $\nu \in \{0, 1\}$, integers $a_1, \dots, a_N$ and $J \geq 0$ be given, with $tN < \xi_0$ and $t > \xi_{i_1}$. For $0 \leq i < i_1$ let $\mathcal{B}_i = \{n : 1 \leq n \leq N, \xi_{i+1} < tn \leq \xi_i\}$. These sets partition $\{1, \dots, N\}$. For nonempty $\mathcal{B}_i$, let $\bar{n}_i$ be the integer part of the average of its least and largest elements, and put

$$M_{i,j} = \sum_{n \in \mathcal{B}_i} a_n n^\nu (n - \bar{n}_i)^j, \quad A_i = \sum_{n \in \mathcal{B}_i} |a_n| n^\nu, \quad P_{i,j} = t^j \sum_{m=j}^J \binom{m}{j} h_{i,m} (t\bar{n}_i - \xi_i)^{m-j},$$

where $h_{i,m}$ are the Taylor coefficients of H at ξ_i . The moments $M_{i,j}$ and the absolute sums A_i are exact integers.

Lemma 4.25. *With this notation,*

$$(4.26) \quad \left| \sum_{n=1}^N a_n n^\nu H(tn) - \sum_i \sum_{j=0}^J P_{i,j} M_{i,j} \right| \leq \sum_i \rho_J(\xi_i) A_i,$$

where i runs over the indices with $\mathcal{B}_i$ nonempty.

Proof. Let $n \in \mathcal{B}_i$. Then $|tn - \xi_i| < \xi_i/32$, so by Lemma 4.23(2) the value $H(tn)$ differs from $\sum_{m=0}^J h_{i,m} (tn - \xi_i)^m$ by at most $\rho_J(\xi_i)$. Since $tn - \xi_i = t(n - \bar{n}_i) + (t\bar{n}_i - \xi_i)$, the binomial theorem gives $\sum_{m=0}^J h_{i,m} (tn - \xi_i)^m = \sum_{j=0}^J P_{i,j} (n - \bar{n}_i)^j$. Multiply by $a_n n^\nu$ and sum over $n \in \mathcal{B}_i$ and over i . $\square$

In the application below $t \geq 2\pi/\sqrt{3470400} > 0.0033$, because $Q_e \leq 3470400$ for every e (Corollary 3.10). So every argument tn exceeds 0.0033, and the part of the grid below that point is not used.

4.6. The Value of ζ_E at $\sigma = 301/300$. From now on $\sigma = 301/300$. Let $e \in \mathbb{F}_2^8 \setminus \{0\}$. By Proposition 3.8, $L(s, \chi_e)$ satisfies the hypotheses of Lemma 4.20 with $Q = Q_e$ and $\nu_k = \nu_k(e)$. Put $t = 2\pi/\sqrt{Q_e}$ and

$$N_e = 4\lfloor \sqrt{Q_e} \rfloor + 1,$$

and let Π_e be the prefactor of that lemma: $\Pi_e = t^\sigma/\Gamma(\sigma)$ if $\nu_1(e) \neq \nu_2(e)$, and $\Pi_e = 4(t/2)^{\sigma+\nu}/\Gamma((\sigma+\nu)/2)^2$ if $\nu_1(e) = \nu_2(e) = \nu$; in the first case put $\nu = 0$. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be the sums $\sum_i \sum_{j=0}^{20} P_{i,j} M_{i,j}$ of Lemma 4.25, with $N = N_e$, $a_n = a_n(e)$ and $J = 20$, for the two functions of the series of Lemma 4.20: $H = H_\sigma$ and $H = H_{1-\sigma}$ in the first case, and $H = I_{\sigma+\nu-1}$ and $H = I_{\nu-\sigma}$ in the second; their envelope is $\mathcal{V} = \mathcal{V}_1$ in the first case and $\mathcal{V} = \mathcal{V}_2$ in the second. For every e , N_e lies between

105 and 7449, and $t(N_e + 1)$ between 24.7 and 25.5 (the supplementary program `check255.gp` prints both ranges). Hence $tN_e < \xi_0$ and $t > \xi_{i_1}$, as Lemma 4.25 requires, and the hypotheses of Lemma 4.22 hold for every ω in the list $\frac{101}{100}, \frac{21}{20}, \frac{11}{10}, \frac{9}{8}, \frac{6}{5}, \frac{5}{4}, \frac{3}{2}, 2$. The value of ω in this list is chosen to minimize the bound

$$\mathcal{T}_e = \sum_i \rho_{20}(\xi_i) A_i + \zeta(\omega)^2 (N_e + 1)^{\omega+\nu} \mathcal{V}(t(N_e + 1)).$$

Lemma 4.27. *For $\sigma = 301/300$ and every $e \in \mathbb{F}_2^8 \setminus \{0\}$,*

$$(4.28) \quad |L(\sigma, \chi_e) - \Pi_e(\mathcal{S}_1 + \mathcal{S}_2)| \leq 2\Pi_e \mathcal{T}_e.$$

Proof. Split each of the two series of Lemma 4.20 at N_e . By Lemma 4.25, each finite part differs from its approximation $\mathcal{S}_1$ or $\mathcal{S}_2$ by at most $\sum_i \rho_{20}(\xi_i) A_i$; the same bound serves both series, since their two functions have the same envelope. By Lemma 4.22, each tail is at most $\zeta(\omega)^2 (N_e + 1)^{\omega+\nu} \mathcal{V}(t(N_e + 1))$. Multiplying by Π_e gives (4.28). $\square$

Proposition 4.29. *For $\sigma = 301/300$,*

$$0.08264460177456 < \frac{\log \zeta_E(\sigma)}{512} < 0.08264460807138.$$

Proof (computer-assisted). By Proposition 3.7,

$$\log \zeta_E(\sigma) = \log \zeta(\sigma) + \log L(\sigma, \chi_B) + \sum_{e \neq 0} \log L(\sigma, \chi_e).$$

The coefficients $a_n(e)$ for $n \leq N_e$ are computed exactly from the Euler factors of Proposition 3.4 by the supplementary program `lfun241.py`. The supplementary program `afe241.py` evaluates (4.28) in Arb midpoint-radius interval arithmetic [15, 38] with 256 bits of precision, rounding every quantity outward. Its routines for Lemmas 4.20–4.25 are taken unchanged from an earlier supplementary archive of the author (Subsection 1.6), and they implement these lemmas as stated here. Every enclosure of $L(\sigma, \chi_e)$ is positive. The factor $\zeta_B(\sigma) = \zeta(\sigma) L(\sigma, \chi_B)$ is evaluated with

$$L(\sigma, \chi_B) = 241^{-\sigma} \sum_{a=1}^{240} \left(\frac{a}{241} \right) \zeta \left(\sigma, \frac{a}{241} \right),$$

where $\zeta(s, x) = \sum_{n \geq 0} (n+x)^{-s}$ is the Hurwitz zeta function, using Arb's rigorous implementation of it [14]. This gives $\zeta_B(\sigma) = 725.51409164864 \dots$ and $L(\sigma, \chi_B) = 2.41373420241 \dots$. Summing the logarithms gives the enclosure

$$[0.08264460177456168 \dots, 0.08264460807137072 \dots]$$

of $\log \zeta_E(\sigma)/512$, which the proposition states rounded outward. So the inequalities follow from Lemmas 4.20–4.27, the exact coefficients, and outward-rounded interval arithmetic. $\square$

As a check independent of the approximate functional equation, the supplementary programs `yecheck.gp` and `lvalues255.gp` evaluate the same values numerically with PARI/GP [41]: each of the 255 values $L(\sigma, \chi_e)$ lies in its enclosure, and PARI's value $0.08264460492293 \dots$ of $\log \zeta_E(\sigma)/512$ lies in the enclosure above.

4.7. Frobenius Vectors and Lower Bounds for the Types.

Lemma 4.30. *The set Σ_2 of Definition 4.15 has exactly 21 elements: zero and the following twenty vectors, written as strings $c_0 c_1 \dots c_7$ of their coordinates, as in Section 2:*

$$\begin{array}{lllll} 00100000 & 11110010 & 11010010 & 00010000 & 10000001 \\ 10010001 & 00001000 & 10100111 & 10101111 & 00000100 \\ 11101011 & 11101111 & 00000010 & 01100101 & 01100111 \\ 00000001 & 01011010 & 01011011 & 10111010 & 11000101. \end{array}$$

In the notation of Table 4, these twenty vectors are the elementary images of the local involutions x_j , y_j and $x_j y_j$ for $j = 1, 2$, of the nonidentity elements of the four local groups $C_2 \times C_2$ above 3 and 5, and of ι_1 and ι_2 .

Proof. Each of these images lies in Σ_2 by Lemma 2.25, since an involution has trivial square. The supplementary program `census241.py` computes Σ_2 by linear algebra over $\mathbb{F}_2$ from the relations of Lemma 2.25, and finds no other vectors. $\square$

Proposition 4.31 (Frobenius vectors of the primes of norm at most 10^6). *Among the 78616 primes $\mathfrak{p} \notin S \cup \{\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2\}$ of B with $N\mathfrak{p} \leq 10^6$, exactly 246 have $\overline{\text{Frob}}_{\mathfrak{p}} = 0$, exactly 5994 have $\overline{\text{Frob}}_{\mathfrak{p}} \in \Sigma_2 \setminus \{0\}$, and the remaining 72376 form $\mathcal{P}_4$.*

Proof. The supplementary program `census241.py` computes the Frobenius vector of each of these primes from Proposition 3.4(1) with exact modular arithmetic, and compares it with the elements of Σ_2 (Lemma 4.30). $\square$

Below we use this classification of the primes, not the three counts.

Lemma 4.32. *For $\sigma = 301/300$,*

$$(4.33) \quad \Delta_{2,7,29}(\sigma) > 0.0344534299, \quad \Delta_{\mathcal{P}_4}(\sigma) > 0.0016298411.$$

Proof. The supplementary program `ceiling241.py` uses the classification of Proposition 4.31 and evaluates (4.17) and (4.18) in Arb interval arithmetic. It gives $\Delta_{2,7,29}(\sigma) = 0.03445342991613\dots$ and $\Delta_{\mathcal{P}_4}(\sigma) = 0.00162984111205\dots$, and the lemma states these values rounded down. $\square$

For every prime $\mathfrak{p}$ of B put

$$(4.34) \quad (e_{\mathfrak{p}}^0, f_{\mathfrak{p}}^0) = \begin{cases} (8, 4) & \mathfrak{p} = \mathfrak{p}_1, \mathfrak{p}_2, \\ (2, 2) & \mathfrak{p} = \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2, \\ (1, 4) & \mathfrak{p} \in \{\mathfrak{t}_0, \mathfrak{t}_1, \mathfrak{t}_2\} \cup \mathcal{P}_4, \\ (1, 2) & N\mathfrak{p} \leq 10^6, \overline{\text{Frob}}_{\mathfrak{p}} \in \Sigma_2 \setminus \{0\}, \\ (1, 1) & \text{otherwise,} \end{cases}$$

where $\mathfrak{q}_1, \mathfrak{q}_2$ and $\mathfrak{r}_1, \mathfrak{r}_2$ are the primes above 3 and 5 (Lemma 2.4).

Lemma 4.35. *For every $K \in \mathcal{K}$ and every prime $\mathfrak{p}$ of B , $e_K(\mathfrak{p}) \geq e_{\mathfrak{p}}^0$ and $f_K(\mathfrak{p}) \geq f_{\mathfrak{p}}^0$. Thus (4.34) gives lower bounds for the types in K/B , as Proposition 4.13 requires.*

Proof. At $\mathfrak{p}_j$ and $\mathfrak{t}_k$ the types in K/B are $(8, 4)$ and $(1, 4)$ by Theorem 2.42, as in the proof of Proposition 4.19. At $\mathfrak{q}_j$ and $\mathfrak{r}_j$ the type in E/B is $(2, 2)$ by Corollary 3.6, and if $\overline{\text{Frob}}_{\mathfrak{p}} \neq 0$, then $f_E(\mathfrak{p}) = 2$ by the same corollary. Since $E \subseteq K$, the ramification indices and residue degrees in E/B divide those in K/B (Lemma 4.10). On $\mathcal{P}_4$ use Lemma 4.16. The bounds $(1, 1)$ hold trivially. $\square$

Lemma 4.36. *For the lower bounds (4.34),*

$$(4.37) \quad \sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{2e_{\mathfrak{p}}^0(N\mathfrak{p}^{2f_{\mathfrak{p}}^0} - 1)} < 0.0085105513.$$

Hence $\mathcal{D} = 0.0085105513$ satisfies the hypothesis of Proposition 4.13.

Proof. The primes of norm greater than 10^6 receive $(1, 1)$. At most two primes of B have a given norm, and $x \mapsto \log x/(x^2 - 1)$ decreases on $[2, \infty)$. So their contribution to the sum is at most

$$\sum_{m > 10^6} \frac{\log m}{m^2 - 1} \leq \int_{10^6}^{\infty} \frac{\log x}{x^2 - 1} dx \leq \frac{\log 10^6 + 1}{10^6} (1 + 10^{-6}).$$

The supplementary program `ceiling241.py` sums the primes of norm at most 10^6 in interval arithmetic and adds this bound for the remaining primes; the result, $0.0085105512261\dots$, is less than 0.0085105513 . $\square$

4.8. Proof of Theorem 4.2.

Corollary 4.38. *Let $\sigma = 301/300$. Every $K \in \mathcal{K}$ satisfies $[K : \mathbb{Q}]^{-1} \log \zeta_K(\sigma) \leq Y_*$, where*

$$Y_* = 0.0826446081 - 0.0344534299 - 0.0016298411 = 0.0465613371.$$

Proof. Combine Proposition 4.19, the upper bound of Proposition 4.29 rounded up, and the lower bounds of Lemma 4.32, which are rounded down. $\square$

Proof of Theorem 4.2. Let $\sigma = 301/300$ and $\varepsilon = 1/300$. We apply Proposition 4.13 with $Y_* = 0.0465613371$ (Corollary 4.38), with the lower bounds (4.34) for the types (Lemma 4.35), and with $\mathcal{D} = 0.0085105513$ (Lemma 4.36). Numerically $\kappa_\infty = (\ell - \gamma - \log(4\pi))/4 = 0.63694120292 \dots < 0.6369412030$, so

$$Y_* + \varepsilon(\kappa_\infty + \mathcal{D}) < 0.0465613371 + \frac{0.6369412030 + 0.0085105513}{300} < 0.0487128430 < C.$$

The interval evaluation of the same expression from the unrounded enclosures, by `ceiling241.py`, gives the upper bound 0.0487128429. Proposition 4.13 with $C' = C$ proves the theorem. $\square$

Remark 4.39. The primes above 2, 3, 5, 7 and 29 alone limit what Proposition 4.13 can give. Let $(K^{(j)})$, β_q and $Z(s) = \sum_q \beta_q g_s(q)$ be as in the proof of that proposition. The absolute types of the primes of $K^{(j)}$ above 2, 3, 5, 7, 29 are known exactly (Theorem 2.42), so these primes contribute exactly

$$\frac{2g_1(2^4)}{64} + \frac{2g_1(3^2)}{8} + \frac{2g_1(5^2)}{8} + \frac{2g_1(29^4)}{8} + \frac{g_1(7^8)}{8} = 0.0416684615 \dots$$

to $Z(1)$, a value printed by `ceiling241.py`; all other contributions are nonnegative. The proof of Proposition 4.13 shows that $Z(1) \leq Y_* + \varepsilon(\kappa_\infty + \mathcal{D})$ for every choice of σ , Y_* , $\mathcal{D}$ and lower bounds for the types that satisfies its hypotheses. So no such choice gives an upper bound below this number. The bound $C = 0.04871285$ exceeds it by 0.0070444.

Remark 4.40 (The hypothesis of the Lean formalization). The Lean formalization [22] proves, under one explicit hypothesis that it does not prove, that there are finite planar sets U_j with $|U_j| \rightarrow \infty$ and $u(U_j)/|U_j|^{1.0427} \rightarrow \infty$. The hypothesis is

$$(4.41) \quad \frac{\log \zeta_E(1 + \frac{1}{300})}{512} + \frac{1}{300} \left(\frac{\ell - \gamma - \log(4\pi)}{4} - \frac{1}{512} \frac{\zeta'_E}{\zeta_E}(2) \right) < 0.0852.$$

In the formalization, E is the subfield of an algebraic closure of $\mathbb{Q}$ generated by $\sqrt{241}$ and square roots of $\alpha_0, \dots, \alpha_7$; it is isomorphic to the Kummer field E , and the formalization calls it the genus field.

The left side of (4.41) is the bound of this section with all local data taken from the fixed subfield E . By (4.12) for $M = E$, $-(\zeta'_E/\zeta_E)(2)/512$ is the sum defining $\mathcal{D}$ in Proposition 4.13 when the lower bounds are the types in E/B . These lower bounds are valid since $E \subseteq K$. The choice $Y_* = \log \zeta_E(\sigma)/512$ is valid by Lemma 4.10. So the left side of (4.41) is the bound given by Proposition 4.13 without the refinements of Proposition 4.19 and with the types in E/B in place of those in K/B . The supplementary program `h241_receipt.py` bounds it by $0.0848335193 < 0.0852$. It uses the upper endpoint in Proposition 4.29, the value of κ_∞ , and $-(\zeta'_E/\zeta_E)(2)/512 < 0.0197321539$, which it obtains by summing (4.12) in interval arithmetic over the primes of norm at most 10^6 and bounding the rest as in the proof of Lemma 4.36.

From (4.41), the formalization subtracts corrections at the primes above 2, 7 and 29 and at the primes above 41, 47, 53, 59, 61, 67, 79, 83 and 97, which lie in $\mathcal{P}_4$. It obtains the weaker bound 0.0495 for $d^{-1} \log L_F(1)$ for the fields of the tower in the formalization. This suffices for the exponent 1.0427 but not for 1.04273. The bound $C = 0.04871285$ of Theorem 4.2 uses Proposition 4.31 and the lower bounds for the types in K/B ; this refinement is not formalized.

5. UNITS OF RELATIVE NORM ONE AND PLANAR POINT SETS

This section and Sections 6 and 7 turn arithmetic data of a quadratic extension into planar point sets. Let K/F be a quadratic extension of number fields, let ι be the nontrivial automorphism of K over F , and let (b, c) be the signature of F . Throughout these three sections we assume:

- (G1) K is totally imaginary, and $b \geq 1$;
- (G2) K/F is unramified at every finite place;
- (G3) $\text{rd}(K) = \text{rd}(F) = \lambda$.

Here the root discriminant rd and the discriminants Δ_M are as in Section 2. By (G2), $|\Delta_K| = |\Delta_F|^2$, so (G3) amounts to $\text{rd}(F) = \lambda$. Put $d = [F : \mathbb{Q}] = b + 2c$, $\theta = c/d$ and $\ell = \log \lambda$. Then $[K : \mathbb{Q}] = 2d$, $|\Delta_K| = \lambda^{2d}$, $|\Delta_F| = \lambda^d$ and $0 \leq \theta < 1/2$, where Δ_K and Δ_F are the absolute discriminants. Theorem 2.42 provides such extensions, with $\lambda = 2^{9/4}\sqrt{3615}$ and $\theta \geq \theta_*$; there ι is the complex conjugation ι_1 . The arguments of these three sections use no Galois structure over B or over $\mathbb{Q}$. For a nonzero fractional ideal $\mathfrak{a}$ of K or of F , $N\mathfrak{a}$ denotes its absolute norm, so that $N(x\mathcal{O}_K) = |N_{K/\mathbb{Q}}x|$ [18, Propositions 4.1 and 4.2]. We take the unit theorem and the covolumes of ideal lattices from [18], and the Herbrand quotient, Hilbert's Theorem 90 and the analytic class-number formula from [19].

The argument has five steps. Proposition 5.2 is the class-number formula for the units of relative norm one: it expresses their regulator, together with the relative class number and the capitulation kernel, through $L_F(1)$. Lemma 5.6 uses the split primes and one ideal class to produce many elements $\beta_1, \dots, \beta_t$ of relative norm one in a single fractional ideal, with pairwise disjoint cosets $\beta_i\mathcal{O}_K^1$. Lemmas 5.9 and 5.13 average over the units of relative norm one and over translates of the ideal lattice; this counts exactly, on average, the pairs of lattice points in a window (Definition 5.11) that differ by the image of an element of $\bigcup_i \beta_i\mathcal{O}_K^1$. Lemmas 5.16 and 5.18 bound the number of lattice points in a window uniformly, by Poisson summation. Finally, Proposition 5.26, the geometric transfer, takes the window to be a sublevel set of the total energy of a pair of profiles (Definition 5.22 and Lemma 5.25) and combines these steps.

5.1. Coordinates. A real place of F extends to K either as two real places or as one complex place, and by (G1) the second case occurs. A complex place of F has two extensions to K , since $\mathbb{C}$ has no quadratic extension. Thus K has exactly d complex places. For each real place v of F , let $\phi_v : K \rightarrow \mathbb{C}$ be one of the two embeddings inducing the place of K above v . Number the complex places of F from 1 to c . For the j -th one fix an embedding $\phi_j^+ : K \rightarrow \mathbb{C}$ whose restriction τ_j to F induces it, and put $\phi_j^- = \phi_j^+ \circ \iota$. The embeddings $\phi_j^\pm$ induce the two places of K above this place: they are distinct, and they are not complex conjugate, because τ_j is not real. We identify $K \otimes_{\mathbb{Q}} \mathbb{R}$ with $\mathbb{C}^d$ through the map $x \mapsto x_\infty$, where

$$x_\infty = ((\phi_v(x))_v, (\phi_j^+(x), \phi_j^-(x))_j),$$

write $\mathfrak{a}_\infty = \{x_\infty : x \in \mathfrak{a}\}$ for $\mathfrak{a} \subset K$, and identify $\mathbb{C}^d$ with $\mathbb{R}^{2d}$ through real and imaginary parts. Volumes are Lebesgue measure in these coordinates, and $\langle x, \xi \rangle = \text{Re} \sum_w x_w \overline{\xi_w}$ is the real inner product, where w runs over the d coordinates. For a Borel set Ω , $|\Omega|$ denotes its volume; for a finite set, $|\cdot|$ denotes its cardinality.

At a real place v of F , the automorphism ι induces complex conjugation on the completion $\mathbb{C}$ of K , so $\phi_v(\iota x) = \overline{\phi_v(x)}$. Writing $v(y) \in \mathbb{R}$ for the image of $y \in F$ under the real embedding v , we obtain for $x \in K$

$$(5.1) \quad |\phi_v(x)|^2 = v(N_{K/F}x), \quad \phi_j^+(x) \phi_j^-(x) = \tau_j(N_{K/F}x).$$

For $x \in K^\times$ put

$$l_j(x) = \frac{1}{2}(\log |\phi_j^+(x)| - \log |\phi_j^-(x)|), \quad l(x) = (l_1(x), \dots, l_c(x)) \in \mathbb{R}^c.$$

If $N_{K/F}\beta = 1$, then by (5.1) $|\phi_v(\beta)| = 1$ for every real place v , and $|\phi_j^\pm(\beta)| = e^{\pm l_j(\beta)}$ for every j . Accordingly the b coordinates ϕ_v are called the *compact coordinates*: there the elements of relative norm one lie on the unit circle. The c pairs (ϕ_j^+, ϕ_j^-) are the *pair coordinates*: there they have reciprocal moduli. A compact coordinate, or a pair of coordinates, is called a *block*. The planar sets will be images under one compact coordinate, which is injective on K and sends every element of relative norm one to a unit vector. We count ordered pairs of points at distance one, and divide by two at the end.

5.2. The Class-Number Formula for Units of Relative Norm One. Let $\mathcal{O}_K^\times$ and $\mathcal{O}_F^\times$ be the unit groups, and put

$$\mathcal{O}_K^1 = \ker(N_{K/F}: \mathcal{O}_K^\times \rightarrow \mathcal{O}_F^\times), \quad I_N = [\mathcal{O}_F^\times : N_{K/F}(\mathcal{O}_K^\times)].$$

Let w_K be the number of roots of unity in K , let h_K and h_F be the class numbers of K and F , put $h_{\text{rel}} = h_K/h_F$, let κ be the order of the *capitulation kernel* $\ker(\text{Cl}(F) \rightarrow \text{Cl}(K))$, the map being induced by extension of ideals, and let $L_F(s) = \zeta_K(s)/\zeta_F(s)$. At $s = 1$, $L_F(1)$ denotes the quotient of the residues of ζ_K and ζ_F . The regulators Reg_K and Reg_F are the ordinary ones, which use twice the logarithm of the absolute value at a complex place [18, Chapter 5].

Proposition 5.2. *The roots of unity of K lie in $\mathcal{O}_K^1$, and the restriction of l to $\mathcal{O}_K^1$ has kernel of order w_K and image a full lattice in $\mathbb{R}^c$. Let Reg^1 be the covolume of this lattice, with $\text{Reg}^1 = 1$ if $c = 0$. Then*

$$\kappa = I_N/2^{b-1}, \quad \text{Reg}_K / \text{Reg}_F = 2^{c-1} I_N \text{Reg}^1,$$

and consequently

$$(5.3) \quad \frac{w_K}{h_{\text{rel}} \kappa \text{Reg}^1} = \frac{2^{d-1} \pi^{b+c}}{\lambda^{d/2} L_F(1)}.$$

Proof. Signs. Fix a real place v_0 of F . By (5.1), $v_0(N_{K/F}x) = |\phi_{v_0}(x)|^2 > 0$ for $x \in K^\times$, so -1 is not a norm from $K^\times$. If $\zeta \in K$ is a root of unity, then $N_{K/F}\zeta$ is a root of unity of F , hence ± 1 because F has a real place, and it is positive at v_0 . Thus $N_{K/F}\zeta = 1$.

Logarithmic embeddings. For $x \in \mathcal{O}_K^\times$ and $y \in \mathcal{O}_F^\times$ let

$$\text{Log}_K(x) = ((2 \log |\phi_v x|)_v, (2 \log |\phi_j^+ x|, 2 \log |\phi_j^- x|)_j), \quad \text{Log}_F(y) = ((\log |v(y)|)_v, (2 \log |\tau_j(y)|)_j).$$

Their images are lattices in the hyperplanes of coordinate sum zero, the kernel of Log_F is $\{\pm 1\}$ [18, Proposition 5.8], and Reg_K and Reg_F are the covolumes of the images after one coordinate is deleted; the choice of the deleted coordinate does not matter.

The lattice $l(\mathcal{O}_K^1)$. Let $\beta \in \mathcal{O}_K^1$. Then $|\phi_v(\beta)| = 1$ and $|\phi_j^\pm(\beta)| = e^{\pm l_j(\beta)}$, so

$$\text{Log}_K(\beta) = (0, (2l_j(\beta), -2l_j(\beta))_j).$$

Hence $l(\beta) = 0$ exactly when every conjugate of β has absolute value one, that is, when β is a root of unity [18, Corollary 5.6]. By the first step the kernel of l on $\mathcal{O}_K^1$ has order w_K . The norm of $y \in \mathcal{O}_F^\times$ is y^2 , so $N_{K/F}(\mathcal{O}_K^\times)$ has finite index in $\mathcal{O}_F^\times$ and rank $b + c - 1$. By the unit theorem [18, Theorem 5.1], $\mathcal{O}_K^\times$ has rank $d - 1$, so $\mathcal{O}_K^1$ has rank c . As $\text{Log}_K(\mathcal{O}_K^1)$ is discrete, so is $l(\mathcal{O}_K^1)$, and it is a full lattice in $\mathbb{R}^c$.

The capitulation kernel. The Herbrand quotient $h(M) = |\widehat{H}^0(\langle \iota \rangle, M)|/|H^1(\langle \iota \rangle, M)|$ [19, Chapter II, §3] of the units satisfies $2h(\mathcal{O}_K^\times) = \prod_v [K_w : F_v]$, where v runs over the archimedean places of F and w lies above v [19, Chapter VII, Proposition 3.1]. Each real place contributes 2 and each complex place 1, so $h(\mathcal{O}_K^\times) = 2^{b-1}$. Since $\widehat{H}^0(\langle \iota \rangle, \mathcal{O}_K^\times) = \mathcal{O}_F^\times / N_{K/F}(\mathcal{O}_K^\times)$ has order I_N , we get $|H^1(\langle \iota \rangle, \mathcal{O}_K^\times)| = I_N/2^{b-1}$. This group is $\mathcal{O}_K^1$ modulo the units $\gamma/\iota\gamma$ with $\gamma \in \mathcal{O}_K^\times$. If $\mathfrak{a}$ is a fractional ideal of F with $\mathfrak{a}\mathcal{O}_K = x\mathcal{O}_K$, the class of the unit $x/\iota x$ depends neither on the choice of x nor on the choice of $\mathfrak{a}$ in its ideal class. This defines a homomorphism from $\ker(\text{Cl}(F) \rightarrow \text{Cl}(K))$ to

$H^1(\langle \iota \rangle, \mathcal{O}_K^\times)$. It is injective: if $x/\iota x = \gamma/\iota \gamma$, then $y = x/\gamma$ lies in F and $\mathfrak{a}\mathcal{O}_K = y\mathcal{O}_K$, so $\mathfrak{a} = y\mathcal{O}_F$ by unique factorization. It is surjective: by Hilbert's Theorem 90 [19, Chapter II, Corollary 1.23], an element of $\mathcal{O}_K^\times$ has the form $x/\iota x$ with $x \in K^\times$, and then the fractional ideal $x\mathcal{O}_K = (\iota x)\mathcal{O}_K$ is invariant under ι . By (G2), every ι -invariant fractional ideal of K is extended from F : at a split prime $\mathfrak{P} \mid \mathfrak{p}$ invariance forces equal exponents, an inert prime of F stays prime, and no prime ramifies. Hence $\kappa = I_N/2^{b-1}$.

Regulators. Delete the coordinate of v_0 from both logarithmic embeddings, and let $\mathcal{U}_K \subset \mathbb{R}^{d-1}$ and $\mathcal{U}_F \subset \mathbb{R}^{b+c-1}$ be the resulting lattices, of covolumes Reg_K and Reg_F . By (5.1), $\text{Log}_F(N_{K/F}x)$ is obtained from $\text{Log}_K(x)$ by keeping the coordinates of the real places and adding the two coordinates of each pair. This induces a linear map $T: \mathbb{R}^{d-1} \rightarrow \mathbb{R}^{b+c-1}$ such that $T(\mathcal{U}_K)$ is the image of $N_{K/F}(\mathcal{O}_K^\times)$ in $\mathcal{U}_F$. The substitution $(x_j, y_j) \mapsto (x_j, x_j + y_j)$ on each pair has determinant one and turns T into a coordinate projection whose kernel consists of the c coordinates x_j . The covolume of a lattice in a product of two coordinate spaces is the covolume of its intersection with the first factor times the covolume of its projection to the second, whenever both are lattices.

A unit $x \in \mathcal{O}_K^\times$ lies in the kernel of T exactly when $\text{Log}_F(N_{K/F}x) = 0$, because the deleted coordinate is minus the sum of the others. Then $N_{K/F}x = \pm 1$, and $N_{K/F}x = 1$ by the first step. So the intersection of $\mathcal{U}_K$ with the kernel is the image of $\mathcal{O}_K^\times$, which after the substitution is $2l(\mathcal{O}_K^\times)$, of covolume 2^cReg_K . Since $-1 \notin N_{K/F}(\mathcal{O}_K^\times)$, the projection $T(\mathcal{U}_K)$ has index $[\mathcal{O}_F^\times : \{\pm 1\}N_{K/F}(\mathcal{O}_K^\times)] = I_N/2$ in $\mathcal{U}_F$. Hence $\text{Reg}_K = 2^c \text{Reg}_F I_N/2$.

The class-number formula. The analytic class-number formula [19, Chapter V, Theorem 2.4] (compare (4.3)), applied to K (with $r_1 = 0$ and $r_2 = d$) and to F (with $r_1 = b$, $r_2 = c$ and $w_F = 2$), gives

$$L_F(1) = \frac{(2\pi)^d h_K \text{Reg}_K}{w_K \lambda^d} \cdot \frac{2\lambda^{d/2}}{2^b (2\pi)^c h_F \text{Reg}_F} = \frac{2^{c+1} \pi^{b+c} h_{\text{rel}}}{w_K \lambda^{d/2}} \frac{\text{Reg}_K}{\text{Reg}_F}.$$

Substituting $\text{Reg}_K / \text{Reg}_F = 2^{c-1} I_N \text{Reg}_F^{-1} = 2^{b+c-2} \kappa \text{Reg}_F^{-1}$ gives (5.3). $\square$

5.3. Norm-One Elements from Split Primes.

Definition 5.4. Let $\mathcal{R}$ be a finite set of rational primes. The extension K/F has *uniform local types* $(e_r, f_r)_{r \in \mathcal{R}}$ if, for every $r \in \mathcal{R}$, every prime of F above r splits in K and has absolute type (e_r, f_r) (Definition 2.41).

If K/F has uniform local types $(e_r, f_r)_{r \in \mathcal{R}}$, then F has exactly $d/(e_r f_r)$ primes above r , each of norm r^{f_r} , since the products $e_{\mathfrak{p}} f_{\mathfrak{p}}$ of the absolute ramification indices and residue degrees of the primes $\mathfrak{p}$ of F above r add up to $[F : \mathbb{Q}] = d$. Given integers $k_r \geq 0$, define

$$(5.5) \quad H = \sum_{r \in \mathcal{R}} \frac{k_r \log r}{e_r}, \quad J = \sum_{r \in \mathcal{R}} \frac{\log(k_r + 1)}{e_r f_r}.$$

Lemma 5.6. Assume that K/F has uniform local types $(e_r, f_r)_{r \in \mathcal{R}}$, and fix integers $k_r \geq 0$. There are a fractional ideal I of K with $N(I) = e^{-dH}$, an integer $t \geq e^{dJ}/(\kappa h_{\text{rel}})$, and elements $\beta_1, \dots, \beta_t \in I$ of relative norm one whose cosets $\beta_i \mathcal{O}_K^\times$ are pairwise disjoint.

Proof. For each prime $\mathfrak{p}$ of F above a prime $r \in \mathcal{R}$, write $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_{\mathfrak{p}} \iota \mathfrak{P}_{\mathfrak{p}}$ and $k_{\mathfrak{p}} = k_r$. For integer vectors $\mathbf{j} = (j_{\mathfrak{p}})$ with $0 \leq j_{\mathfrak{p}} \leq k_{\mathfrak{p}}$ put

$$\mathfrak{A}_{\mathbf{j}} = \prod_{\mathfrak{p}} \mathfrak{P}_{\mathfrak{p}}^{j_{\mathfrak{p}}}, \quad \mathfrak{J}_{\mathbf{j}} = \prod_{\mathfrak{p}} \mathfrak{P}_{\mathfrak{p}}^{j_{\mathfrak{p}}} (\iota \mathfrak{P}_{\mathfrak{p}})^{k_{\mathfrak{p}} - j_{\mathfrak{p}}}.$$

There are $\prod_{\mathfrak{p}} (k_{\mathfrak{p}} + 1) = e^{dJ}$ such vectors. The quotient of $\text{Cl}(K)$ by the image of $\text{Cl}(F)$ has order $h_K \kappa / h_F = \kappa h_{\text{rel}}$, so one class of this quotient contains the classes of $\mathfrak{A}_{\mathbf{j}}$ for a set of $t \geq e^{dJ}/(\kappa h_{\text{rel}})$

vectors $\mathbf{j}$. Fix one of them, $\mathbf{j}_0$, and put $I = \mathfrak{J}_{\mathbf{j}_0}^{-1}$. For each $\mathbf{j}$ in the set, write $\mathfrak{A}_{\mathbf{j}}\mathfrak{A}_{\mathbf{j}_0}^{-1} = x\mathfrak{a}\mathcal{O}_K$ with $x \in K^\times$ and $\mathfrak{a}$ a fractional ideal of F , and put $\beta_{\mathbf{j}} = x/\iota x$. Then $N_{K/F}\beta_{\mathbf{j}} = 1$, and since ι fixes $\mathfrak{a}\mathcal{O}_K$,

$$\beta_{\mathbf{j}}\mathcal{O}_K = \mathfrak{A}_{\mathbf{j}}\mathfrak{A}_{\mathbf{j}_0}^{-1}(\iota\mathfrak{A}_{\mathbf{j}})^{-1}\iota\mathfrak{A}_{\mathbf{j}_0} = \mathfrak{J}_{\mathbf{j}}I.$$

As $\mathfrak{J}_{\mathbf{j}}$ is integral, $\beta_{\mathbf{j}} \in I$. The ideals $\mathfrak{J}_{\mathbf{j}}I$ are distinct for distinct $\mathbf{j}$, and every element of $\beta_{\mathbf{j}}\mathcal{O}_K^1$ generates $\mathfrak{J}_{\mathbf{j}}I$, so the cosets are disjoint. Finally, since each $\mathfrak{p}$ splits in K , $N(I)^{-1} = \prod_{\mathfrak{p}} (N\mathfrak{p})^{k_{\mathfrak{p}}} = \prod_{\mathfrak{p}} r^{f_{\mathfrak{p}}k_{\mathfrak{p}}d/(e_{\mathfrak{p}}f_{\mathfrak{p}})} = e^{dH}$. $\square$

5.4. Unit Averaging and Translation. In this subsection and the next, I is a fractional ideal of K and $\beta_1, \dots, \beta_t \in I$ are elements of relative norm one whose cosets $\beta_i\mathcal{O}_K^1$ are pairwise disjoint; Lemma 5.6 provides such data. For $h \in \mathbb{R}^c$ let $W_h: \mathbb{C}^d \rightarrow \mathbb{C}^d$ multiply the coordinate ϕ_j^+ by e^{-h_j} and ϕ_j^- by e^{h_j} , and fix the compact coordinates. It is a real diagonal map of determinant one. Put $\Lambda_h = W_h I_\infty$. For a lattice $\Lambda \subset \mathbb{C}^d$, $\text{covol}(\Lambda)$ denotes the volume of a fundamental domain. By [18, Proposition 4.26], extended to fractional ideals by scaling and [18, Proposition 4.2],

$$(5.7) \quad \text{covol}(\mathfrak{a}_\infty) = 2^{-d}|\Delta_K|^{1/2}N\mathfrak{a}$$

for every fractional ideal $\mathfrak{a}$ of K . Hence $\text{covol}(\Lambda_h) = 2^{-d}\lambda^d N(I)$, independently of h ; for the ideal of Lemma 5.6,

$$(5.8) \quad \text{covol}(\Lambda_h) = 2^{-d}\lambda^d e^{-dH}.$$

If $N_{K/F}\beta = 1$, then $W_h\beta_\infty$ has compact coordinates of modulus one and pair coordinates of moduli $e^{\pm(l_j(\beta)-h_j)}$. Let Π^1 be a fundamental parallelepiped of the lattice $l(\mathcal{O}_K^1)$; its volume is Reg^1 . When $c = 0$, integrals over $\mathbb{R}^0$ and over Π^1 are evaluations at the single point.

Lemma 5.9. *For every Borel function $\Phi: \mathbb{R}^c \rightarrow [0, \infty]$,*

$$(5.10) \quad \frac{1}{\text{Reg}^1} \int_{\Pi^1} \sum_{i=1}^t \sum_{\beta \in \beta_i \mathcal{O}_K^1} \Phi(l(\beta) - h) dh = \frac{tw_K}{\text{Reg}^1} \int_{\mathbb{R}^c} \Phi(u) du.$$

Proof. The map l is a homomorphism on $K^\times$, so $l(\beta_i\mathcal{O}_K^1) = l(\beta_i) + l(\mathcal{O}_K^1)$, and by Proposition 5.2 each point of this translate of $l(\mathcal{O}_K^1)$ is the image of exactly w_K elements of $\beta_i\mathcal{O}_K^1$. The translates $\Pi^1 - x$, with $x \in l(\mathcal{O}_K^1)$, tile $\mathbb{R}^c$, so by Tonelli's theorem $\int_{\Pi^1} \sum_{x \in l(\mathcal{O}_K^1)} \Phi(l(\beta_i) + x - h) dh = \int_{\mathbb{R}^c} \Phi(u) du$ for each i . $\square$

Definition 5.11. A *window* is a bounded Borel set $\Omega \subset \mathbb{C}^d$ of positive volume that is invariant under rotation of each coordinate separately. For $u \in \mathbb{R}^c$ let $\nu(u) \in \mathbb{C}^d$ have compact coordinates 1 and pair coordinates (e^{u_j}, e^{-u_j}) , and for a Borel set $\Omega \subset \mathbb{C}^d$ put

$$\Phi_\Omega(u) = |\Omega \cap (\Omega - \nu(u))|.$$

Lemma 5.12. *Let Ω be a window, let $h \in \mathbb{R}^c$, and let $\beta \in K$ satisfy $N_{K/F}\beta = 1$. Then $|\Omega \cap (\Omega - W_h\beta_\infty)| = \Phi_\Omega(l(\beta) - h)$.*

Proof. If $x \in \mathbb{C}^d$ has compact coordinates of modulus one and pair coordinates of moduli $e^{\pm u_j}$, then a rotation of the coordinates preserves Ω and maps $\nu(u)$ to x , so $|\Omega \cap (\Omega - x)| = \Phi_\Omega(u)$. By the remark before Lemma 5.9, $x = W_h\beta_\infty$ is such a point, with $u = l(\beta) - h$. $\square$

For a window Ω , the function Φ_Ω is continuous, bounded by $|\Omega|$, and vanishes when some $e^{|u_j|}$ exceeds the diameter of Ω : if x and $x + \nu(u)$ both lie in Ω , then $e^{|u_j|}$, the modulus of a coordinate of their difference $\nu(u)$, is at most the diameter of Ω .

Let Ω be a window. Fix a $\mathbb{Z}$ -basis of I_∞ , and for $y \in [0, 1)^{2d}$ let $y_I \in \mathbb{C}^d$ be the point with coordinate vector y in this basis. For $h \in \mathbb{R}^c$ let $\mathcal{X}(h, y) = (\Lambda_h + W_h y_I) \cap \Omega$ and $n(h, y) = |\mathcal{X}(h, y)|$,

and let $\mathcal{E}(h, y)$ be the number of *ordered edges* of $\mathcal{X}(h, y)$, that is, of pairs (x, β) with $x \in \mathcal{X}(h, y)$, $\beta \in \bigcup_i \beta_i \mathcal{O}_K^1$ and $x + W_h \beta_\infty \in \Omega$. Since $\beta \in I$, the point $x + W_h \beta_\infty$ then lies in $\mathcal{X}(h, y)$.

Lemma 5.13. *Let Ω be a window and suppose $n(h, y) \leq n_{\max} < \infty$ for all (h, y) . Then there is a pair (h, y) with $n(h, y) > 0$ and*

$$(5.14) \quad \frac{\mathcal{E}(h, y)}{n(h, y)} \geq \frac{tw_K}{\text{Reg}^1} \frac{\int_{\mathbb{R}^c} \Phi_\Omega(u) du}{|\Omega|}.$$

Proof. For fixed x , distinct β give distinct points $x + W_h \beta_\infty \neq x$, so $\mathcal{E} \leq n^2 \leq n_{\max}^2$. Both n and $\mathcal{E}$ are countable sums of indicator functions of Borel sets in (h, y) . For fixed h , the map $y \mapsto W_h y_I$ has Jacobian $\text{covol}(\Lambda_h)$ and maps $[0, 1)^{2d}$ onto a fundamental domain of Λ_h , so tiling and Lemma 5.12 give

$$\int_{[0, 1)^{2d}} n(h, y) dy = \frac{|\Omega|}{\text{covol}(\Lambda_h)}, \quad \int_{[0, 1)^{2d}} \mathcal{E}(h, y) dy = \frac{1}{\text{covol}(\Lambda_h)} \sum_i \sum_{\beta \in \beta_i \mathcal{O}_K^1} \Phi_\Omega(l(\beta) - h).$$

Average over $h \in \Pi^1$ with respect to dh/Reg^1 and apply (5.10). For the probability measure $dh dy/\text{Reg}^1$ on $\Pi^1 \times [0, 1)^{2d}$ this gives $\mathbb{E} \mathcal{E} = \rho \mathbb{E} n$ and $\mathbb{E} n = |\Omega|/\text{covol}(\Lambda_h) > 0$, where ρ is the right side of (5.14). If $\mathcal{E} < \rho n$ held wherever $n > 0$, then, since $\mathcal{E} = 0$ where $n = 0$ and $\{n > 0\}$ has positive measure, we would get $\mathbb{E} \mathcal{E} < \rho \mathbb{E} n$. $\square$

Lemma 5.15. *Let Ω be a window, let (h, y) be a pair, and let v_0 be a real place of F . For $x \in \mathbb{C}^d$ let x_{v_0} be its compact coordinate at v_0 , and let $U = \{x_{v_0} : x \in \mathcal{X}(h, y)\} \subset \mathbb{C} = \mathbb{R}^2$. Then $|U| = n(h, y)$ and $u(U) \geq \mathcal{E}(h, y)/2$.*

Proof. Two distinct points of $\mathcal{X}(h, y)$ differ by $W_h \gamma_\infty$ with $0 \neq \gamma \in I$, whose v_0 -coordinate $\phi_{v_0}(\gamma)$ is nonzero, so $|U| = n(h, y)$. An ordered edge (x, β) gives two points of U at distance $|\phi_{v_0}(\beta)| = 1$, and distinct ordered edges give distinct ordered pairs of points. Hence $u(U) \geq \mathcal{E}(h, y)/2$. $\square$

5.5. Uniform Lattice Counting. For a lattice $\Lambda \subset \mathbb{C}^d$ let $\Lambda^* = \{\xi \in \mathbb{C}^d : \langle \xi, x \rangle \in \mathbb{Z} \text{ for all } x \in \Lambda\}$ be its dual lattice, and let $\|\xi\|_* = \sum_w |\xi_w|$, a norm on $\mathbb{C}^d$. We use the Fourier transform $\widehat{\Psi}(\xi) = \int_{\mathbb{C}^d} \Psi(x) e^{-2\pi i \langle x, \xi \rangle} dx$.

Lemma 5.16. *Let $\mathfrak{a}$ be a fractional ideal of K and $h \in \mathbb{R}^c$. Every nonzero ξ in the dual lattice of $W_h \mathfrak{a}_\infty$ satisfies*

$$\prod_w |\xi_w| \geq \frac{2^d}{\lambda^d (N\mathfrak{a})^{1/2}}, \quad \|\xi\|_* \geq \frac{2d}{\lambda (N\mathfrak{a})^{1/(2d)}}.$$

In particular, if $N(I) = e^{-dH}$, as for the ideal of Lemma 5.6, every nonzero dual vector of Λ_h satisfies

$$(5.17) \quad \prod_w |\xi_w| \geq \mu^d, \quad \mu = 2e^{H/2-\ell}, \quad \|\xi\|_* \geq d\mu.$$

Proof. First let $h = 0$. For $x, y \in K$ we have $\langle x_\infty, \overline{y_\infty} \rangle = \text{Re} \sum_w \phi_w(xy) = \frac{1}{2} \text{Tr}_{K/\mathbb{Q}}(xy)$, where the bar is coordinatewise complex conjugation and ϕ_w is the embedding of the coordinate w , because these embeddings and their complex conjugates are all the embeddings of K . Let $\mathfrak{a}^\vee = \{y \in K : \text{Tr}_{K/\mathbb{Q}}(y\mathfrak{a}) \subset \mathbb{Z}\}$. It is an $\mathcal{O}_K$ -module, and since the trace form is nondegenerate, the dual basis of a $\mathbb{Z}$ -basis of $\mathfrak{a}$ is a $\mathbb{Z}$ -basis of $\mathfrak{a}^\vee$. So $\mathfrak{a}^\vee$ is a fractional ideal, and the dual lattice of $\mathfrak{a}_\infty$ is $(2\mathfrak{a}^\vee)_\infty$. Dual lattices have reciprocal covolumes, and complex conjugation preserves volume. With (5.7) and $N(2\mathfrak{a}^\vee) = 2^{2d} N(\mathfrak{a}^\vee)$, this gives $N(\mathfrak{a}^\vee) = \lambda^{-2d} (N\mathfrak{a})^{-1}$. If $0 \neq y \in \mathfrak{a}^\vee$, then $y\mathcal{O}_K \subset \mathfrak{a}^\vee$ and $|N_{K/\mathbb{Q}} y| = N(y\mathcal{O}_K) \geq N(\mathfrak{a}^\vee)$ [18, Propositions 4.1 and 4.2]. For $\xi = (2y)_\infty$,

$$\prod_w |\xi_w| = |N_{K/\mathbb{Q}}(2y)|^{1/2} \geq (2^{2d} \lambda^{-2d} (N\mathfrak{a})^{-1})^{1/2}.$$

For general h , the dual lattice of $W_h \mathbf{a}_\infty$ is the image of the dual lattice of $\mathbf{a}_\infty$ under W_{-h} , because W_h is real diagonal, and W_{-h} preserves $\prod_w |\xi_w|$. The bound for $\|\xi\|_*$ follows from the arithmetic-geometric mean inequality. For (5.17) take $\mathbf{a} = I$. $\square$

Lemma 5.18. *Let $\Lambda \subset \mathbb{C}^d$ be a lattice such that $\prod_w |\xi_w| \geq \mu^d$ for every nonzero $\xi \in \Lambda^*$, where $\mu > 0$. Let $\Psi: \mathbb{C}^d \rightarrow [0, \infty)$ be smooth, bounded and integrable, with $\int \Psi > 0$ and all partial derivatives bounded, and suppose that*

$$|\widehat{\Psi}(\xi)| \leq M^d e^{-\sigma \|\xi\|_*} \int \Psi \quad (\xi \in \mathbb{C}^d)$$

for some $M \geq 1$ and $\sigma > 0$. If the Fourier condition

$$(5.19) \quad \sigma \mu \geq \log M + 2 \log 5 + 2$$

holds, then for every $y \in \mathbb{C}^d$,

$$(5.20) \quad \sum_{x \in \Lambda + y} \Psi(x) \leq \frac{2}{\text{covol}(\Lambda)} \int \Psi.$$

Proof. A nonzero $\xi \in \Lambda^*$ has no zero coordinate, and the arithmetic-geometric mean inequality gives $\|\xi\|_* \geq d\mu$. Hence distinct points of Λ^* are at $\|\cdot\|_*$ -distance at least $d\mu$, and the open $\|\cdot\|_*$ -balls of radius $d\mu/2$ about them are disjoint. For $j \geq 1$, the balls about the points with $j d\mu \leq \|\xi\|_* < (j+1)d\mu$ lie in the ball of radius $(j+3/2)d\mu$ about 0. Comparing volumes in $\mathbb{R}^{2d}$ bounds the number of these points by $(2j+3)^{2d} \leq 5^{2dj}$. By the Fourier condition (5.19) and $M \geq 1$,

$$M^d \sum_{\xi \in \Lambda^* \setminus \{0\}} e^{-\sigma \|\xi\|_*} \leq \sum_{j \geq 1} e^{d(\log M + 2j \log 5 - j \sigma \mu)} \leq \sum_{j \geq 1} e^{-2dj} \leq 1.$$

For $\varepsilon > 0$ put $\Psi_\varepsilon(x) = \Psi(x) e^{-\varepsilon |x|^2}$, a Schwartz function. Its Fourier transform is $\widehat{\Psi}_\varepsilon * G_\varepsilon$, where $G_\varepsilon(\zeta) = (\pi/\varepsilon)^d e^{-\pi^2 |\zeta|^2 / \varepsilon}$ is a probability density on $\mathbb{R}^{2d}$. Hence $|\widehat{\Psi}_\varepsilon(\xi)| \leq m_\varepsilon M^d e^{-\sigma \|\xi\|_*} \int \Psi$, with $m_\varepsilon = \int e^{\sigma \|\zeta\|_*} G_\varepsilon(\zeta) d\zeta$. The function $y \mapsto \sum_{x \in \Lambda} \Psi_\varepsilon(x+y)$ is smooth and Λ -periodic, its Fourier coefficient at $\xi \in \Lambda^*$ is $\widehat{\Psi}_\varepsilon(\xi) / \text{covol}(\Lambda)$, and these coefficients are absolutely summable. This gives the Poisson summation formula

$$\sum_{x \in \Lambda} \Psi_\varepsilon(x+y) = \frac{1}{\text{covol}(\Lambda)} \sum_{\xi \in \Lambda^*} \widehat{\Psi}_\varepsilon(\xi) e^{2\pi i \langle \xi, y \rangle}.$$

Using $\widehat{\Psi}_\varepsilon(0) = \int \Psi_\varepsilon$ and the bound above, the sum is at most $(\int \Psi_\varepsilon + m_\varepsilon \int \Psi) / \text{covol}(\Lambda)$. As $\varepsilon \rightarrow 0$, we have $m_\varepsilon \rightarrow 1$ by dominated convergence, since G_ε is the image of G_1 under $\zeta \mapsto \sqrt{\varepsilon} \zeta$; moreover Ψ_ε increases to Ψ . Monotone convergence gives (5.20). $\square$

The next bound is used in Section 7 for the Gaussian real-place profile.

Lemma 5.21. *If $0 < a_{\mathbb{R}} \leq 1$ and $\Psi_{\mathbb{R}}(z) = e^{-a_{\mathbb{R}} |z|^2}$ on $\mathbb{C}$, then $\widehat{\Psi}_{\mathbb{R}}(\xi) = (\pi/a_{\mathbb{R}}) e^{-\pi^2 |\xi|^2 / a_{\mathbb{R}}}$ and $|\widehat{\Psi}_{\mathbb{R}}(\xi)| \leq 2e^{-|\xi|} \int \Psi_{\mathbb{R}}$.*

Proof. The formula is the Gaussian integral, and $\int \Psi_{\mathbb{R}} = \pi/a_{\mathbb{R}}$. Since $a_{\mathbb{R}} \leq 1$, it suffices that $\pi^2 x^2 - x + \log 2 \geq 0$ for $x \geq 0$, and the minimum of the left side is $\log 2 - 1/(4\pi^2) > 0$. $\square$

5.6. Profiles at Real and Complex Places.

Definition 5.22. Fix $0 < \delta < 1$ and put $p = 2/(1+\delta)$, the *Lebesgue exponent* (not a prime), so that $1 < p < 2$ and $p(1+\delta) = 2$. A *real-place profile* is a positive radial function $f_{\mathbb{R}}$ on $\mathbb{C}$, used at the compact coordinates, and a *complex-place profile* is a positive function $g_{\mathbb{C}}$ on $\mathbb{C}^2$ that depends only

on $|z|$ and $|w|$, used at the pair coordinates. Their *masses* $A_{\mathbb{R}}, A_{\mathbb{C}}$, *overlaps* $I_{\mathbb{R}}, I_{\mathbb{C}}$ and *functionals* $J_{\mathbb{R}}, J_{\mathbb{C}}$ are

$$\begin{aligned} A_{\mathbb{R}} &= \int_{\mathbb{C}} f_{\mathbb{R}}^p, & I_{\mathbb{R}} &= \int_{\mathbb{C}} f_{\mathbb{R}}(z) f_{\mathbb{R}}(z+1) dz, & A_{\mathbb{C}} &= \int_{\mathbb{C}^2} g_{\mathbb{C}}^p, \\ I_{\mathbb{C}} &= \int_{\mathbb{R}} \int_{\mathbb{C}^2} g_{\mathbb{C}}(z, w) g_{\mathbb{C}}(z + e^u, w + e^{-u}) dz dw du, \\ J_{\mathbb{R}} &= \log I_{\mathbb{R}} - (1 + \delta) \log A_{\mathbb{R}}, & J_{\mathbb{C}} &= \log I_{\mathbb{C}} - (1 + \delta) \log A_{\mathbb{C}}. \end{aligned}$$

When these integrals are finite and positive, the *endpoint laws* are the probability densities $f_{\mathbb{R}}(z)f_{\mathbb{R}}(z+1)/I_{\mathbb{R}}$ on $\mathbb{C}$ and $g_{\mathbb{C}}(z, w)g_{\mathbb{C}}(z + e^u, w + e^{-u})/I_{\mathbb{C}}$ on $\mathbb{C}^2 \times \mathbb{R}$. The functions $V_{\mathbb{R}} = -\log f_{\mathbb{R}}$ and $V_{\mathbb{C}} = -\log g_{\mathbb{C}}$ are the *energies* of the profiles.

The exponent p is chosen so that the terms in the mean energy cancel at the end of the proof of Proposition 5.26.

Definition 5.23. Let $M \geq 1$ and $\sigma > 0$. The pair $(f_{\mathbb{R}}, g_{\mathbb{C}})$ is *admissible with Fourier constants* (M, σ) if:

- (P1) $f_{\mathbb{R}}^p$ and $g_{\mathbb{C}}^p$ are smooth and bounded, and all their partial derivatives are bounded;
- (P2) $A_{\mathbb{R}}, I_{\mathbb{R}}, A_{\mathbb{C}}$ and $I_{\mathbb{C}}$ are finite and positive;
- (P3) $V_{\mathbb{R}}$ and $V_{\mathbb{C}}$ are bounded below and coercive, that is, their sublevel sets are bounded;
- (P4) $V_{\mathbb{R}}(z)$ and $V_{\mathbb{C}}(z, w)$ have finite second moments under the endpoint laws;
- (P5) $|\widehat{f_{\mathbb{R}}^p}(\xi)| \leq M e^{-\sigma|\xi|} A_{\mathbb{R}}$ and $|\widehat{g_{\mathbb{C}}^p}(\xi_1, \xi_2)| \leq M^2 e^{-\sigma(|\xi_1| + |\xi_2|)} A_{\mathbb{C}}$ for all $\xi, \xi_1, \xi_2 \in \mathbb{C}$.

Section 7 proves admissibility for the profiles we use.

Lemma 5.24. Let $(f_{\mathbb{R}}, g_{\mathbb{C}})$ be admissible with Fourier constants (M, σ) , and let $\Psi = \prod_v f_{\mathbb{R}}^p \prod_j g_{\mathbb{C}}^p$ be the product function on $\mathbb{C}^d$, with one factor for each block. Then Ψ satisfies the hypotheses that Lemma 5.18 places on Ψ , other than the Fourier condition (5.19): it is smooth and bounded, with bounded derivatives, $\int \Psi = A_{\mathbb{R}}^b A_{\mathbb{C}}^c$, and

$$|\widehat{\Psi}(\xi)| \leq M^d e^{-\sigma\|\xi\|_*} \int \Psi \quad (\xi \in \mathbb{C}^d).$$

Proof. The first properties follow from (P1) and (P2). The Fourier transform of Ψ is the product of the transforms of the factors, so (P5) gives $|\widehat{\Psi}(\xi)| \leq M^{b+2c} e^{-\sigma\|\xi\|_*} \int \Psi = M^d e^{-\sigma\|\xi\|_*} \int \Psi$. $\square$

Lemma 5.25. Let $f_{\mathbb{R}}$ and $g_{\mathbb{C}}$ be profiles satisfying (P1), (P2) and (P4), and let $\eta > 0$. Let $m_{\mathbb{R}}$ and $m_{\mathbb{C}}$ be the means of $V_{\mathbb{R}}(z)$ and $V_{\mathbb{C}}(z, w)$ under the endpoint laws, and let $\text{Var}_{\mathbb{R}}$ and $\text{Var}_{\mathbb{C}}$ be their variances. For $x \in \mathbb{C}^d$ with compact coordinates x_v and pair coordinates (x_j^+, x_j^-) , let $V(x) = \sum_v V_{\mathbb{R}}(x_v) + \sum_j V_{\mathbb{C}}(x_j^+, x_j^-)$ be the total energy, put $\bar{m} = (bm_{\mathbb{R}} + cm_{\mathbb{C}})/d$, and let

$$\Omega = \{x \in \mathbb{C}^d : V(x) \leq d(\bar{m} + \eta)\}.$$

Then, for all d larger than a bound that depends only on $\eta, \text{Var}_{\mathbb{R}}$ and $\text{Var}_{\mathbb{C}}$,

$$\int_{\mathbb{R}^c} \Phi_{\Omega}(u) du \geq \frac{1}{2} I_{\mathbb{R}}^b I_{\mathbb{C}}^c e^{2d(\bar{m} - \eta)}.$$

Proof. By (P1), $f_{\mathbb{R}}$ and $g_{\mathbb{C}}$ are continuous, so V is continuous and Ω is closed, hence a Borel set. The function $(x, u) \mapsto e^{-V(x)} e^{-V(x+\nu(u))} / (I_{\mathbb{R}}^b I_{\mathbb{C}}^c)$ is the product of the endpoint densities of the blocks, hence a probability density on $\mathbb{C}^d \times \mathbb{R}^c$. Under it, the energies $V(x)$ and $V(x + \nu(u))$ of the two endpoints are sums of independent terms, one for each block, and $V(x)$ has mean $d\bar{m}$. On a compact block the map $z \mapsto -z - 1$, and on a pair block the map $(z, w, u_j) \mapsto (-z - e^{u_j}, -w - e^{-u_j}, u_j)$, preserves the endpoint density and carries the first endpoint to minus the second. Since the profiles are even, $V(x + \nu(u))$ has the same law as $V(x)$. By Chebyshev's inequality, each of the two energies differs from $d\bar{m}$ by more than ηd with probability at most $\max(\text{Var}_{\mathbb{R}}, \text{Var}_{\mathbb{C}})/(\eta^2 d)$. So the

set $\mathcal{Y} \subset \mathbb{C}^d \times \mathbb{R}^c$ where both energies lie in $[d(\bar{m} - \eta), d(\bar{m} + \eta)]$ has probability at least $1/2$ for all d larger than a bound that depends only on η , $\text{Var}_{\mathbb{R}}$ and $\text{Var}_{\mathbb{C}}$. On $\mathcal{Y}$ both endpoints lie in Ω and $e^{-V(x)}e^{-V(x+\nu(u))} \leq e^{-2d(\bar{m}-\eta)}$. Therefore, with $|\mathcal{Y}|$ the Lebesgue measure of $\mathcal{Y}$,

$$\int_{\mathbb{R}^c} \Phi_{\Omega}(u) du \geq |\mathcal{Y}| \geq e^{2d(\bar{m}-\eta)} I_{\mathbb{R}}^b I_{\mathbb{C}}^c \mathbb{P}(\mathcal{Y}) \geq \frac{1}{2} I_{\mathbb{R}}^b I_{\mathbb{C}}^c e^{2d(\bar{m}-\eta)}.$$

□

Proposition 5.26 (Geometric transfer). *Let $0 < \delta < 1$ and $C \in \mathbb{R}$. Let $(K_i/F_i)_{i \geq 1}$ be quadratic extensions satisfying (G1)–(G3) with a common λ and with $d_i = [F_i : \mathbb{Q}] \rightarrow \infty$, such that $\log L_{F_i}(1) \leq d_i C$ and such that every K_i/F_i has the same uniform local types $(e_r, f_r)_{r \in \mathcal{R}}$. Fix integers $k_r \geq 0$, let H and J be as in (5.5), and let $\mu = 2e^{H/2-\ell}$. Let $(f_{\mathbb{R}}, g_{\mathbb{C}})$ be admissible with Fourier constants (M, σ) satisfying the Fourier condition (5.19). Put*

$$(5.27) \quad \mathcal{M}(\theta) = J - \delta H - (1/2 - \delta)\ell - C + (1 - \delta) \log 2 + (1 - \theta) \log \pi + (1 - 2\theta)J_{\mathbb{R}} + \theta J_{\mathbb{C}}.$$

We call $\mathcal{M}(\theta)$ the margin. If $\inf_i \mathcal{M}(\theta_i) > 0$, where θ_i is the value of θ for F_i , then there are finite sets $U_i \subset \mathbb{R}^2$ with $|U_i| \rightarrow \infty$ and $u(U_i)/|U_i|^{1+\delta} \rightarrow \infty$.

Proof. The window. Let $m_{\mathbb{R}}, m_{\mathbb{C}}, \text{Var}_{\mathbb{R}}$ and $\text{Var}_{\mathbb{C}}$ be as in Lemma 5.25; the variances are finite by (P4). Fix $\eta > 0$ with $4\eta < \inf_i \mathcal{M}(\theta_i)$, and consider one extension K/F of the sequence, with d large. Take I, t and $\beta_1, \dots, \beta_t$ from Lemma 5.6, so that Λ_h is defined; the counts $n(h, y)$ and $\mathcal{E}(h, y)$ are those of the window Ω chosen next. With the total energy V and the mean $\bar{m}$ of Lemma 5.25, let

$$\Omega = \{x \in \mathbb{C}^d : V(x) \leq d(\bar{m} + \eta)\}.$$

By (P1) and (P3) (see the proof of Lemma 5.25), this is a bounded Borel set, and it is invariant under coordinate rotations because the profiles are radial in each coordinate. By Lemma 5.25,

$$\int_{\mathbb{R}^c} \Phi_{\Omega}(u) du \geq \frac{1}{2} I_{\mathbb{R}}^b I_{\mathbb{C}}^c e^{2d(\bar{m}-\eta)}$$

for all large d , uniformly in the signature. In particular $|\Omega| > 0$ for large d , so Ω is a window.

Counting points. With the product function $\Psi = \prod_v f_{\mathbb{R}}^p \prod_j g_{\mathbb{C}}^p = e^{-pV}$ of Lemma 5.24, we have $\mathbf{1}_{\Omega} \leq e^{pd(\bar{m}+\eta)} \Psi$, so

$$|\Omega| \leq e^{pd(\bar{m}+\eta)} A_{\mathbb{R}}^b A_{\mathbb{C}}^c,$$

and Lemmas 5.16, 5.18 and 5.24 give, for all (h, y) ,

$$n(h, y) \leq \frac{2e^{pd(\bar{m}+\eta)} A_{\mathbb{R}}^b A_{\mathbb{C}}^c}{\text{covol}(\Lambda_h)} = 2e^{dY_{\eta}}, \quad Y_{\eta} = H + \log 2 - \ell + (1 - 2\theta) \log A_{\mathbb{R}} + \theta \log A_{\mathbb{C}} + p(\bar{m} + \eta),$$

by (5.8), $b/d = 1 - 2\theta$ and $c/d = \theta$.

Counting edges. Now take a pair (h, y) from Lemma 5.13, applied with $n_{\max} = 2e^{dY_{\eta}}$. By $t \geq e^{dJ}/(\kappa h_{\text{rel}})$, Proposition 5.2, $\log L_F(1) \leq dC$ and $b + c = (1 - \theta)d$,

$$\frac{tw_K}{\text{Reg}^1} \geq \frac{e^{dJ} 2^{d-1} \pi^{b+c}}{\lambda^{d/2} L_F(1)} \geq \frac{1}{2} \exp(d[J + \log 2 + (1 - \theta) \log \pi - \ell/2 - C]).$$

Combined with the bounds for $|\Omega|$ and for the integral of Φ_{Ω} , (5.14) shows that the set $\mathcal{X} = \mathcal{X}(h, y)$ has $n = |\mathcal{X}| > 0$ points and at least $\frac{1}{4} e^{dX_{\eta}} n$ ordered edges, where

$$\begin{aligned} X_{\eta} &= J + \log 2 + (1 - \theta) \log \pi - \ell/2 - C + (1 - 2\theta)(\log I_{\mathbb{R}} - \log A_{\mathbb{R}}) \\ &\quad + \theta(\log I_{\mathbb{C}} - \log A_{\mathbb{C}}) + (2 - p)\bar{m} - (2 + p)\eta. \end{aligned}$$

Since $n \leq 2e^{dY_{\eta}}$ and $p(1 + \delta) = 2$, the terms in $\bar{m}$ cancel, and

$$\frac{\mathcal{E}(h, y)}{n^{1+\delta}} \geq \frac{e^{dX_{\eta}}}{4 \cdot 2^{\delta} e^{\delta dY_{\eta}}} = 2^{-2-\delta} e^{d(\mathcal{M}(\theta) - 4\eta)}.$$

The planar set. Finally let v_0 be a real place of F , and let $U = \{x_{v_0} : x \in \mathcal{X}\} \subset \mathbb{C} = \mathbb{R}^2$. By Lemma 5.15, $|U| = n$ and $u(U) \geq \mathcal{E}(h, y)/2$, so

$$\frac{u(U)}{|U|^{1+\delta}} \geq 2^{-3-\delta} e^{d(\mathcal{M}(\theta)-4\eta)},$$

which tends to infinity along the sequence. Since $u(U) \leq |U|^2/2$ and $\delta < 1$, also $|U| \rightarrow \infty$. These sets are the U_i . The conclusion concerns a sequence of cardinalities, not every large cardinality. $\square$

6. SHELL PROFILES AT SPLIT FINITE PLACES

We now place locally constant weights at finitely many finite places of F that split in K ; in Section 8 these are the places above 2, 3, 5, 7 and 29. In Lemma 5.6, the count at each prime of F above $r \in \mathcal{R}$ corresponds to the indicator function of a product of two balls in the completion, the unweighted shell profile of Definition 6.5; shell profiles replace this indicator by weighted sums of indicators of products of shells (Corollary 6.23). We keep the hypotheses (G1)–(G3) and the notation of Section 5, and put

$$\text{covol}_0 = \text{covol}((\mathcal{O}_K)_\infty) = (\lambda/2)^d.$$

6.1. The Local Functional. Let L be a nonarchimedean local field with valuation ring $\mathcal{O}$, uniformizer ϖ and residue field of cardinality Q . We use the additive Haar measure on L with $|\mathcal{O}| = 1$, the product measure on the plane $L^2 = L \times L$, and the multiplicative Haar measure $d\omega$ on $\mathcal{O}^\times$ of total measure one. For $n \in \mathbb{Z}$ and $\omega \in \mathcal{O}^\times$ put

$$s(n, \omega) = (\varpi^n \omega, \varpi^{-n} \omega^{-1}) \in L^2, \quad \mathcal{T}g(z) = \sum_{n \in \mathbb{Z}} \int_{\mathcal{O}^\times} g(z + s(n, \omega)) d\omega.$$

The two coordinates of $s(n, \omega)$ have product one; they model the finite coordinates of an element of relative norm one at a split place. If g_1 and g_2 are locally constant and compactly supported on L^2 , only finitely many n contribute to $\int_{L^2} g_1 \mathcal{T}g_2$: if $g_1(z)g_2(z + s(n, \omega)) \neq 0$, then both coordinates of $s(n, \omega)$ lie in the compact set $\text{supp } g_2 - \text{supp } g_1$, which bounds n from above and from below.

Definition 6.1. For locally constant, compactly supported functions g_1, g_2 on L^2 put $\langle g_1, g_2 \rangle_{\mathcal{T}} = \int_{L^2} g_1 \mathcal{T}g_2$. For a nonnegative, locally constant, compactly supported function g on L^2 with $g \neq 0$, and $0 < \delta < 1$, $p = 2/(1 + \delta)$, put

$$(6.2) \quad A(g) = \int_{L^2} g^p, \quad Z(g) = \langle g, g \rangle_{\mathcal{T}}, \quad \mathcal{F}_\delta(g) = \frac{Z(g)}{A(g)^{1+\delta}}.$$

We call $\mathcal{F}_\delta$ the *local functional*.

For $i \in \mathbb{Z}$ let $\mathcal{B}_i = \varpi^{-i} \mathcal{O}$, a ball of measure Q^i . Write $[x]_+ = \max(x, 0)$.

Lemma 6.3. For all integers i_1, j_1, i_2, j_2 ,

$$(6.4) \quad \langle \mathbf{1}_{\mathcal{B}_{i_1} \times \mathcal{B}_{j_1}}, \mathbf{1}_{\mathcal{B}_{i_2} \times \mathcal{B}_{j_2}} \rangle_{\mathcal{T}} = Q^{\min(i_1, i_2) + \min(j_1, j_2)} [\max(i_1, i_2) + \max(j_1, j_2) + 1]_+.$$

Proof. Two balls of an ultrametric space are disjoint or nested. Hence $\mathcal{B}_{i_1} \cap (\mathcal{B}_{i_2} - x)$ has measure $Q^{\min(i_1, i_2)}$ if $x \in \mathcal{B}_{\max(i_1, i_2)}$, and is empty otherwise. The left side of (6.4) is therefore $Q^{\min(i_1, i_2) + \min(j_1, j_2)}$ times the measure of the set of (n, ω) with $\varpi^n \omega \in \mathcal{B}_{\max(i_1, i_2)}$ and $\varpi^{-n} \omega^{-1} \in \mathcal{B}_{\max(j_1, j_2)}$. These conditions say $-\max(i_1, i_2) \leq n \leq \max(j_1, j_2)$ and do not involve ω , and $d\omega$ has total measure one. $\square$

Definition 6.5. Put $\mathcal{S}_0 = \mathcal{O}$ and $\mathcal{S}_i = \mathcal{B}_i \setminus \mathcal{B}_{i-1}$ for $i \geq 1$. These are the *shells*, and their measures $m_0 = 1$ and $m_i = Q^i - Q^{i-1}$ are the *shell measures*. Let $k \geq 0$ be an integer, and let $w = (w_{ij})_{i,j \geq 0}$

be nonnegative weights, finitely many of them nonzero, with $w_{00} > 0$. The *shell profile* with parameters (Q, k, w) on L^2 is

$$g = \sum_{i,j \geq 0} w_{ij} \mathbf{1}_{\mathcal{S}_i \times \varpi^{-k} \mathcal{S}_j}.$$

The shell profile with $w_{00} = 1$ and $w_{ij} = 0$ otherwise, that is, the indicator function of $\mathcal{O} \times \varpi^{-k} \mathcal{O}$, is the *unweighted shell profile* with parameters (Q, k) .

Lemma 6.6. *A shell profile g with parameters (Q, k, w) is nonnegative, locally constant and compactly supported. It is invariant under $(x, y) \mapsto (\omega x, \omega' y)$ for all $\omega, \omega' \in \mathcal{O}^\times$; in particular it is even. It is also invariant under translation by the group*

$$(6.7) \quad \mathcal{C} = \mathcal{O} \times \varpi^{-k} \mathcal{O}, \quad |\mathcal{C}| = Q^k.$$

Proof. The first assertion holds because the shells are compact open sets and finitely many of the nonnegative weights are nonzero. Multiplication by a unit preserves valuations and hence each shell. Adding an element of $\mathcal{O}$ does not change the shell of a point, whatever the number of shells; this gives the invariance under $\mathcal{C}$, applied to the first coordinate and to ϖ^k times the second. $\square$

We call $\mathcal{C}$ the *period* of g . Define the symmetric matrix $\Delta = (\Delta_{ii'})_{i,i' \geq 0}$ by

$$\Delta_{ii'} = m_{\min(i,i')} \quad (i \neq i'), \quad \Delta_{00} = 0, \quad \Delta_{ii} = im_i - Q^{i-1} \quad (i \geq 1),$$

and the matrix $\mathcal{G}$ by

$$\mathcal{G}_{(i,j),(i',j')} = (k+1)m_i m_j \mathbf{1}_{i=i', j=j'} + m_j \Delta_{ii'} \mathbf{1}_{j=j'} + m_i \Delta_{jj'} \mathbf{1}_{i=i'}.$$

Lemma 6.8. *The shell profile g with parameters (Q, k, w) satisfies*

$$(6.9) \quad A(g) = Q^k \sum_{i,j} m_i m_j w_{ij}^p, \quad Z(g) = Q^k \sum_{(i,j),(i',j')} w_{ij} \mathcal{G}_{(i,j),(i',j')} w_{i'j'}.$$

All entries of $\mathcal{G}$ are nonnegative, and $Z(g) \geq (k+1)Q^k w_{00}^2 > 0$. In particular $\mathcal{F}_\delta(g)$ depends only on the parameters, and the unweighted shell profile has $\mathcal{F}_\delta(g) = (k+1)Q^{-\delta k}$.

Proof. The formula for $A(g)$ holds because the sets $\mathcal{S}_i \times \varpi^{-k} \mathcal{S}_j$ are disjoint of measure $Q^k m_i m_j$. For $Z(g)$, write $\mathbf{1}_{\mathcal{S}_0} = \mathbf{1}_{\mathcal{B}_0}$ and $\mathbf{1}_{\mathcal{S}_i} = \mathbf{1}_{\mathcal{B}_i} - \mathbf{1}_{\mathcal{B}_{i-1}}$ for $i \geq 1$, and note $\varpi^{-k} \mathcal{B}_j = \mathcal{B}_{j+k}$. Only balls with nonnegative indices occur, so by (6.4) and $k \geq 0$ the positive part can be dropped, and $\langle \mathbf{1}_{\mathcal{B}_{i_1} \times \mathcal{B}_{j_1+k}}, \mathbf{1}_{\mathcal{B}_{i_2} \times \mathcal{B}_{j_2+k}} \rangle_{\mathcal{T}}$, for $i_1, j_1, i_2, j_2 \geq 0$, is

$$Q^k [(k+1)Q^{\min(i_1,i_2)} Q^{\min(j_1,j_2)} + \max(i_1, i_2) Q^{\min(i_1,i_2)} Q^{\min(j_1,j_2)} + Q^{\min(i_1,i_2)} \max(j_1, j_2) Q^{\min(j_1,j_2)}].$$

For a function φ of two nonnegative integers put $(\partial\varphi)(i, i') = \varphi(i, i') - \varphi(i-1, i') - \varphi(i, i'-1) + \varphi(i-1, i'-1)$, where terms with an index -1 are omitted; this is the expansion of the shells into balls. Apply ∂ in (i_1, i_2) and in (j_1, j_2) . A direct computation gives, for $i, i' \geq 0$, that $\partial Q^{\min(i_1,i_2)}$ at (i, i') is $m_i \mathbf{1}_{i=i'}$, and that $\partial(\max(i_1, i_2) Q^{\min(i_1,i_2)})$ is $\Delta_{ii'}$. For example, when $1 \leq i < i'$ the latter is $i'Q^i - i'Q^{i-1} - (i'-1)Q^i + (i'-1)Q^{i-1} = m_i$, and when $i = i' \geq 1$ it is $iQ^i - 2iQ^{i-1} + (i-1)Q^{i-1} = im_i - Q^{i-1}$. This gives $\langle \mathbf{1}_{\mathcal{S}_i \times \varpi^{-k} \mathcal{S}_j}, \mathbf{1}_{\mathcal{S}_{i'} \times \varpi^{-k} \mathcal{S}_{j'}} \rangle_{\mathcal{T}} = Q^k \mathcal{G}_{(i,j),(i',j')}$, and hence the formula for $Z(g)$. All entries of $\mathcal{G}$ are nonnegative, since $\Delta_{ii} = Q^{i-1}(iQ - i - 1) \geq 0$ for $i \geq 1$; as $\mathcal{G}_{(0,0),(0,0)} = k+1$, this gives $Z(g) \geq (k+1)Q^k w_{00}^2$. For the unweighted shell profile only $\mathcal{G}_{(0,0),(0,0)} = k+1$ contributes. $\square$

By Lemma 6.8, a shell profile g has $Z(g) > 0$, so $g(z)g(z+s(n, \omega))/Z(g)$ is a probability density on $L^2 \times \mathbb{Z} \times \mathcal{O}^\times$, with counting measure on $\mathbb{Z}$. As at the archimedean places (Definition 5.22), we call it the *endpoint law* of g ; its first endpoint is z and its second endpoint is $z + s(n, \omega)$.

Corollary 6.10. *Let $x = (x_i)_{i \geq 0}$ and $x' = (x'_j)_{j \geq 0}$ be finitely supported vectors of nonnegative numbers with $x_0 x'_0 > 0$, put*

$$P_x = \sum_i m_i x_i^p, \quad S_x = \sum_i m_i x_i^2, \quad R_x = \sum_{i,i'} x_i \Delta_{ii'} x_{i'},$$

and define $P_{x'}, S_{x'}, R_{x'}$ in the same way. The shell profile g with parameters (Q, k, w) and product weights $w_{ij} = x_i x'_j$ satisfies

$$(6.11) \quad A(g) = Q^k P_x P_{x'}, \quad Z(g) = Q^k [(k+1)S_x S_{x'} + R_x S_{x'} + S_x R_{x'}].$$

Proof. Substitute $w_{ij} = x_i x'_j$ in (6.9). □

Remark 6.12. Suppose that only $\mathcal{S}_0$ and $\mathcal{S}_1$ carry weight, with $x = x' = (1, t)$ and $t \geq 0$. Then $S_x = 1 + (Q-1)t^2$ and $R_x = 2t + (Q-2)t^2$, and the difference between $\log \mathcal{F}_\delta(g)$ and the value $\log((k+1)Q^{-\delta k})$ of the unweighted shell profile is

$$(6.13) \quad \log \frac{(k+1)S_x^2 + 2S_x R_x}{k+1} - 2(1+\delta) \log(1 + (Q-1)t^p).$$

Since $p > 1$, its right derivative at $t = 0$ is $4/(k+1) > 0$, so a sufficiently small weight on $\mathcal{S}_1$ always improves on the unweighted shell profile.

Section 8 uses the exact formulas (6.11).

6.2. Finite Periods and Lattice Counting. Let $\mathcal{P}$ be a finite set of finite places of F that split in K . For $\mathfrak{p} \in \mathcal{P}$ write $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_{\mathfrak{p}} \iota \mathfrak{P}_{\mathfrak{p}}$, where we also write $\mathfrak{p}$ for the prime ideal of F . The completion of K at $\mathfrak{P}_{\mathfrak{p}}$ is $F_{\mathfrak{p}}$; for $x \in K$ let $x_{\mathfrak{p}} \in F_{\mathfrak{p}}$ be its image under the completion map. The map $x \mapsto (x_{\mathfrak{p}}, (\iota x)_{\mathfrak{p}})$ records the completions at $\mathfrak{P}_{\mathfrak{p}}$ and at $\iota \mathfrak{P}_{\mathfrak{p}}$, and ι exchanges the two coordinates. If $N_{K/F}\beta = 1$, then $\beta_{\mathfrak{p}}(\iota\beta)_{\mathfrak{p}} = 1$. Let $\mathcal{O}_{\mathfrak{p}}$, $\varpi_{\mathfrak{p}}$ and $Q_{\mathfrak{p}}$ be the valuation ring, a uniformizer and the residue cardinality of $F_{\mathfrak{p}}$.

Definition 6.14. Put

$$\mathbb{A}_{\mathcal{P}} = \prod_{\mathfrak{p} \in \mathcal{P}} (F_{\mathfrak{p}} \times F_{\mathfrak{p}}),$$

with the Haar measure that gives $\prod_{\mathfrak{p}} (\mathcal{O}_{\mathfrak{p}} \times \mathcal{O}_{\mathfrak{p}})$ measure one. For a point (z, ζ) of $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ we call z its *archimedean part* and ζ its *finite part*. Let $\Gamma = \mathcal{O}_{K, \mathcal{P}}$ be the ring of elements of K that are integral at every prime other than the $\mathfrak{P}_{\mathfrak{p}}$ and $\iota \mathfrak{P}_{\mathfrak{p}}$. We embed Γ in $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ by $\gamma \mapsto (\gamma_{\infty}, \gamma_f)$, where $\gamma_f = (\gamma_{\mathfrak{p}}, (\iota\gamma)_{\mathfrak{p}})_{\mathfrak{p}}$; thus γ_{∞} and γ_f are the archimedean part and the finite part of the image of γ . A subgroup of $\mathbb{A}_{\mathcal{P}}$ of the form

$$\mathcal{C}_f = \prod_{\mathfrak{p} \in \mathcal{P}} (\varpi_{\mathfrak{p}}^{a_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}} \times \varpi_{\mathfrak{p}}^{b_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}), \quad a_{\mathfrak{p}}, b_{\mathfrak{p}} \in \mathbb{Z},$$

is called *rectangular*.

A rectangular group has measure $|\mathcal{C}_f| = \prod_{\mathfrak{p}} Q_{\mathfrak{p}}^{-a_{\mathfrak{p}} - b_{\mathfrak{p}}}$.

Lemma 6.15. *Let $\mathcal{C}_f$ be rectangular and put $\mathfrak{L} = \prod_{\mathfrak{p}} \mathfrak{P}_{\mathfrak{p}}^{a_{\mathfrak{p}}} (\iota \mathfrak{P}_{\mathfrak{p}})^{b_{\mathfrak{p}}}$.*

- (a) *The elements $\gamma \in \Gamma$ with $\gamma_f \in \mathcal{C}_f$ form $\mathfrak{L}$, and $N\mathfrak{L} = |\mathcal{C}_f|^{-1}$, so $\text{covol}(\mathfrak{L}_{\infty}) = \text{covol}_0 / |\mathcal{C}_f|$.*
- (b) *Every coset of $\mathcal{C}_f$ in $\mathbb{A}_{\mathcal{P}}$ contains γ_f for some $\gamma \in \Gamma$.*
- (c) *Γ is a lattice in $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$, that is, a discrete subgroup with a fundamental domain of finite measure. If $P_{\mathfrak{L}}$ is a fundamental parallelepiped of $\mathfrak{L}_{\infty}$, then $P_{\mathfrak{L}} \times \mathcal{C}_f$ is a fundamental domain for Γ , of measure covol_0 .*
- (d) *For $h \in \mathbb{R}^c$, the set $\Gamma_h = \{(W_h \gamma_{\infty}, \gamma_f) : \gamma \in \Gamma\}$ is again a lattice, with fundamental domain $W_h P_{\mathfrak{L}} \times \mathcal{C}_f$ of measure covol_0 . Put $H_f = d^{-1} \log |\mathcal{C}_f|$. Every nonzero vector ξ of the dual lattice of $W_h \mathfrak{L}_{\infty}$ satisfies $\prod_w |\xi_w| \geq \mu_f^d$, where $\mu_f = 2e^{H_f/2-\ell}$.*

Proof. (a) The valuation of γ_p is the exponent of $\mathfrak{P}_p$ in γ , and that of $(\iota\gamma)_p$ is the exponent of $\iota\mathfrak{P}_p$. Together with integrality at the other primes, $\gamma_f \in \mathcal{C}_f$ says exactly that $\gamma \in \mathfrak{L}$. As $N\mathfrak{P}_p = N(\iota\mathfrak{P}_p) = Q_p$, we get $N\mathfrak{L} = \prod_p Q_p^{a_p+b_p} = |\mathcal{C}_f|^{-1}$, and the covolume follows from the covolume formula (5.7).

(b) Choose $\tilde{a}_p \leq a_p$ and $\tilde{b}_p \leq b_p$ such that the given coset lies in $\tilde{\mathcal{C}}_f = \prod_p (\varpi_p^{\tilde{a}_p} \mathcal{O}_p \times \varpi_p^{\tilde{b}_p} \mathcal{O}_p)$, and let $\tilde{\mathfrak{L}} \supset \mathfrak{L}$ be the corresponding ideal. The map $\gamma \mapsto \gamma_f$ induces a homomorphism $\tilde{\mathfrak{L}}/\mathfrak{L} \rightarrow \tilde{\mathcal{C}}_f/\mathcal{C}_f$. It is injective by (a), applied to $\mathcal{C}_f$. Both groups are finite of the same order: $|\tilde{\mathcal{C}}_f/\mathcal{C}_f| = |\tilde{\mathcal{C}}_f|/|\mathcal{C}_f|$, and $|\tilde{\mathfrak{L}}/\mathfrak{L}| = N\mathfrak{L}/N\tilde{\mathfrak{L}}$ [18, Proposition 4.2], which is the same number by (a). So the map is bijective, and every coset of $\mathcal{C}_f$ in $\tilde{\mathcal{C}}_f$ contains γ_f for some $\gamma \in \tilde{\mathfrak{L}} \subset \Gamma$. No principality is needed.

(c) Given $(z, \zeta) \in \mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$, by (b) there is $\gamma \in \Gamma$ with $\zeta - \gamma_f \in \mathcal{C}_f$, and then a unique $\gamma' \in \mathfrak{L}$ with $z - (\gamma + \gamma')_{\infty} \in P_{\mathfrak{L}}$. If (z, ζ) had two such representations, the difference of the two elements of Γ would have finite part in $\mathcal{C}_f$, hence lie in $\mathfrak{L}$ by (a), and then it would vanish because $P_{\mathfrak{L}}$ is a fundamental domain. Thus $P_{\mathfrak{L}} \times \mathcal{C}_f$ is a fundamental domain, of measure $(\text{covol}_0/|\mathcal{C}_f|) \cdot |\mathcal{C}_f| = \text{covol}_0$. Finally Γ is discrete: for a bounded open set $Y \ni 0$ in $\mathbb{C}^d$, its intersection with the neighborhood $Y \times \mathcal{C}_f$ of 0 consists of the finitely many $\gamma \in \mathfrak{L}$ with $\gamma_{\infty} \in Y$.

(d) The map $(z, \zeta) \mapsto (W_h z, \zeta)$ preserves measure, because W_h is real diagonal of determinant one, and it carries Γ to Γ_h and $P_{\mathfrak{L}} \times \mathcal{C}_f$ to $W_h P_{\mathfrak{L}} \times \mathcal{C}_f$; so the first assertion follows from (c). By (a), $N\mathfrak{L} = e^{-dH_f}$, and Lemma 5.16 gives the bound for the dual vectors. $\square$

Accordingly, the Fourier condition used in this section is

$$(6.16) \quad \sigma \cdot 2e^{H_f/2-\ell} \geq \log M + 2 \log 5 + 2.$$

Lemma 6.17. *Let $(f_{\mathbb{R}}, g_{\mathbb{C}})$ be admissible with Fourier constants (M, σ) , and let $\Psi_{\infty} = \prod_v f_{\mathbb{R}}^p \prod_j g_{\mathbb{C}}^p$ on $\mathbb{C}^d$, with one factor for each real place v and each complex place j of F (Lemma 5.24). Let $\Psi_f \geq 0$ be a function on $\mathbb{A}_{\mathcal{P}}$ that is invariant under translation by a rectangular group $\mathcal{C}_f$ and vanishes outside a finite union of its cosets. If (6.16) holds, with H_f defined by this $\mathcal{C}_f$, then for every $h \in \mathbb{R}^c$ and every $z_0 \in \mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ (a point of the whole space, not an archimedean part),*

$$(6.18) \quad \sum_{(z, \zeta) \in \Gamma_h + z_0} \Psi_{\infty}(z) \Psi_f(\zeta) \leq \frac{2}{\text{covol}_0} \int \Psi_{\infty} \int \Psi_f.$$

Proof. Group the points by the coset of $\mathcal{C}_f$ containing their finite part. If two points of $\Gamma_h + z_0$ have finite parts in the same coset, their difference comes from an element of $\mathfrak{L}$, by Lemma 6.15(a). So the archimedean parts of the points in one coset form a translate of $W_h \mathfrak{L}_{\infty}$, or the empty set. By Lemma 5.18, with the dual bound of Lemma 6.15(d) and the Fourier bound for Ψ_{∞} of Lemma 5.24, the sum of Ψ_{∞} over such a translate is at most $2|\mathcal{C}_f| \int \Psi_{\infty} / \text{covol}_0$. The values of Ψ_f on its finitely many nonzero cosets sum to $\int \Psi_f / |\mathcal{C}_f|$. $\square$

Remark 6.19. Let $\alpha \in \mathbb{A}_{\mathcal{P}}$ have coordinates $(\varpi_p^{n_p}, \varpi_p^{-n_p})$. Multiplication by α preserves the Haar measure, and for a rectangular group $\mathcal{C}_f$ the group $\alpha\mathcal{C}_f$ is rectangular, of the same measure. Hence, if Ψ_f satisfies the hypotheses of Lemma 6.17 with $\mathcal{C}_f$, then $\Psi_f \circ \alpha$ satisfies them with the rectangular group $\alpha^{-1}\mathcal{C}_f$, which gives the same H_f , and $\int \Psi_f \circ \alpha = \int \Psi_f$.

6.3. Class Selection. For $u \in \mathbb{R}^c$ and $n = (n_p) \in \mathbb{Z}^P$ let $\nu(u, n) \in \mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ have archimedean part $\nu(u)$ and finite part $(\varpi_p^{n_p}, \varpi_p^{-n_p})_p$.

Lemma 6.20. *Let $\mathcal{N} \subset \mathbb{Z}^P$ be finite, and let $\mathcal{W}: \mathcal{N} \rightarrow [0, \infty)$ have positive sum. There are a subset $\mathcal{N}' \subset \mathcal{N}$ with*

$$\sum_{n \in \mathcal{N}'} \mathcal{W}(n) \geq \frac{1}{\kappa h_{\text{rel}}} \sum_{n \in \mathcal{N}} \mathcal{W}(n),$$

an element $n_0 \in \mathcal{N}'$ with $\mathcal{W}(n_0) > 0$, and elements $\beta_n \in \Gamma$, for $n \in \mathcal{N}'$, with $N_{K/F}\beta_n = 1$ and

$$\beta_n \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{P}_{\mathfrak{p}}^{n_{\mathfrak{p}} - n_{0,\mathfrak{p}}} (\iota \mathfrak{P}_{\mathfrak{p}})^{-(n_{\mathfrak{p}} - n_{0,\mathfrak{p}})}.$$

The cosets $\beta_n \mathcal{O}_K^1$ are pairwise disjoint, and $\beta_n \mathcal{O}_K^1$ is the set of all elements of relative norm one that generate this ideal. Moreover, let $\varpi_0 \in \mathbb{A}_{\mathcal{P}}$ have coordinates $(\varpi_{\mathfrak{p}}^{n_{0,\mathfrak{p}}}, \varpi_{\mathfrak{p}}^{-n_{0,\mathfrak{p}}})$. Then for $n \in \mathcal{N}'$ and $\beta \in \beta_n \mathcal{O}_K^1$, the point $\varpi_0 \beta_f$ has coordinates $(\varpi_{\mathfrak{p}}^{n_{\mathfrak{p}}} \omega_{\mathfrak{p}}, \varpi_{\mathfrak{p}}^{-n_{\mathfrak{p}}} \omega_{\mathfrak{p}}^{-1})$ with units $\omega_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times}$.

Proof. Map n to the class of $\mathfrak{A}(n) = \prod_{\mathfrak{p}} \mathfrak{P}_{\mathfrak{p}}^{n_{\mathfrak{p}}}$ in $\text{Cl}(K)$ modulo the image of $\text{Cl}(F)$, a group of order κh_{rel} . Let $\mathcal{N}'$ be a fiber on which the sum of $\mathcal{W}$ is largest; this sum is positive, so we can choose $n_0 \in \mathcal{N}'$ with $\mathcal{W}(n_0) > 0$. For $n \in \mathcal{N}'$ write $\mathfrak{A}(n)\mathfrak{A}(n_0)^{-1} = x_n \mathfrak{a}_n \mathcal{O}_K$ with $x_n \in K^{\times}$ and $\mathfrak{a}_n$ a fractional ideal of F , and put $\beta_n = x_n / \iota x_n$. As in the proof of Lemma 5.6, $N_{K/F}\beta_n = 1$ and β_n generates the displayed ideal, which is supported on the primes $\mathfrak{P}_{\mathfrak{p}}, \iota \mathfrak{P}_{\mathfrak{p}}$; hence $\beta_n \in \Gamma$. Two elements of relative norm one generating the same ideal differ by an element of $\mathcal{O}_K^1$, and distinct $n \in \mathcal{N}'$ give distinct ideals. Finally, if $\beta \in \beta_n \mathcal{O}_K^1$, then $\beta_{\mathfrak{p}}$ has valuation $n_{\mathfrak{p}} - n_{0,\mathfrak{p}}$ and $(\iota \beta)_{\mathfrak{p}} = \beta_{\mathfrak{p}}^{-1}$, which gives the last assertion. $\square$

6.4. Transfer with Shell Profiles.

Proposition 6.21 (Transfer with shell profiles). *Let $0 < \delta < 1$ and $C \in \mathbb{R}$. Let $(K_j/F_j)_{j \geq 1}$ be quadratic extensions satisfying (G1)–(G3) with a common λ , with $d_j = [F_j : \mathbb{Q}] \rightarrow \infty$ and $\log L_{F_j}(1) \leq d_j C$. For each j let $\mathcal{P}_j$ be a finite set of finite places of F_j that split in K_j , and for $\mathfrak{p} \in \mathcal{P}_j$ let $g_{\mathfrak{p}}$ be a shell profile on $F_{\mathfrak{p}}^2$ with parameters $(Q_{\mathfrak{p}}, k_{\mathfrak{p}}, w^{(\mathfrak{p})})$, where the parameters range over a fixed finite set independent of j . Let $\mathcal{F}_{\delta,\mathfrak{p}} = \mathcal{F}_{\delta}(g_{\mathfrak{p}})$, let $(f_{\mathbb{R}}, g_{\mathbb{C}})$ be admissible with Fourier constants (M, σ) , and suppose that (6.16) holds for every j , with $\mathcal{C}_f = \prod_{\mathfrak{p} \in \mathcal{P}_j} (\mathcal{O}_{\mathfrak{p}} \times \varpi_{\mathfrak{p}}^{-k_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}})$ the product of the periods of the $g_{\mathfrak{p}}$, that is, with $H_f = d_j^{-1} \sum_{\mathfrak{p} \in \mathcal{P}_j} k_{\mathfrak{p}} \log Q_{\mathfrak{p}}$. Let θ_j be the value of θ for F_j , and put*

$$(6.22) \quad \begin{aligned} \mathcal{M}_{\text{fin},j} &= \frac{1}{d_j} \sum_{\mathfrak{p} \in \mathcal{P}_j} \log \mathcal{F}_{\delta,\mathfrak{p}} - (1/2 - \delta)\ell - C + (1 - \delta) \log 2 + (1 - \theta_j) \log \pi \\ &\quad + (1 - 2\theta_j)J_{\mathbb{R}} + \theta_j J_{\mathbb{C}}; \end{aligned}$$

we call $\mathcal{M}_{\text{fin},j}$ the margin of K_j/F_j with these shell profiles. If $\inf_j \mathcal{M}_{\text{fin},j} > 0$, then there are finite sets $U_j \subset \mathbb{R}^2$ with $|U_j| \rightarrow \infty$ and $u(U_j)/|U_j|^{1+\delta} \rightarrow \infty$.

Compared with (5.27), the margin (6.22) has no separate term $-\delta H$: by (6.9), each $\mathcal{F}_{\delta,\mathfrak{p}}$ contains the factor $Q_{\mathfrak{p}}^{-\delta k_{\mathfrak{p}}}$, and Corollary 6.23 shows that for uniform local types and unweighted shell profiles (6.22) reduces to (5.27).

Proof of Proposition 6.21. Fix $\eta > 0$ with $4\eta < \inf_j \mathcal{M}_{\text{fin},j}$, and consider one extension K/F of the sequence, with d large. We drop the sequence index j and write $\mathcal{M}_{\text{fin}}$ for the margin of K/F ; below, j indexes the complex places of F .

The profile and the probability measure. On $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ let $f = \prod_v f_{\mathbb{R}} \prod_{j=1}^c g_{\mathbb{C}} \prod_{\mathfrak{p} \in \mathcal{P}} g_{\mathfrak{p}}$, with one factor for each real place v of F , each complex place j of F and each $\mathfrak{p} \in \mathcal{P}$, let $V = -\log f$ on the set where $f > 0$, and put

$$A = \int f^p = A_{\mathbb{R}}^b A_{\mathbb{C}}^c \prod_{\mathfrak{p} \in \mathcal{P}} A(g_{\mathfrak{p}}), \quad Z = I_{\mathbb{R}}^b I_{\mathbb{C}}^c \prod_{\mathfrak{p} \in \mathcal{P}} Z(g_{\mathfrak{p}}).$$

Besides the points $\nu(u, n)$ defined before Lemma 6.20, let $\nu(u, n, \omega)$, for $\omega = (\omega_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times}$, have archimedean part $\nu(u)$ and finite part $(\varpi_{\mathfrak{p}}^{n_{\mathfrak{p}}} \omega_{\mathfrak{p}}, \varpi_{\mathfrak{p}}^{-n_{\mathfrak{p}}} \omega_{\mathfrak{p}}^{-1})_{\mathfrak{p}}$. Let $\mathbb{P}$ be the probability measure on $(\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}) \times \mathbb{R}^c \times \mathbb{Z}^{\mathcal{P}} \times \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times}$ with density $f(x)f(x + \nu(u, n, \omega))/Z$ with respect to $dx du d\omega$ and

counting measure in n , where $d\omega$ is the Haar probability measure. It is the product of the endpoint laws of the archimedean blocks (Definition 5.22) and of the endpoint laws of the g_p . Its endpoints are x and $x + \nu(u, n, \omega)$. Their energies $V(x)$ and $V(x + \nu(u, n, \omega))$ have the same distribution and are sums of independent terms, one for each block and each $\mathfrak{p} \in \mathcal{P}$: at the archimedean blocks this is shown in the proof of Lemma 5.25, and at $\mathfrak{p} \in \mathcal{P}$ the map $(z, n, \omega) \mapsto (-z - s(n, \omega), n, \omega)$ preserves the endpoint law of g_p and carries its first endpoint to minus the second, g_p is even, and the energy $-\log g_p$ of the first endpoint takes finitely many values. Let $d\bar{m}$ be their common mean; this $\bar{m}$ includes the places of $\mathcal{P}$ and is not the $\bar{m}$ of Lemma 5.25. The Q_p take finitely many values, since the parameters of the shell profiles do, and each is a power of the residue characteristic of $\mathfrak{p}$; so these characteristics lie in a fixed finite set, and $|\mathcal{P}| = O(d)$. Since the parameters range over a finite set, the variance of either energy is $O(d)$. Let χ be the indicator of the event that both energies lie in $[d(\bar{m} - \eta), d(\bar{m} + \eta)]$. By Chebyshev's inequality, as in the proof of Lemma 5.25, $\mathbb{P}(\chi = 1) \geq 1/2$ for large d .

The set Ω . Let Ω be the set of points of $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ where $f > 0$ and $V \leq d(\bar{m} + \eta)$; it plays the role of the window of Definition 5.11. It is a bounded Borel set: the archimedean energies are coercive and bounded below, and the finite part lies in the compact support of $\prod_p g_p$, on which the finite energies are bounded. It is invariant under rotations of the archimedean coordinates, and, by Lemma 6.6, under $(x_p, y_p) \mapsto (\omega x_p, \omega' y_p)$ for units at each $\mathfrak{p} \in \mathcal{P}$ and under translation by $\mathcal{C}_f$. For $u \in \mathbb{R}^c$ and $n \in \mathbb{Z}^{\mathcal{P}}$ let $\Phi(u, n) = |\Omega \cap (\Omega - \nu(u, n))|$, and let $\mathcal{W}(n) = \int_{\mathbb{R}^c} \Phi(u, n) du$. Only finitely many n have $\mathcal{W}(n) \neq 0$. By these invariances, the measure of the intersection of Ω with its translate by any vector whose archimedean part has the moduli of $\nu(u)$ and whose finite part is that of some $\nu(u, n, \omega)$ equals $\Phi(u, n)$. Where $\chi = 1$, both endpoints lie in Ω and $f(x)f(x + \nu(u, n, \omega)) \leq e^{-2d(\bar{m} - \eta)}$. Integrating over x, u and ω and summing over n , we obtain

$$\begin{aligned} \sum_n \mathcal{W}(n) &= \sum_n \int \mathbf{1}_{\Omega}(x) \mathbf{1}_{\Omega}(x + \nu(u, n, \omega)) dx du d\omega \\ &\geq e^{2d(\bar{m} - \eta)} \sum_n \int \chi f(x) f(x + \nu(u, n, \omega)) dx du d\omega = e^{2d(\bar{m} - \eta)} Z \mathbb{P}(\chi = 1) \geq \frac{1}{2} Z e^{2d(\bar{m} - \eta)}. \end{aligned}$$

Moreover $\mathbf{1}_{\Omega} \leq e^{pd(\bar{m} + \eta)} f^p$, so $|\Omega| \leq A e^{pd(\bar{m} + \eta)}$.

Class selection and rescaling. Apply Lemma 6.20 to the finitely many n with $\mathcal{W}(n) > 0$, obtaining $n_0, \mathcal{N}'$ and β_n , and let ϖ_0 be as in that lemma. Put $\Omega' = \varpi_0^{-1}\Omega$, where ϖ_0 acts on the finite part. Then $|\Omega'| = |\Omega|$, and Ω' is invariant under the rectangular group $\mathcal{C}'_f = \varpi_0^{-1}\mathcal{C}_f$, of measure $|\mathcal{C}'_f|$. For $n \in \mathcal{N}'$, $\beta \in \beta_n \mathcal{O}_K^1$ and $h \in \mathbb{R}^c$, the element $\beta^{(h)} = (W_h \beta_{\infty}, \beta_f) \in \Gamma_h$ satisfies

$$|\Omega' \cap (\Omega' - \beta^{(h)})| = |\Omega \cap (\Omega - (W_h \beta_{\infty}, \varpi_0 \beta_f))| = \Phi(l(\beta) - h, n),$$

by the last assertion of Lemma 6.20 and the invariances of Ω , as in Lemma 5.12.

Points and edges. Let $\mathfrak{L}'$ be the ideal attached to $\mathcal{C}'_f$ in Lemma 6.15. Fix a $\mathbb{Z}$ -basis of $\mathfrak{L}'_{\infty}$, let $P_{\mathfrak{L}'}$ be the fundamental parallelepiped that it spans, and for $y \in [0, 1)^{2d}$ let $y_{\mathfrak{L}'}$ be the point with coordinate vector y in this basis. For $h \in \mathbb{R}^c$, $y \in [0, 1)^{2d}$ and $\zeta \in \mathcal{C}'_f$ put $z_0 = (W_h y_{\mathfrak{L}'}, \zeta)$; these points form the fundamental domain $W_h P_{\mathfrak{L}'} \times \mathcal{C}'_f$ of Γ_h of Lemma 6.15(d). Let $\mathcal{X}(h, z_0) = (\Gamma_h + z_0) \cap \Omega'$ and let $N(h, z_0) = |\mathcal{X}(h, z_0)|$ be the number of its points (the analogue of the count $n(h, y)$ of Section 5), and let $\mathcal{E}(h, z_0)$ count the pairs (x, β) with $x \in \mathcal{X}(h, z_0)$, $\beta \in \bigcup_{n \in \mathcal{N}'} \beta_n \mathcal{O}_K^1$ and $x + \beta^{(h)} \in \Omega'$. Averages over (h, z_0) are taken with respect to the probability measure $dh dy d\zeta / (\text{Reg}^1 |\mathcal{C}'_f|)$ on $\Pi^1 \times [0, 1)^{2d} \times \mathcal{C}'_f$. Since $\mathbf{1}_{\Omega'} \leq e^{pd(\bar{m} + \eta)} (f \circ \varpi_0)^p$ and $(f \circ \varpi_0)^p$ is the product of an archimedean factor and a function invariant under $\mathcal{C}'_f$, Lemma 6.17 and Remark 6.19 give

$$N(h, z_0) \leq N_{\max} = \frac{2A e^{pd(\bar{m} + \eta)}}{\text{covol}_0}$$

for all (h, z_0) . By tiling, for fixed h the average of $N(h, z_0)$ over (y, ζ) is $|\Omega'|/\text{covol}_0$, and the average of $\mathcal{E}(h, z_0)$ is $\text{covol}_0^{-1} \sum_{n \in \mathcal{N}'} \sum_{\beta \in \beta_n \cap \mathcal{O}_K^1} \Phi(l(\beta) - h, n)$. Averaging over $h \in \Pi^1$ as in Lemma 5.9, the average of $\mathcal{E}$ becomes

$$\frac{w_K}{\text{Reg}^1 \text{covol}_0} \sum_{n \in \mathcal{N}'} \mathcal{W}(n) \geq \frac{w_K}{\kappa h_{\text{rel}} \text{Reg}^1 \text{covol}_0} \sum_n \mathcal{W}(n).$$

Measurability and integrability hold as in Lemma 5.13, since $\mathcal{E} \leq N^2 \leq N_{\text{max}}^2$. The argument of that lemma yields a pair (h, z_0) with $N = N(h, z_0) > 0$ and

$$\frac{\mathcal{E}(h, z_0)}{N} \geq \frac{w_K}{\kappa h_{\text{rel}} \text{Reg}^1} \frac{\sum_n \mathcal{W}(n)}{|\Omega|} \geq \frac{w_K}{\kappa h_{\text{rel}} \text{Reg}^1} \frac{Z e^{2d(\bar{m}-\eta)}}{2A e^{pd(\bar{m}+\eta)}}.$$

With $N \leq N_{\text{max}}$ and $p(1+\delta) = 2$,

$$\frac{\mathcal{E}(h, z_0)}{N^{1+\delta}} \geq \frac{w_K \text{covol}_0^\delta}{2^{1+\delta} \kappa h_{\text{rel}} \text{Reg}^1} \frac{Z}{A^{1+\delta}} e^{-4\eta d}.$$

By (5.3) and $\log L_F(1) \leq dC$, the first factor is at least $2^{-2-\delta} 2^{d(1-\delta)} \pi^{(1-\theta)d} \lambda^{-(1/2-\delta)d} e^{-dC}$, and $Z/A^{1+\delta} = \exp(bJ_{\mathbb{R}} + cJ_{\mathbb{C}} + \sum_{\mathfrak{p}} \log \mathcal{F}_{\delta, \mathfrak{p}})$. Hence $\mathcal{E}/N^{1+\delta} \geq 2^{-2-\delta} e^{d(\mathcal{M}_{\text{fin}} - 4\eta)}$.

The planar set. Let v_0 be a real place of F and let U be the set of v_0 -coordinates of the points of $\mathcal{X}(h, z_0)$. Distinct points differ by $(W_h \gamma_\infty, \gamma_f)$ with $0 \neq \gamma \in \Gamma$, whose v_0 -coordinate is nonzero, so $|U| = N$. Each counted pair (x, β) gives two points at distance $|\phi_{v_0}(\beta)| = 1$, and distinct pairs give distinct ordered pairs of points. As in the proof of Proposition 5.26 (Lemma 5.15), $u(U) \geq \mathcal{E}/2$, the ratio $u(U)/|U|^{1+\delta}$ tends to infinity, and the bound $u(U) \leq |U|^2/2$ forces $|U| \rightarrow \infty$. $\square$

6.5. Uniform Local Types.

Corollary 6.23 (Uniform local types). *Let $0 < \delta < 1$ and $C \in \mathbb{R}$. Let $(K_j/F_j)_{j \geq 1}$ be quadratic extensions satisfying (G1)–(G3) with a common λ , with $d_j = [F_j : \mathbb{Q}] \rightarrow \infty$ and $\log L_{F_j}(1) \leq d_j C$, and with the same uniform local types $(e_r, f_r)_{r \in \mathcal{R}}$ (Definition 5.4). For each $r \in \mathcal{R}$ fix an integer $k_r \geq 0$ and weights $w^{(r)}$ as in Definition 6.5, let $\mathcal{F}_{\delta, r}$ be the value of the local functional $\mathcal{F}_\delta$ at the shell profile with parameters $(r^{f_r}, k_r, w^{(r)})$, and let H be as in (5.5). Let $(f_{\mathbb{R}}, g_{\mathbb{C}})$ be admissible with Fourier constants (M, σ) satisfying (5.19) with $\mu = 2e^{H/2-\ell}$, and put*

$$\begin{aligned} \mathcal{M}_{\mathcal{R}}(\theta) &= \sum_{r \in \mathcal{R}} \frac{\log \mathcal{F}_{\delta, r}}{e_r f_r} - (1/2 - \delta)\ell - C + (1 - \delta) \log 2 + (1 - \theta) \log \pi \\ &\quad + (1 - 2\theta)J_{\mathbb{R}} + \theta J_{\mathbb{C}}. \end{aligned}$$

If $\inf_j \mathcal{M}_{\mathcal{R}}(\theta_j) > 0$, where θ_j is the value of θ for F_j , then there are finite sets $U_j \subset \mathbb{R}^2$ with $|U_j| \rightarrow \infty$ and $u(U_j)/|U_j|^{1+\delta} \rightarrow \infty$. For unweighted shell profiles, $\sum_r \log \mathcal{F}_{\delta, r}/(e_r f_r) = J - \delta H$, so that $\mathcal{M}_{\mathcal{R}}$ is the margin $\mathcal{M}$ of (5.27).

Proof. Apply Proposition 6.21 with $\mathcal{P}_j$ the set of all places of F_j above $\mathcal{R}$, which split in K_j , and with $g_{\mathfrak{p}}$ the shell profile with parameters $(r^{f_r}, k_r, w^{(r)})$ for $\mathfrak{p}$ above r ; these parameters take $|\mathcal{R}|$ values, and $\mathcal{F}_{\delta, \mathfrak{p}} = \mathcal{F}_{\delta, r}$. Since there are $d/(e_r f_r)$ places above r , each with $Q_{\mathfrak{p}} = r^{f_r}$,

$$(6.24) \quad \frac{1}{d} \sum_{\mathfrak{p} \in \mathcal{P}} \log \mathcal{F}_{\delta, \mathfrak{p}} = \sum_{r \in \mathcal{R}} \frac{\log \mathcal{F}_{\delta, r}}{e_r f_r}, \quad H_f = \sum_{r \in \mathcal{R}} \frac{k_r \log r}{e_r} = H.$$

In particular (6.16) coincides with (5.19), whatever the shell weights, and the margin (6.22) of K_j/F_j equals $\mathcal{M}_{\mathcal{R}}(\theta_j)$. For unweighted shell profiles, Lemma 6.8 gives $\log \mathcal{F}_{\delta, r} = \log(k_r + 1) - \delta k_r f_r \log r$, and the sum in (6.24) is $J - \delta H$. $\square$

Thus Proposition 6.21 contains Proposition 5.26, and the shell weights replace the term $J - \delta H$ of (5.27) by $\sum_r \log \mathcal{F}_{\delta, r}/(e_r f_r)$ without changing the Fourier condition.

7. ARCHIMEDEAN PROFILES

We use a Gaussian at the compact coordinates, and at the pair coordinates a Student profile multiplied by a positive polynomial.

Definition 7.1. Let $s > 0$ and $a > 0$, and let P be a real polynomial in two variables that is positive on $[0, 1]^2$. For $(z, w) \in \mathbb{C}^2$ put

$$t = (1 + a|z|^2)^{-1}, \quad t' = (1 + a|w|^2)^{-1}, \quad g_{\mathbb{C}}(z, w) = t^s t'^s P(t, t').$$

We call $g_{\mathbb{C}}$ the *Student–Bernstein profile* with parameters (s, a, P) . For $P \equiv 1$ it is the *Student profile* $t^s t'^s$; for $s > 1$, each factor $(1 + a|z|^2)^{-s}$ is proportional to the density of a bivariate Student t -distribution. If P has degree at most m in each variable, its *Bernstein coefficients* of degree m are the numbers β_{ij} with

$$P(t, t') = \sum_{i,j=0}^m \beta_{ij} b_i^m(t) b_j^m(t'), \quad b_i^m(t) = \binom{m}{i} t^i (1-t)^{m-i}.$$

The Bernstein polynomials b_i^m are nonnegative on $[0, 1]$ and sum to one, so $\min \beta \leq P \leq \max \beta$ on $[0, 1]^2$, where $\min \beta$ and $\max \beta$ are the smallest and largest Bernstein coefficients. From now on, $g_{\mathbb{C}}$ denotes a Student–Bernstein profile with parameters (s, a, P) . Section 8 uses

$$s = 1.14600585, \quad a = 0.0000128633241758,$$

and the polynomial P of degree $m = 3$ in each variable whose Bernstein coefficients form the symmetric matrix

$$(7.2) \quad (\beta_{ij}) = \begin{pmatrix} 1 & 2.4129438977 & 2.7721799210 & 6.6857798061 \\ 2.4129438977 & 3.8532983888 & 4.6371750119 & 8.1307168183 \\ 2.7721799210 & 4.6371750119 & 5.4628959084 & 9.5512647588 \\ 6.6857798061 & 8.1307168183 & 9.5512647588 & 13.8659430610 \end{pmatrix}.$$

All finite decimals here are exact rational numbers.

Heuristic. The shape of $g_{\mathbb{C}}$ is adapted to the displacements at a pair of coordinates. By (5.1) they have moduli (e^u, e^{-u}) , so as u varies they run along a hyperbola. A profile of width $a^{-1/2}$ in each coordinate stays close to its translate for all u with $e^{|u|} \lesssim a^{-1/2}$, a range of length about $\log(1/a)$; this produces the factor $\log(1/a)$ in Proposition 7.17, against the term $2\delta \log a$ in (7.25), which comes from the exponent $1 + \delta$ on the mass $A_{\mathbb{C}}$. For Student–Bernstein profiles the overlap $I_{\mathbb{C}}$ reduces to beta integrals and digamma values (Lemmas 7.5–7.10), which makes rigorous bounds possible, and the polynomial P couples the two radii.

In this section we prove that these profiles are admissible in the sense of Definition 5.23, and we derive bounds for the functionals $J_{\mathbb{R}}$ and $J_{\mathbb{C}}$ (Definition 5.22) that reduce to finite computations with rational data. Section 8 carries out these computations at $\delta = 0.04273$. Throughout, $0 < \delta < 1$ and $p = 2/(1 + \delta)$. We write $\psi = \Gamma'/\Gamma$, γ for Euler's constant, $(x)_n$ for the rising factorial, $H_n = \sum_{k=1}^n 1/k$ with $H_0 = 0$, and $\text{Beta}(\alpha, \alpha')$ for the beta distribution on $(0, 1)$ with density proportional to $t^{\alpha-1}(1-t)^{\alpha'-1}$.

7.1. The Gaussian at the Compact Coordinates.

Lemma 7.3. Let $a_{\mathbb{R}} = 2p\delta$ and $f_{\mathbb{R}}(z) = e^{-a_{\mathbb{R}}|z|^2/p}$, so that $f_{\mathbb{R}}^p = e^{-a_{\mathbb{R}}|z|^2}$. Then

$$(7.4) \quad J_{\mathbb{R}} = \log(p/2) + \delta \log(a_{\mathbb{R}}/\pi) - a_{\mathbb{R}}/(2p) = \log(p/2) + \delta(\log(a_{\mathbb{R}}/\pi) - 1),$$

and $a_{\mathbb{R}}$ maximizes $J_{\mathbb{R}}$ over the Gaussians $e^{-a'|z|^2/p}$, $a' > 0$.

Proof. For $f = e^{-a'|z|^2/p}$ we have $A_{\mathbb{R}} = \pi/a'$ and, since $|z|^2 + |z+1|^2 = 2|z+1/2|^2 + 1/2$, $I_{\mathbb{R}} = (\pi p/(2a'))e^{-a'/(2p)}$. Hence $J_{\mathbb{R}} = \log(p/2) + \delta \log(a'/\pi) - a'/(2p)$, a concave function of $\log a'$ with its maximum at $a' = 2p\delta$. $\square$

By (5.27), the margin is affine in θ with slope $-\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}$. This slope depends on the profiles; for ours it is positive (Section 8).

7.2. The Pair Convolution.

Lemma 7.5. *Let $\alpha, \alpha' > 0$ with $A = \alpha + \alpha' - 1 > 0$, and let $h \in \mathbb{C}$. Then*

$$(7.6) \quad \int_{\mathbb{C}} (1 + |z|^2)^{-\alpha} (1 + |z + h|^2)^{-\alpha'} dz = \frac{\pi}{A} \mathbb{E}(1 + T(1 - T)|h|^2)^{-A}, \quad T \sim \text{Beta}(\alpha, \alpha').$$

Proof. Insert $(1 + |z|^2)^{-\alpha} = \Gamma(\alpha)^{-1} \int_0^\infty r^{\alpha-1} e^{-r(1+|z|^2)} dr$ and the analogous formula with a variable r' . Since $r|z|^2 + r'|z + h|^2 = (r + r')|z + r'h/(r + r')|^2 + rr'|h|^2/(r + r')$, the integral of $e^{-r|z|^2 - r'|z + h|^2}$ over $z \in \mathbb{C}$ is $\pi(r + r')^{-1} e^{-rr'|h|^2/(r+r')}$; the factors e^{-r} and $e^{-r'}$ remain in the Laplace integrals. Substitute $r = RT$, $r' = R(1 - T)$, with Jacobian R , and integrate over R . This gives

$$\frac{\pi \Gamma(A)}{\Gamma(\alpha) \Gamma(\alpha')} \int_0^1 T^{\alpha-1} (1 - T)^{\alpha'-1} (1 + T(1 - T)|h|^2)^{-A} dT,$$

which equals the right side of (7.6) because $\Gamma(\alpha + \alpha') = A \Gamma(A)$. All integrands are nonnegative, so Tonelli's theorem justifies the interchanges. $\square$

For $A, B > 0$ and $y > 0$ define

$$Q_{AB}(y) = \int_{\mathbb{R}} (1 + ye^{2v})^{-A} (1 + ye^{-2v})^{-B} dv.$$

Lemma 7.7. *Let $A, B > 0$.*

(a) *For $y > 0$,*

$$(7.8) \quad \left| Q_{AB}(y) - \log(1/y) + \frac{\psi(A) + \psi(B) + 2\gamma}{2} \right| \leq \frac{(A + B)y}{2}.$$

(b) *For $0 < y < 1$, with absolutely convergent series,*

$$Q_{AB}(y) = \sum_{n \geq 0} \frac{(A)_n (B)_n}{(n!)^2} y^{2n} \left[\log(1/y) + \psi(n + 1) - \frac{\psi(A + n) + \psi(B + n)}{2} \right].$$

(c) *Suppose $A, B \geq 1$, $0 < y < 1$, $AB y^2 < 1$ and $2 \log(1/y) \geq H_{[A]-1} + H_{[B]-1}$. Then every term of the series in (b) is nonnegative, and for every integer $n_* \geq 0$ its remainder $\text{Rem}_{n_*}(y)$ after the terms $n \leq n_*$ satisfies*

$$0 \leq \text{Rem}_{n_*}(y) \leq \log(1/y) \frac{(AB y^2)^{n_*+1}}{1 - AB y^2}.$$

Proof. (a) Split the integral at $v = 0$. On $v \geq 0$, first replace $(1 + ye^{-2v})^{-B}$ by 1. Since $0 \leq 1 - (1 + ye^{-2v})^{-B} \leq B y e^{-2v}$, this changes the half-integral by an amount in $[0, By/2]$. The substitution $x = ye^{2v}$ gives $\int_0^\infty (1 + ye^{2v})^{-A} dv = \frac{1}{2} \int_y^\infty (1 + x)^{-A} dx/x$, and

$$\int_y^\infty \frac{dx}{x(1+x)^A} = \log \frac{1}{y} + \kappa_A + \int_0^y (1 - (1+x)^{-A}) \frac{dx}{x}, \quad \kappa_A = \int_0^\infty ((1+x)^{-A} - \mathbf{1}_{x < 1}) \frac{dx}{x}.$$

The last integral lies in $[0, Ay]$, because $0 \leq 1 - (1+x)^{-A} \leq Ax$; in particular it tends to 0 with y . On the other hand, the substitution $t = 1/(1+x)$ gives

$$\int_y^\infty \frac{dx}{x(1+x)^A} = \int_0^{1/(1+y)} \frac{t^{A-1} - 1}{1-t} dt + \log \frac{1+y}{y}.$$

Letting $y \rightarrow 0$ in the two expressions yields $\kappa_A = \int_0^1 (t^{A-1} - 1)(1-t)^{-1} dt = -\psi(A) - \gamma$ [25, Equation (5.9.16)]. Thus the half $v \geq 0$ equals $\frac{1}{2}(\log(1/y) - \psi(A) - \gamma)$ plus a term in $[0, Ay/2]$

minus a term in $[0, By/2]$. The half $v \leq 0$ is the same with A and B exchanged. Adding the halves proves (a).

(b) The substitutions $x = ye^{2v}$ and then $t = x/(x + y^2)$ give

$$2Q_{AB}(y) = \int_0^1 t^{B-1}(1-t)^{A-1}(1-(1-y^2)t)^{-A} dt.$$

By Euler's integral [25, Equation (15.6.1)], the right side is $\Gamma(A)\Gamma(B)\mathbf{F}(A, B; A+B; 1-y^2)$, where $\mathbf{F}$ is Olver's regularized hypergeometric function. The expansion [25, Equation (15.8.10)], in the case where the third parameter is the sum of the first two, gives

$$\mathbf{F}(A, B; A+B; 1-y^2) = \frac{1}{\Gamma(A)\Gamma(B)} \sum_{n \geq 0} \frac{(A)_n(B)_n}{(n!)^2} y^{2n} [2\psi(n+1) - \psi(A+n) - \psi(B+n) - \log y^2]$$

for $0 < y < 1$. Dividing by two proves (b). The coefficients grow at most polynomially in n , so the series converges absolutely.

(c) For $A \geq 1$ and $n \geq 0$, monotonicity of ψ and the recurrence $\psi(x+1) = \psi(x) + 1/x$ give $\psi(n+1) \leq \psi(A+n) \leq \psi([A] + n) \leq \psi(n+1) + H_{[A]-1}$. Hence the bracket in (b) lies between $\log(1/y) - \frac{1}{2}(H_{[A]-1} + H_{[B]-1}) \geq 0$ and $\log(1/y)$. Moreover $(A)_n/n! = \prod_{k < n} (A+k)/(k+1) \leq A^n$ for $A \geq 1$, and similarly for B . Summing the geometric series proves (c). $\square$

Definition 7.9. Let d_{ij} be the monomial coefficients of P , so that $P(t, t') = \sum_{i,j} d_{ij} t^i t'^j$, and put $\eta_0 = 2s - 1$,

$$A_{ik} = \eta_0 + i + k, \quad B_{jl} = \eta_0 + j + l, \quad w_{ijkl} = \frac{d_{ij}d_{kl}}{A_{ik}B_{jl}}.$$

A quadruple (i, j, k, l) with $d_{ij}d_{kl} \neq 0$ is a *cross*.

Lemma 7.10. Let $s \geq 1$ and $a > 0$. Then

$$I_{\mathbb{C}} = \frac{\pi^2}{a^2} \sum_{(i,j,k,l)} w_{ijkl} \mathbb{E} Q_{A_{ik}B_{jl}}(y), \quad y = a\sqrt{T(1-T)T'(1-T')} \leq a/4,$$

where the sum runs over all crosses and, for each cross, $T \sim \text{Beta}(s+i, s+k)$ and $T' \sim \text{Beta}(s+j, s+l)$ are independent. Each expectation is finite.

Proof. Expand $g_{\mathbb{C}}(z, w) = \sum_{i,j} d_{ij}(1 + a|z|^2)^{-s-i}(1 + a|w|^2)^{-s-j}$ and multiply out $g_{\mathbb{C}}(z, w)g_{\mathbb{C}}(z + e^u, w + e^{-u})$. For one cross, the scaling $z \mapsto z/\sqrt{a}$ and Lemma 7.5 give

$$\int_{\mathbb{C}} (1 + a|z|^2)^{-s-i}(1 + a|z + e^u|^2)^{-s-k} dz = \frac{\pi}{aA_{ik}} \mathbb{E}(1 + aT(1-T)e^{2u})^{-A_{ik}},$$

and similarly in w with e^{-2u} , B_{jl} and T' . By Tonelli's theorem, the u -integral of the product is $\mathbb{E} \int_{\mathbb{R}} (1 + Ye^{2u})^{-A_{ik}}(1 + Y'e^{-2u})^{-B_{jl}} du$ with $Y = aT(1-T)$ and $Y' = aT'(1-T')$, and the translation $u \mapsto u + \frac{1}{4} \log(Y'/Y)$ turns the inner integral into $Q_{A_{ik}B_{jl}}(\sqrt{YY'})$. By (7.8), $Q_{AB}(y)$ is at most $\log(1/y)$ plus a constant, and $\log(1/(T(1-T)))$ is integrable under every beta law; so each term is finite and the finite signed sum is legitimate. $\square$

7.3. Admissibility. For the Fourier bound we assume that P has positive Bernstein coefficients β_{ij} of some degree $m \geq 1$.

Definition 7.11. Let Δ_1 and Δ_2 be the forward difference operators in the two indices of (β_{ij}) . For $0 < \rho < 1$, the width of the complex tube in the proof of Lemma 7.12, put $\omega = (\rho + \rho^2)/(1 - \rho^2)$,

$$E_{rr'} = \binom{m}{r} \binom{m}{r'} \max_{i,j} |\Delta_1^r \Delta_2^{r'} \beta_{ij}|, \quad q_0 = \frac{1}{\min \beta} \sum_{r+r' > 0} E_{rr'} \omega^{r+r'}.$$

We call q_0 the *tube constant*.

Lemma 7.12. *Let $s > 0$, $sp > 1$ and $a > 0$, let P have positive Bernstein coefficients β_{ij} of degree $m \geq 1$, let $0 < \rho < 1$, and suppose that the tube constant satisfies $q_0 < 1$. Then for all $\xi_1, \xi_2 \in \mathbb{C}$,*

$$|\widehat{g_{\mathbb{C}}^p}(\xi_1, \xi_2)| \leq K_{\mathbb{C}} e^{-\sigma_{\mathbb{C}}(|\xi_1| + |\xi_2|)} A_{\mathbb{C}}, \quad K_{\mathbb{C}} = (1 - \rho^2)^{-2sp} (1 + q_0)^p, \quad \sigma_{\mathbb{C}} = 2\pi\rho/\sqrt{a}.$$

Proof. Write $x = \sqrt{a}z \in \mathbb{R}^2$ and consider complex vectors $x + iy$ with $x, y \in \mathbb{R}^2$ and $|y| \leq \rho$. Put $\mathcal{D}(x + iy) = 1 + (x_1 + iy_1)^2 + (x_2 + iy_2)^2$. Then

$$\operatorname{Re} \mathcal{D} = 1 + |x|^2 - |y|^2 \geq (1 - \rho^2)(1 + |x|^2), \quad |\mathcal{D}^{-1} - (1 + |x|^2)^{-1}| \leq \frac{2|x|\rho + \rho^2}{(1 - \rho^2)(1 + |x|^2)^2} \leq \omega.$$

So the complexified $t = \mathcal{D}^{-1}$ lies within ω of the real $t_0 = (1 + |x|^2)^{-1} \in (0, 1]$, and likewise for t' . By the Bernstein derivative formula, $\partial_t^r \partial_{t'}^{r'} P / (r! r'!) = \binom{m}{r} \binom{m}{r'} \sum_{i,j} (\Delta_1^r \Delta_2^{r'} \beta)_{ij} b_i^{m-r}(t) b_j^{m-r'}(t')$, which is at most $E_{rr'}$ in absolute value on $[0, 1]^2$. Taylor expansion of the polynomial P about (t_0, t'_0) therefore gives $|P(t, t') - P(t_0, t'_0)| \leq q_0 \min \beta \leq q_0 P(t_0, t'_0)$. Thus $P(t, t')$ lies in the right half-plane, and with principal branches,

$$|\mathcal{D}(x + iy)^{-sp} \mathcal{D}(x' + iy')^{-sp} P(t, t')^p| \leq K_{\mathbb{C}} t_0^{sp} t'_0{}^{sp} P(t_0, t'_0)^p,$$

where $x' + iy'$ is the variable attached to w . The same bounds hold for $|y|, |y'| < \rho'$ with some $\rho' > \rho$, since q_0 depends continuously on ρ , so the left side is holomorphic in each complex coordinate on a neighborhood of the closed tube.

The function $g_{\mathbb{C}}^p$ is invariant under rotations of z and of w . Rotate so that ξ_1 and ξ_2 are positive multiples of the first basis vector, and shift the first real coordinate of x by $-i\rho$, then that of x' by $-i\rho$. Each shift is justified by Cauchy's theorem in one variable: the integrand is holomorphic in the strip and bounded there by a constant times $(1 + |x|^2)^{-sp} (1 + |x'|^2)^{-sp}$, which tends to zero at infinity and is integrable because $sp > 1$. After the shifts the Fourier factor is multiplied by $e^{-2\pi\rho(|\xi_1| + |\xi_2|)/\sqrt{a}}$, and the displayed bound gives the lemma. $\square$

Proposition 7.13. *Let $s \geq 1$, $a > 0$, and let P have positive Bernstein coefficients β_{ij} of some degree $m \geq 1$ in each variable. Let $0 < \delta < 1$ with $a_{\mathbb{R}} = 2p\delta \leq 1$, let $f_{\mathbb{R}}$ be the Gaussian of Lemma 7.3, and let $0 < \rho < 1$ with $q_0 < 1$. Then $(f_{\mathbb{R}}, g_{\mathbb{C}})$ is admissible with Fourier constants*

$$(7.14) \quad M = \max\{2, \sqrt{K_{\mathbb{C}}}\}, \quad \sigma = \min\{1, \sigma_{\mathbb{C}}\}.$$

Proof. (P1) The functions $f_{\mathbb{R}}^p$ and $g_{\mathbb{C}}^p = (1 + a|z|^2)^{-sp} (1 + a|w|^2)^{-sp} P(t, t')^p$ are smooth, because $P \geq \min \beta > 0$ on $[0, 1]^2$, and they and all their derivatives are bounded.

(P2) The integrals at the compact coordinates are computed in Lemma 7.3. The mass $A_{\mathbb{C}}$ is finite because $sp > 1$ (Proposition 7.20 below), and $0 < I_{\mathbb{C}} < \infty$ because $g_{\mathbb{C}} \leq \max \beta t^s t'^s$ and Lemma 7.10 applies to the Student profile $t^s t'^s$.

(P3) $V_{\mathbb{R}} = a_{\mathbb{R}}|z|^2/p$, and $V_{\mathbb{C}} = s \log(1 + a|z|^2) + s \log(1 + a|w|^2) - \log P(t, t')$ is at least $-\log \max \beta$ and tends to infinity with $|z|$ or $|w|$.

(P4) The endpoint law at a compact coordinate is Gaussian. For the pair, $-\log P$ is bounded, so it suffices to bound the second moments of $\log(1 + a|z|^2)$ and $\log(1 + a|w|^2)$. Choose $0 < \tau < s$; then $\tau < 2s - 1$ as well, since $s \geq 1$. We have $\log^2(1 + x) \leq c_{\tau}(1 + x)^{\tau}$ for $x \geq 0$ and some constant c_{τ} , and $g_{\mathbb{C}} \leq \max \beta t^s t'^s$. Hence the second moment of $\log(1 + a|z|^2)$ is at most a constant times the integral of $(1 + a|z|^2)^{-(s-\tau)} (1 + a|z + e^u|^2)^{-s} (1 + a|w|^2)^{-s} (1 + a|w + e^{-u}|^2)^{-s}$. By the argument of Lemma 7.10, with exponents $s - \tau > 0$ and s and $A = 2s - \tau - 1 > 0$, this integral is a multiple of $\mathbb{E} Q_{A, 2s-1}(y)$, which is finite by (7.8). The same holds for w .

(P5) By Lemma 5.21 the Gaussian satisfies $|\widehat{f_{\mathbb{R}}^p}(\xi)| \leq 2e^{-|\xi|} A_{\mathbb{R}} \leq M e^{-\sigma|\xi|} A_{\mathbb{R}}$, and by Lemma 7.12 the pair profile satisfies the bound with $K_{\mathbb{C}} e^{-\sigma_{\mathbb{C}}(|\xi_1| + |\xi_2|)} \leq M^2 e^{-\sigma(|\xi_1| + |\xi_2|)}$. $\square$

7.4. A Lower Bound for the Overlap $I_{\mathbb{C}}$.

Definition 7.15. For $n \geq 0$ and integers $i, k \geq 0$ put

$$K_n(i, k) = \frac{(s+i)_n(s+k)_n}{n! (\eta_0 + i + k + n)_{n+1}}, \quad D_x(j) = \sum_{h=0}^{j-1} \frac{1}{x+h} \quad (D_x(0) = 0),$$

$$r_n(i, k) = -\frac{1}{\eta_0} + \frac{H_n}{2} - \frac{D_{\eta_0}(i+k+n)}{2} + D_{\eta_0}(i+k+2n+1) - \frac{D_s(i+n) + D_s(k+n)}{2},$$

$$R_n(i, k) = K_n(i, k)r_n(i, k), \text{ and}$$

$$G_n = \sum d_{ij}d_{kl}K_n(i, k)K_n(j, l), \quad \tilde{G}_n = \sum d_{ij}d_{kl}[R_n(i, k)K_n(j, l) + K_n(i, k)R_n(j, l)],$$

where the sums run over all crosses. Put

$$(7.16) \quad c_s = -2\psi(s) + \psi(2s) + (2s-1)^{-1} - \gamma, \quad y_0 = a/4.$$

For rational s and d_{ij} , the numbers $K_n(i, k)$, $r_n(i, k)$, $R_n(i, k)$, G_n and $\tilde{G}_n$ are rational.

Proposition 7.17. Let $s \geq 1$ and $a > 0$, and suppose that for every cross

$$(7.18) \quad A_{ik}B_{jl}y_0^2 < 1, \quad 2\log(4/a) \geq H_{\lceil A_{ik} \rceil - 1} + H_{\lceil B_{jl} \rceil - 1}, \quad \log(4/a) > 1/2.$$

Then for every integer $n_* \geq 0$,

$$(7.19) \quad \frac{I_{\mathbb{C}}}{\pi^2 a^{-2}} \geq \sum_{n=0}^{n_*} a^{2n} \{G_n[\log(1/a) + c_s] + \tilde{G}_n\} - E_{-,n_*},$$

where the remainder term is

$$E_{-,n_*} = \log(4/a) \sum_{w_{ijkl} < 0} (-w_{ijkl}) \frac{(A_{ik}B_{jl}y_0^2)^{n_*+1}}{1 - A_{ik}B_{jl}y_0^2}.$$

Proof. Start from Lemma 7.10. Since $y \leq y_0 = a/4 < 1$, the hypotheses of Lemma 7.7(c) hold at every value of y , with $A = A_{ik} \geq 1$ and $B = B_{jl} \geq 1$. Split each $Q_{A_{ik}B_{jl}}(y)$ into the terms $n \leq n_*$ of Lemma 7.7(b) and the remainder $\text{Rem}_{n_*}(y)$.

Consider the term of index n for one cross, with $\alpha = s+i$, $\alpha' = s+k$, $A = A_{ik} = \alpha + \alpha' - 1$, and similarly for T' . Its factor y^{2n} is $a^{2n}(T(1-T))^n(T'(1-T'))^n$, and $\log(1/y) = \log(1/a) - \frac{1}{2}\log(T(1-T)) - \frac{1}{2}\log(T'(1-T'))$. The beta integral gives $\mathbb{E}(T(1-T))^n = (\alpha)_n(\alpha')_n/(A+1)_{2n}$, so

$$\frac{(A)_n}{A n!} \mathbb{E}(T(1-T))^n = \frac{(\alpha)_n(\alpha')_n}{n!(A+n)_{n+1}} = K_n(i, k).$$

Weighting by $(T(1-T))^n$ turns $\text{Beta}(\alpha, \alpha')$ into $\text{Beta}(\alpha+n, \alpha'+n)$, under which the mean of $\log(T(1-T))$ is $\psi(\alpha+n) + \psi(\alpha'+n) - 2\psi(A+2n+1)$. The recurrence $\psi(x+j) = \psi(x) + D_x(j)$ and $\psi(1) = -\gamma$ give

$$\begin{aligned} \psi(n+1) &= -\gamma + H_n, & \psi(\alpha+n) &= \psi(s) + D_s(i+n), & \psi(\alpha'+n) &= \psi(s) + D_s(k+n), \\ \psi(A+n) &= \psi(\eta_0) + D_{\eta_0}(i+k+n), & \psi(A+2n+1) &= \psi(\eta_0) + D_{\eta_0}(i+k+2n+1), \\ \frac{1}{2}c_s &= -\psi(s) + \frac{1}{2}\psi(\eta_0) + \eta_0^{-1} - \frac{1}{2}\gamma, \end{aligned}$$

the last one because $\psi(2s) = \psi(\eta_0) + 1/\eta_0$. Substituting,

$$\frac{1}{2}\psi(n+1) - \frac{1}{2}\psi(A+n) - \frac{1}{2}[\psi(\alpha+n) + \psi(\alpha'+n)] + \psi(A+2n+1) = \frac{1}{2}c_s + r_n(i, k).$$

Hence the expectation of the term of index n , multiplied by w_{ijkl} , is

$$a^{2n}d_{ij}d_{kl}K_n(i, k)K_n(j, l)[\log(1/a) + c_s + r_n(i, k) + r_n(j, l)].$$

Summing over crosses gives the displayed main terms.

By Lemma 7.7(c), $0 \leq \text{Rem}_{n_*}(y) \leq \log(1/y)(AB y^2)^{n_*+1}/(1 - AB y^2)$. The right side increases with y on $(0, y_0]$, because the derivative of $y^{2n_*+2} \log(1/y)$ is $y^{2n_*+1}((2n_*+2) \log(1/y) - 1) > 0$ when $\log(1/y) > 1/2$. So $0 \leq \text{Rem}_{n_*}(y) \leq \log(4/a)(AB y_0^2)^{n_*+1}/(1 - AB y_0^2)$. For crosses with $w_{ijkl} > 0$ we discard the remainder, and for crosses with $w_{ijkl} < 0$ we subtract its upper bound. This proves (7.19). $\square$

With $n_* = 1$ the bound keeps the exact term of order a^2 ; the terms it discards or subtracts are of order $a^4 \log(1/a)$. It is a lower bound for $I_{\mathbb{C}}$ only.

7.5. An Upper Bound for the Mass $A_{\mathbb{C}}$.

Proposition 7.20. *Let $g_{\mathbb{C}}$ be a Student–Bernstein profile with parameters (s, a, P) such that $q = sp - 1 > 0$. Then*

$$(7.21) \quad A_{\mathbb{C}} = \frac{\pi^2}{a^2 q^2} \bar{A}_{\mathbb{C}}, \quad \bar{A}_{\mathbb{C}} = \mathbb{E} P(T, T')^p,$$

where T and T' are independent with density $q t^{q-1}$ on $(0, 1)$. Partition $[0, 1]^2$ into rectangles $\mathcal{Q} = [l, r] \times [l', r']$, and use on $\mathcal{Q}$ the coordinates $x = (T - l)/(r - l)$ and $x' = (T' - l')/(r' - l')$. Suppose that the Bernstein coefficients, of some degree, of the restriction of P to $\mathcal{Q}$ in these coordinates lie in $[m_{\mathcal{Q}}, M_{\mathcal{Q}}]$ with $m_{\mathcal{Q}} > 0$, and put

$$c_{\mathcal{Q}} = \frac{m_{\mathcal{Q}} + M_{\mathcal{Q}}}{2}, \quad \rho_{\mathcal{Q}} = \frac{M_{\mathcal{Q}} - m_{\mathcal{Q}}}{M_{\mathcal{Q}} + m_{\mathcal{Q}}}, \quad P = c_{\mathcal{Q}}(1 + W_{\mathcal{Q}}) \text{ on } \mathcal{Q}.$$

Define

$$(7.22) \quad M_i(l, r) = \int_l^r q v^{q-1} \left(\frac{v-l}{r-l} \right)^i dv = \frac{q}{(r-l)^i} \sum_{j=0}^i \binom{i}{j} (-l)^{i-j} \frac{r^{q+j} - l^{q+j}}{q+j},$$

and, writing $W_{\mathcal{Q}}^k = \sum_{i,j} c_{ij}^{(k)} x^i x'^j$,

$$\Sigma_{\mathcal{Q}, N} = c_{\mathcal{Q}}^p \sum_{k=0}^N \binom{p}{k} \sum_{i,j} c_{ij}^{(k)} M_i(l, r) M_j(l', r').$$

Then for every $N \geq 1$,

$$(7.23) \quad \left| \bar{A}_{\mathbb{C}} - \sum_{\mathcal{Q}} \Sigma_{\mathcal{Q}, N} \right| \leq \sum_{\mathcal{Q}} c_{\mathcal{Q}}^p \frac{\left| \binom{p}{N+1} \right| \rho_{\mathcal{Q}}^{N+1}}{1 - \rho_{\mathcal{Q}}} M_0(l, r) M_0(l', r').$$

Proof. The substitution $t = (1 + a|z|^2)^{-1}$ gives $dz = \pi dt/(at^2)$ on $\mathbb{C}$. Hence

$$A_{\mathbb{C}} = \frac{\pi^2}{a^2} \int_0^1 \int_0^1 t^{sp-2} t'^{sp-2} P(t, t')^p dt dt',$$

which is (7.21) since $sp - 2 = q - 1$. The Bernstein convex-hull property gives $|W_{\mathcal{Q}}| \leq \rho_{\mathcal{Q}} < 1$ on $\mathcal{Q}$. For $1 < p < 2$ the binomial coefficients satisfy $\left| \binom{p}{k+1} \right| / \left| \binom{p}{k} \right| = |p - k|/(k + 1) < 1$ for $k \geq 1$, so the binomial series of $(1 + W)^p$ converges uniformly on $|W| \leq \rho_{\mathcal{Q}}$, and its tail after index $N \geq 1$ is at most $\left| \binom{p}{N+1} \right| \rho_{\mathcal{Q}}^{N+1}/(1 - \rho_{\mathcal{Q}})$. Integrate against the density on $\mathcal{Q}$, whose integral over $\mathcal{Q}$ is $M_0(l, r) M_0(l', r')$. The moment formula follows by expanding $(v - l)^i$; the convention $0^q = 0$ is valid since $q > 0$. $\square$

If P is symmetric and both axes are partitioned alike, a rectangle and its reflection contribute equally, so off-diagonal rectangles may be counted twice and diagonal ones once. Subsection 8.5 describes how the quantities in Proposition 7.20 are evaluated.

7.6. A Lower Bound for the Functional $J_{\mathbb{C}}$.

Corollary 7.24. *Under the hypotheses of Propositions 7.17 and 7.20, let Z_* be the right side of (7.19) for some n_* , and suppose $Z_* > 0$. If $\bar{A}_{\mathbb{C}}^* \geq \bar{A}_{\mathbb{C}}$, then*

$$(7.25) \quad J_{\mathbb{C}} \geq \log Z_* + 2(1 + \delta) \log q - 2\delta \log \pi + 2\delta \log a - (1 + \delta) \log \bar{A}_{\mathbb{C}}^*.$$

Proof. By Proposition 7.17, $I_{\mathbb{C}} \geq \pi^2 a^{-2} Z_*$, and by (7.21), $A_{\mathbb{C}} \leq \pi^2 a^{-2} q^{-2} \bar{A}_{\mathbb{C}}^*$. Substitute into $J_{\mathbb{C}} = \log I_{\mathbb{C}} - (1 + \delta) \log A_{\mathbb{C}}$. $\square$

Interval evaluation of the right side of (7.25) gives a rigorous lower bound for $J_{\mathbb{C}}$; the upper endpoint of such an enclosure is not an upper bound for $J_{\mathbb{C}}$. For rational s , all digamma values in Proposition 7.17 reduce to rational corrections and to $c_s = 2/\eta_0 + \psi(\eta_0) - 2\psi(s) + \psi(1)$, since $\psi(2s) = \psi(\eta_0) + 1/\eta_0$ and $\psi(1) = -\gamma$. The digamma function at rational arguments is enclosed as follows.

Lemma 7.26. *For $x > 0$ and integers $L \geq 0$ and $k_* \geq 1$, put $z = x + L$. Then*

$$\left| \psi(x) - \left(\log z - \frac{1}{2z} - \sum_{k=1}^{k_*-1} \frac{B_{2k}}{2kz^{2k}} - \sum_{j=0}^{L-1} \frac{1}{x+j} \right) \right| \leq \frac{|B_{2k_*}|}{2k_* z^{2k_*}},$$

where B_{2k} are the Bernoulli numbers.

Proof. By Binet's formula [25, Equation (5.9.15)],

$$\psi(z) = \log z - \frac{1}{2z} - 2 \int_0^\infty \frac{t \, dt}{(t^2 + z^2)(e^{2\pi t} - 1)}.$$

Write

$$\frac{1}{t^2 + z^2} = \sum_{k=1}^{k_*-1} (-1)^{k-1} \frac{t^{2k-2}}{z^{2k}} + (-1)^{k_*-1} \frac{t^{2k_*-2}}{z^{2k_*-2}(t^2 + z^2)},$$

and use $\int_0^\infty t^{2k-1} (e^{2\pi t} - 1)^{-1} dt = |B_{2k}|/(4k)$ and $(-1)^{k-1} |B_{2k}| = B_{2k}$. The remaining integral has a fixed sign and is at most $|B_{2k_*}|/(2k_* z^{2k_*})$ in absolute value, because $(t^2 + z^2)^{-1} \leq z^{-2}$. Finally apply the recurrence $\psi(x+1) = \psi(x) + 1/x$ L times. $\square$

8. PROOF OF THEOREM 1.1

We prove Theorem 1.1 by applying Corollary 6.23 to the fields of Theorem 2.42, with the upper bound for the relative zeta value in Theorem 4.2 and the data of Definition 8.1. Propositions 8.4 and 8.5 are verified by computer, in exact rational arithmetic and in outward-rounded interval arithmetic, as described in Subsection 8.5; the other steps are proved in the text. The inequalities between decimals in Propositions 8.4 and 8.5 and in Remarks 8.11 and 8.12, and the entries of Tables 6 and 8, are computed and printed by the supplementary program `geom241.py`. In the inequalities the decimals are rounded outward from interval enclosures, and the table entries are rounded to ten decimals. No rounded decimal is substituted into a later calculation; in particular, $\bar{A}_{\mathbb{C}}^*$ in Definition 8.3 is the exact upper end of a computed enclosure, not its rounded decimal.

8.1. Parameters and Local Data.

Definition 8.1. The *data* of this section are the following.

- (a) $\delta = 4273/100000 = 0.04273$, $p = 2/(1 + \delta) = 200000/104273$ and $C = 4871285/10^8 = 0.04871285$; $\lambda = 2^{9/4} \sqrt{3615}$ and $\ell = \log \lambda$, as in Theorem 2.42.
- (b) At the compact coordinates, $f_{\mathbb{R}}$ is the Gaussian of Lemma 7.3, with $f_{\mathbb{R}}^p = e^{-a_{\mathbb{R}}|z|^2}$ and $a_{\mathbb{R}} = 2p\delta = 17092/104273 < 1$.

- (c) At the pair coordinates, $g_{\mathbb{C}}$ is the Student–Bernstein profile of Definition 7.1 (the polynomial P below is positive on $[0, 1]^2$, since its Bernstein coefficients are positive by Proposition 8.4(b)) with $s = 1.14600585$, $a = 0.0000128633241758$ and the polynomial P of degree $m = 3$ in each variable whose Bernstein coefficients are (7.2). We put $q = sp - 1 = 12492817/10427300$.
- (d) In Definition 7.11 and Lemma 7.12 we take $\rho = 10^{-3}$, with the Bernstein coefficients of degree $m = 3$ of (c). In Proposition 7.20 we partition $[0, 1]^2$ into the 64 squares of side $1/8$, use on each square the Bernstein coefficients of degree 3, with m_Q and M_Q the smallest and largest of these coefficients, and take $N = 18$. In Proposition 7.17 we take $n_* = 1$.
- (e) $\mathcal{R} = \{2, 3, 5, 7, 29\}$. For $r \in \mathcal{R}$, (e_r, f_r) is the absolute type (Definition 2.41) of the primes of F above r given by Theorem 2.42 (Table 5, repeated in Table 6), the exponent k_r is that of Table 6, and $Q_r = r^{f_r}$. For a prime $\mathfrak{p}$ of F above r , g_r is the shell profile on $F_{\mathfrak{p}}^2$ with parameters $(Q_r, k_r, (w_{r,i}w_{r,j})_{i,j \geq 0})$, where $w_{r,0} = 1$, the weights $w_{r,i}$ with $1 \leq i < n_r$ are those of Table 7, and $w_{r,i} = 0$ for $i \geq n_r$; these weights are nonnegative by Proposition 8.4(a). By Lemma 6.8, the value $\mathcal{F}_{\delta,r} = \mathcal{F}_{\delta}(g_r)$ depends only on these parameters.

Every parameter written as a finite decimal is exact. We recall $\theta_* = 65535/131072$ from Theorem 2.42. Since the weights $w_{r,i}$ are nonnegative (Proposition 8.4(a)) and $w_{r,0} = 1$, Corollary 6.10, with $x = x' = (w_{r,i})_{i \geq 0}$, gives

$$(8.2) \quad \log \mathcal{F}_{\delta,r} = -\delta k_r \log Q_r + \log((k_r + 1)S_r^2 + 2S_r R_r) - 2(1 + \delta) \log P_r,$$

where $P_r = \sum_i m_i w_{r,i}^p$, $S_r = \sum_i m_i w_{r,i}^2$ and $R_r = \sum_{i,i'} \Delta_{ii'} w_{r,i} w_{r,i'}$, with the shell measures m_i and the matrix Δ of Section 6 for $Q = Q_r$. Table 6 lists the local data and Table 7 the exact weights. At 7 and 29 only $\mathcal{S}_0, \mathcal{S}_1$, respectively $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2$, carry weight, and these shell profiles improve only slightly on the unweighted shell profiles (Table 6).

TABLE 6. Local data at the primes of $\mathcal{R}$. Here $Q_r = r^{f_r}$, the profile g_r uses the weights $w_{r,0}, \dots, w_{r,n_r-1}$, and the last two columns give $\log \mathcal{F}_{\delta,r}/(e_r f_r)$ for g_r and for the unweighted shell profile with parameters (Q_r, k_r) , rounded to ten decimals.

r	e_r	f_r	Q_r	k_r	n_r	g_r	unweighted
2	8	4	16	7	6	0.0393401103	0.0390666415
3	2	2	9	9	6	0.3675484302	0.3643996093
5	2	2	25	6	6	0.2817099488	0.2801636913
7	1	8	5764801	1	2	0.0034946608	0.0034946569
29	1	4	707281	1	3	0.0294023321	0.0294022443

Definition 8.3. Let Z_* be the right side of (7.19) for the data of Definition 8.1, with $n_* = 1$. Let $\bar{A}_{\mathbb{C}}^*$ be the upper end of the rigorous interval enclosure of $\bar{A}_{\mathbb{C}}$ computed by the program of Subsection 8.5 (Proposition 8.5(a)), so that $\bar{A}_{\mathbb{C}} \leq \bar{A}_{\mathbb{C}}^* < 38.7888697256861071$, the last number being $\bar{A}_{\mathbb{C}}^*$ rounded up. Let $J_{\mathbb{C}}^*$ be the right side of (7.25) for these Z_* and $\bar{A}_{\mathbb{C}}^*$, and put

$$\begin{aligned} \mathcal{M}_*(\theta) = & \sum_{r \in \mathcal{R}} \frac{\log \mathcal{F}_{\delta,r}}{e_r f_r} - (1/2 - \delta)\ell - C + (1 - \delta) \log 2 + (1 - \theta) \log \pi \\ & + (1 - 2\theta)J_{\mathbb{R}} + \theta J_{\mathbb{C}}^*. \end{aligned}$$

We call $\mathcal{M}_*(\theta)$ the *lower bound for the margin* $\mathcal{M}_{\mathcal{R}}(\theta)$ of Corollary 6.23; Lemma 8.10 justifies the name.

TABLE 7. The exact shell weights $w_{r,i}$ for $1 \leq i < n_r$; all $w_{r,0} = 1$, and $w_{r,i} = 0$ for $i \geq n_r$. The last column gives the weights rounded to six significant digits, for orientation only; the computations of Section 8 use the exact fractions.

r	i	$w_{r,i}$	$\approx w_{r,i}$
2	1	2854206002066/59041214756005	$4.83426 \cdot 10^{-2}$
2	2	198349814036/95709219081499	$2.07242 \cdot 10^{-3}$
2	3	7762557303/86561984122975	$8.96763 \cdot 10^{-5}$
2	4	109894931/27828186078256	$3.94905 \cdot 10^{-6}$
2	5	17033757/96603874664399	$1.76326 \cdot 10^{-7}$
3	1	5693537714695/63764117760919	$8.92906 \cdot 10^{-2}$
3	2	567838527095/78237129879259	$7.25792 \cdot 10^{-3}$
3	3	43356430379/72943614524859	$5.94383 \cdot 10^{-4}$
3	4	2265261068/45953937834745	$4.92942 \cdot 10^{-5}$
3	5	74149907/18018553422030	$4.11520 \cdot 10^{-6}$
5	1	1343081168627/46386563301209	$2.89541 \cdot 10^{-2}$
5	2	61788974773/82067065665364	$7.52908 \cdot 10^{-4}$
5	3	1389672153/69896165011649	$1.98820 \cdot 10^{-5}$
5	4	32644248/60812698834313	$5.36800 \cdot 10^{-7}$
5	5	511565/34657937034136	$1.47604 \cdot 10^{-8}$
7	1	2309805/69240611498956	$3.33591 \cdot 10^{-8}$
29	1	36498535/95956876917664	$3.80364 \cdot 10^{-7}$
29	2	4/29090285629613	$1.37503 \cdot 10^{-13}$

8.2. Finite Checks and Rigorous Bounds.

Proposition 8.4. *For the data of Definition 8.1:*

- (a) $w_{r,i} > 0$ for every $r \in \mathcal{R}$ and $0 \leq i < n_r$;
- (b) the coefficients (7.2) are positive, and the tube constant satisfies $q_0 < 0.026$;
- (c) on each of the 64 squares $\mathcal{Q}$, the Bernstein coefficients of degree 3 of the restriction of P to $\mathcal{Q}$ are positive, and $\rho_{\mathcal{Q}} < 0.332$;
- (d) every cross satisfies (7.18).

Proof. These are finite checks, made by the supplementary program `geom241.py` as described in Subsection 8.5. The comparisons in (a)–(c), and the first condition in (d), are exact comparisons of rational numbers; the other two conditions in (d) are checked by outward-rounded interval evaluation of $\log(4/a)$. $\square$

Proposition 8.5. *For the data of Definition 8.1, with Z_* , $J_{\mathbb{C}}^*$ and $\mathcal{M}_*$ as in Definition 8.3, the following hold.*

- (a) With T and T' independent with density qt^{q-1} on $(0, 1)$,
- $$(8.6) \quad 38.7888697256861058 < \bar{A}_{\mathbb{C}} = \mathbb{E} P(T, T')^p < 38.7888697256861071,$$
- and the right side of (7.23) is less than $5.9 \cdot 10^{-16}$.*
- (b) The expression Z_* satisfies
- $$(8.7) \quad 348.4186894704059951 < Z_* < 348.4186894704059952,$$
- and the remainder term satisfies $E_{-,1} < 6.1 \cdot 10^{-17}$.*
- (c) $1.3556525171042125 < J_{\mathbb{C}}^* < 1.3556525171042127$.
 - (d) $-0.2107595968649958 < J_{\mathbb{R}} < -0.2107595968649957$.
 - (e) $0.7214954821109038790 < \sum_{r \in \mathcal{R}} \log \mathcal{F}_{\delta,r} / (e_r f_r) < 0.7214954821109038791$.

- (f) The numbers $H = \sum_r k_r \log r / e_r$ and $\ell = \frac{9}{4} \log 2 + \frac{1}{2} \log 3615$ satisfy
 $15.6917787983405342 < H < 15.6917787983405343$,
 $5.6560047235563094 < \ell < 5.6560047235563095$.

(g) $\log K_{\mathbb{C}} < 0.0491254364$, $\sigma_{\mathbb{C}} > 1.7518755886$ and $\mu = 2e^{H/2-\ell} > 17.8683654522$.

(h) $0.6324418249848039 < -\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}^* < 0.6324418249848040$.

(i) The lower bound for the margin satisfies

$$(8.8) \quad \mathcal{M}_*(\theta_*) > 0.000176730033534598.$$

Proof. The supplementary program `geom241.py` evaluates these quantities in outward-rounded interval arithmetic from the exact data, as described in Subsection 8.5: (a) by Proposition 7.20; (b) from (7.19), with Lemma 7.26 for the digamma values; (c) from (7.25); (d) from (7.4); (e) from (8.2); (f) from the definitions of H and ℓ ; (g) from Lemma 7.12 and the definition of μ ; and (h) and (i) from Definition 8.3, where $\bar{A}_{\mathbb{C}}^*$ is the upper end of the enclosure computed for (a). $\square$

In (b), the upper endpoint bounds the expression Z_* , not the overlap $I_{\mathbb{C}}$. The proof of Theorem 1.1 uses Proposition 8.4 and, from Proposition 8.5, only the fact, established by the computation for (a), that $\bar{A}_{\mathbb{C}} \leq \bar{A}_{\mathbb{C}}^*$, the positivity of Z_* given by (b), and (g), (h) and (i); the other bounds in Proposition 8.5 are not used in the proof. Table 8 lists the terms of $\mathcal{M}_*(\theta_*)$.

TABLE 8. The terms of $\mathcal{M}_*(\theta_*)$, rounded to ten decimals.

Term	Value
$\sum_r \log \mathcal{F}_{\delta,r} / (e_r f_r)$	0.7214954821
$-(1/2 - \delta)\ell$	-2.5863212799
$-C$	-0.0487128500
$(1 - \delta) \log 2$	0.6635290015
$(1 - \theta_*) \log \pi$	0.5723736765
$(1 - 2\theta_*)J_{\mathbb{R}}$	-0.0000032159
$\theta_* J_{\mathbb{C}}^*$	0.6778159157
$\mathcal{M}_*(\theta_*)$	0.0001767300

8.3. Conclusion of the Proof.

Corollary 8.9. *The pair $(f_{\mathbb{R}}, g_{\mathbb{C}})$ of Definition 8.1 is admissible with Fourier constants $M = 2$ and $\sigma = 1$, and these satisfy (5.19) with $\mu = 2e^{H/2-\ell}$.*

Proof. Proposition 7.13 applies, since $s \geq 1$, $a > 0$, $a_{\mathbb{R}} \leq 1$ and $0 < \rho < 1$, the Bernstein coefficients (7.2) of degree $m = 3$ are positive, and $q_0 < 1$ (Proposition 8.4(b)). It gives the Fourier constants $M = \max\{2, \sqrt{K_{\mathbb{C}}}\}$ and $\sigma = \min\{1, \sigma_{\mathbb{C}}\}$. By Proposition 8.5(g), $K_{\mathbb{C}} < 4$ and $\sigma_{\mathbb{C}} > 1$, so $M = 2$ and $\sigma = 1$. The right side of (5.19) is then $\log 50 + 2 < 5.9121$, while $\sigma\mu = \mu > 17.8683654522$ by Proposition 8.5(g). $\square$

Lemma 8.10. *For the data of Definition 8.1, $J_{\mathbb{C}} \geq J_{\mathbb{C}}^*$. Consequently, for $\theta_* \leq \theta < 1/2$, the margin $\mathcal{M}_{\mathcal{R}}(\theta)$ of Corollary 6.23 for these data satisfies*

$$\mathcal{M}_{\mathcal{R}}(\theta) \geq \mathcal{M}_*(\theta) \geq \mathcal{M}_*(\theta_*) > 0.000176730033534598.$$

Proof. Corollary 7.24 applies: the hypotheses of Propositions 7.17 and 7.20 hold by Proposition 8.4(c),(d), $Z_* > 0$ by (8.7), and $\bar{A}_{\mathbb{C}} \leq \bar{A}_{\mathbb{C}}^*$ by Proposition 8.5(a) and Definition 8.3. Hence $J_{\mathbb{C}} \geq J_{\mathbb{C}}^*$. Since $\mathcal{M}_{\mathcal{R}}(\theta) - \mathcal{M}_*(\theta) = \theta(J_{\mathbb{C}} - J_{\mathbb{C}}^*)$ and $\theta \geq 0$, we get $\mathcal{M}_{\mathcal{R}}(\theta) \geq \mathcal{M}_*(\theta)$. The function $\mathcal{M}_*$ is affine in θ with slope $-\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}^*$, which is positive by Proposition 8.5(h); so $\mathcal{M}_*(\theta) \geq \mathcal{M}_*(\theta_*)$ for $\theta \geq \theta_*$, and (8.8) completes the proof. $\square$

Proof of Theorem 1.1. For each $n \geq 49$, let $K^{(n)}/B$ be a Galois extension with $[K^{(n)} : B] = 2^n$ as in Theorem 2.42, let ι_1 be a complex conjugation at a place of $K^{(n)}$ above the real place v_1 of B , put $F^{(n)} = (K^{(n)})^{\langle \iota_1 \rangle}$ and $d_n = [F^{(n)} : \mathbb{Q}]$, and let θ_n be the value of θ for $F^{(n)}$. By Theorem 4.2, $d_n^{-1} \log L_{F^{(n)}}(1) < C$ for all sufficiently large n ; we discard the finitely many other fields.

We apply Corollary 6.23 to this sequence, with $\delta = 0.04273$, the exponents k_r , the weights $w^{(r)} = (w_{r,i} w_{r,j})_{i,j \geq 0}$ and the pair $(f_{\mathbb{R}}, g_{\mathbb{C}})$ of Definition 8.1, and check its hypotheses. By Theorem 2.42, each $K^{(n)}/F^{(n)}$ satisfies (G1)–(G3) with the common $\lambda = 2^{9/4} \sqrt{3615}$, $d_n = 2^n \rightarrow \infty$, and all these extensions have the uniform local types $(e_r, f_r)_{r \in \mathcal{R}}$ of Table 5. By the choice above, $\log L_{F^{(n)}}(1) \leq d_n C$. The weights are as in Definition 6.5, since $w_{r,0} = 1$, $w_{r,i} > 0$ for $i < n_r$ by Proposition 8.4(a), and $w_{r,i} = 0$ for $i \geq n_r$. The pair $(f_{\mathbb{R}}, g_{\mathbb{C}})$ is admissible, with Fourier constants that satisfy (5.19) with $\mu = 2e^{H/2-\ell}$, by Corollary 8.9. Finally, $\theta_* \leq \theta_n < 1/2$ by Theorem 2.42, so Lemma 8.10 gives $\mathcal{M}_{\mathcal{R}}(\theta_n) \geq \mathcal{M}_*(\theta_*) > 0$ for all n .

Corollary 6.23 therefore gives finite sets $U_n \subset \mathbb{R}^2$ with $|U_n| \rightarrow \infty$ and $u(U_n)/|U_n|^{1+\delta} \rightarrow \infty$, where $1 + \delta = 1.04273$; these are the sets of Theorem 1.1, indexed by n . In particular $u(U_n) \geq |U_n|^{1.04273}$ for all large n , which gives the last assertion of Theorem 1.1 at the cardinalities $|U_n|$. $\square$

8.4. Remarks.

Remark 8.11. The proof uses the bound $\theta \geq \theta_*$ only through Lemma 8.10, that is, through the positivity of $\mathcal{M}_*$ on $[\theta_*, 1/2)$. The program `geom241.py` also encloses the value at $\theta = 0$ and the zero θ_0 of the affine function $\mathcal{M}_*$:

$$\mathcal{M}_*(0) < -0.316, \quad \theta_0 < 0.49971293.$$

So $\mathcal{M}_*(\theta) > 0$ for $\theta \geq 0.49971293$; these enclosures are not used in the proof. By Theorem 2.42, $b/d = 1/(2N_\ell)$, where N_ℓ is the number of conjugates of ι_1 in $\text{Gal}(K/B)$, so that $\theta = 1/2 - 1/(4N_\ell)$. Hence $N_\ell \geq 871$ would suffice, whereas that theorem gives $N_\ell \geq 2^{15}$. On the other hand, at $\theta = 0$ the margin $\mathcal{M}_{\mathcal{R}}(0)$ does not involve $J_{\mathbb{C}}$ and equals $\mathcal{M}_*(0) < 0$: with these profiles, mixed signature is essential.

Remark 8.12. The following numerical observations are not used in the proof. For the unweighted shell profiles with the same exponents k_r , the sum in Proposition 8.5(e) is replaced by $J - \delta H < 0.7165268434$. The proof of Proposition 6.21 needs only some $\eta > 0$ with 4η below the lower bound of the margins, where η is the auxiliary parameter of that proof; for instance, $\eta = 10^{-9}$ gives

$$(8.13) \quad \mathcal{M}_*(\theta_*) - 4\eta > 0.000176726033534598 > 0.$$

The value $\mathcal{M}_*(\theta_*)$ is small compared with the individual terms in Table 8. Since $\mathcal{M}_*$ decreases with slope 1 in C and with slope $1/2 - \delta$ in ℓ , it would be absorbed by an increase of $1.77 \cdot 10^{-4}$ in C , or of $3.87 \cdot 10^{-4}$ in ℓ . For $\delta = 0.0428$, with the same pair profile $g_{\mathbb{C}}$ (the same s , a and coefficients (7.2)), the Gaussian of Lemma 7.3 for this δ , the same C , and exponents and weights produced by the optimization program `shells241.py` for this δ (its exponents k_r and numbers n_r agree with Table 6), the same evaluation gives $\mathcal{M}_*(\theta_*) < -0.0015$.

Remark 8.14. The weights $w_{r,i}$ are nonincreasing in i ; this is an exact rational comparison. So g_r is the nonnegative combination $\sum_{i,j} (w_{r,i} - w_{r,i+1})(w_{r,j} - w_{r,j+1}) \mathbf{1}_{\mathcal{B}_i \times \varpi^{-k_r} \mathcal{B}_j}$ of indicators of products of balls. As a consistency check, the rational number $Z(g_r)Q_r^{-k_r}$ is computed twice for each r : from (6.11), and from this combination and (6.4). The two exact values agree.

8.5. Computations. The program `geom241.py` evaluates the formulas of Sections 6 and 7 for the data of Definition 8.1: the local functionals (8.2) from the exponents and weights of Tables 6 and 7, and the quantities of Propositions 7.20 and 7.17, of Lemma 7.12 and of Corollary 7.24 from the profile data. For these it uses, unchanged, three modules of an earlier supplementary archive of the author (Subsection 1.6), which implement exactly these formulas. In Proposition 7.20 it uses the symmetry of (7.2): each square off the diagonal is evaluated once and counted twice. The program

checks the hypotheses listed in Proposition 8.4 (for (c), on the squares on or above the diagonal; the others follow by the symmetry of (7.2), since the restriction of P to a reflected square has the transposed Bernstein coefficients), the conditions $a_{\mathbb{R}} \leq 1$, $\sigma_{\mathbb{C}} > 1$, $\log K_{\mathbb{C}} < 2 \log 2$ and $\mu > 10$ (which implies (5.19) for $M = 2$ and $\sigma = 1$, since $\log 50 + 2 < 10$), and the positivity of the slope in Proposition 8.5(h); it also makes the consistency check of Remark 8.14. It then prints the enclosures stated in this section. The exponents and weights were produced by the separate optimization program `shells241.py`; they enter the proof only as the exact rational data of Table 7.

Rational quantities are computed exactly: q_0 , the restrictions of P to the squares and their Bernstein coefficients, the coefficients of the powers W_Q^k and the binomial coefficients in Proposition 7.20, G_n and $\tilde{G}_n$, and the shell sums S_r and R_r ; the polynomial arithmetic is done with integers after clearing denominators. The remaining quantities involve the logarithm, the exponential (also through the real powers $x^y = \exp(y \log x)$ in (7.22), in c_Q^p and in $w_{r,i}^p$), the square root in $\sigma_{\mathbb{C}}$, the constant π , and the digamma function, which enters only through Lemma 7.26; that lemma is applied with exact rational arguments and Bernoulli numbers, $L = 64$ and $k_* = 16$, without rounding the rational parameters of the profile. These quantities are evaluated in the interval arithmetic of `mpmath` [40], which computes each arithmetic operation and each of these elementary functions with the lower endpoint rounded down and the upper endpoint rounded up, at a working precision of 80 decimal digits; exact rational algebra followed by interval evaluation keeps the bound of Proposition 7.20 valid despite the cancellation in (7.22). Hence every computed interval contains the exact value, and the decimals stated above, which are coarser than the working precision by more than fifty orders of magnitude, are rigorous bounds.

REFERENCES

1. Noga Alon, Thomas F. Bloom, W. T. Gowers, Daniel Litt, Will Sawin, Arul Shankar, Jacob Tsimerman, Victor Wang, and Melanie Matchett Wood, *Remarks on the disproof of the unit distance conjecture*, 2026, arXiv:2605.20695v1; <https://arxiv.org/abs/2605.20695v1>.
2. Leonardo de Moura and Sebastian Ullrich, *The Lean 4 theorem prover and programming language*, Automated Deduction—CADE 28 (Cham) (André Platzer and Geoff Sutcliffe, eds.), Lecture Notes in Computer Science, vol. 12699, Springer, 2021, pp. 625–635.
3. Tim Dokchitser, *Computing special values of motivic L-functions*, Experimental Mathematics **13** (2004), no. 2, 137–149.
4. Michael T. M. Emmerich, *Optimizing explicit unit-distance lower-bound certificates*, 2026, arXiv:2606.03419v5, June 9, 2026 (v1 June 2, 2026); certificate with $\delta = 0.015263\dots$; <https://arxiv.org/abs/2606.03419v5>.
5. Michael T. M. Emmerich and Francesco Cordella, *Optimized certificate for the unit distance problem with extended prime number range*, Zenodo record, June 5, 2026, Certificate and verification code. <https://doi.org/10.5281/zenodo.20551478>.
6. Paul Erdős, *On sets of distances of n points*, The American Mathematical Monthly **53** (1946), no. 5, 248–250, <https://doi.org/10.1080/00029890.1946.11991674>.
7. ———, *Some problems in number theory, combinatorics and combinatorial geometry*, Mathematica Pannonica **5** (1994), no. 2, 261–269.
8. Mikhail Ershov, *Golod–Shafarevich groups: a survey*, International Journal of Algebra and Computation **22** (2012), no. 5, 1230001, 68 pages.
9. Ralph H. Fox, *Free differential calculus. I: Derivation in the free group ring*, Annals of Mathematics **57** (1953), no. 3, 547–560.
10. E. S. Golod and I. R. Shafarevich, *On the class field tower*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), no. 2, 261–272 (Russian), English translation: Amer. Math. Soc. Transl. (2) **48** (1965), 91–102; <https://www.mathnet.ru/eng/im2955>.
11. Farshid Hajir, Christian Maire, and Ravi Ramakrishna, *Cutting towers of number fields*, Annales mathématiques du Québec **45** (2021), no. 2, 321–345.
12. Erich Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. Zweite Mitteilung*, Mathematische Zeitschrift **6** (1920), 11–51, <https://doi.org/10.1007/BF01202991>.
13. S. A. Jennings, *The structure of the group ring of a p -group over a modular field*, Transactions of the American Mathematical Society **50** (1941), no. 1, 175–185, <https://doi.org/10.2307/1989916>.

14. Fredrik Johansson, *Rigorous high-precision computation of the Hurwitz zeta function and its derivatives*, Numerical Algorithms **69** (2015), no. 2, 253–270.
15. ———, *Arb: Efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Transactions on Computers **66** (2017), no. 8, 1281–1292, <https://doi.org/10.1109/TC.2017.2690633>.
16. Stéphane Louboutin, *Explicit bounds for residues of Dedekind zeta functions, values of L -functions at $s = 1$, and relative class numbers*, Journal of Number Theory **85** (2000), no. 2, 263–282, <https://doi.org/10.1006/jnth.2000.2545>.
17. James S. Milne, *Lectures on étale cohomology*, 2013, Version 2.21, March 22, 2013; <https://www.jmilne.org/math/CourseNotes/LEC.pdf>.
18. ———, *Algebraic number theory*, 2020, Version 3.08, July 19, 2020; <https://www.jmilne.org/math/CourseNotes/ANT.pdf>.
19. ———, *Class field theory*, 2020, Version 4.03, August 6, 2020; <https://www.jmilne.org/math/CourseNotes/CFT.pdf>.
20. mlewko, *Post in the discussion thread of Erdős Problem #90*, Erdős Problems forum, May 21, 2026, Reports $\delta = 0.031849981 \dots$ in Sawin’s criterion, with finite data found by ChatGPT; accessed September 30, 2026; <https://www.erdosproblems.com/forum/thread/90>.
21. Eric Naslund, *Answer to “What is the unit distance exponent?”*, MathOverflow, answer 511576, 2026, Posted May 23, 2026, last edited June 9, 2026; accessed September 30, 2026; <https://mathoverflow.net/a/511576>.
22. ———, *An exponent of 1.04273 for the unit distance problem: Lean formalization at exponent 1.0427, conditional on one zeta inequality*, Palomar registry, PALOMAR-2026-10-01-000018, version 1, 2026, <https://palomar-registry.org/entry?id=PALOMAR-2026-10-01-000018&version=1>; Lean 4 source at <https://github.com/enaslund/unit-distance-bound-0.0427/tree/e0ac836176016dbefae28646bc91fc3a5aca30e8/lean>.
23. ———, *An improved explicit lower bound for the unit distance problem*, Unpublished manuscript, 2026, Records exponent 1.0358324. <https://github.com/enaslund/unit-distance-bound-0.0427/tree/8ab94da4ba4faf6f6d8fe43c298f04c3b284e796/papers/0.0358324>.
24. ———, *Supplementary programs and data for “An exponent of 1.04273 for the unit distance problem”*, GitHub repository, directory `papers/0.04273/certificates`, 2026, <https://github.com/enaslund/unit-distance-bound-0.0427>.
25. National Institute of Standards and Technology, *NIST Digital Library of Mathematical Functions*, 2026, Release 1.2.8, September 15, 2026; accessed September 27, 2026; <https://dlmf.nist.gov/>.
26. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2 ed., Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, Berlin, Heidelberg, 2008.
27. OpenAI, *Planar point sets with many unit distances*, Research manuscript, May 20, 2026, <https://cdn.openai.com/pdf/74c24085-19b0-4534-9c90-465b8e29ad73/unit-distance-proof.pdf>.
28. *Erdős unit distance exponent*, Entry 84a of *Optimization Constants in Mathematics*, a crowdsourced repository started by Terence Tao, 2026, Accessed September 30, 2026; <https://teorth.github.io/optimizationproblems/constants/84a.html>.
29. Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017, <https://math.mit.edu/~poonen/papers/Qpoints.pdf>.
30. Claudio Quadrelli, *Pro- p groups with few relations and universal Koszulity*, Mathematica Scandinavica **127** (2021), no. 1, 28–42, <https://doi.org/10.7146/math.scand.a-123644>.
31. D. G. Quillen, *On the associated graded ring of a group ring*, Journal of Algebra **10** (1968), no. 4, 411–418, [https://doi.org/10.1016/0021-8693\(68\)90069-0](https://doi.org/10.1016/0021-8693(68)90069-0).
32. Will Sawin, *An explicit lower bound for the unit distance problem*, 2026, arXiv:2605.20579v1; <https://arxiv.org/abs/2605.20579v1>.
33. Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, New York, 1973.
34. Joel Spencer, Endre Szemerédi, and William T. Trotter, Jr., *Unit distances in the Euclidean plane*, Graph Theory and Combinatorics (Béla Bollobás, ed.), Academic Press, London, 1984, <https://trotter.math.gatech.edu/papers/44.pdf>, pp. 293–303.
35. spiderduckpig, *Answer to “What is the unit distance exponent?”*, MathOverflow, answer 511531, 2026, Posted May 21, 2026, with $1 + \delta \geq 1.03188306553964 \dots$; comment of May 22, 2026 proposing a weighted count in the Zassenhaus filtration in Sawin’s Golod–Shafarevich step, with $\delta \geq 0.0333487156372102$; last edited June 9, 2026; accessed September 30, 2026; <https://mathoverflow.net/a/511531>.
36. László A. Székely, *Crossing numbers and hard Erdős problems in discrete geometry*, Combinatorics, Probability and Computing **6** (1997), no. 3, 353–358, <https://doi.org/10.1017/S0963548397002976>.
37. John T. Tate, *Fourier analysis in number fields and Hecke’s zeta-functions*, Algebraic Number Theory (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, London, 1967, Originally a Princeton University doctoral thesis, 1950; <https://www.lms.ac.uk/publications/algebraic-number-theory>, pp. 305–347.

- 38. The FLINT team, *FLINT: Fast Library for Number Theory*, 2026, Version 3.6.0, used through python-flint 0.9.0; <https://flintlib.org>.
- 39. The mathlib Community, *The Lean mathematical library*, Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, ACM, 2020, pp. 367–381.
- 40. The mpmath development team, *mpmath: A Python library for arbitrary-precision floating-point arithmetic*, 2023, Version 1.3.0; <https://github.com/mpmath/mpmath/releases/tag/1.3.0>.
- 41. The PARI Group, *PARI/GP*, Université de Bordeaux, 2025, Version 2.17.2; <https://pari.math.u-bordeaux.fr/>.
- 42. M. A. Tsfasman and S. G. Vlăduț, *Infinite global fields and the generalized Brauer–Siegel theorem*, Moscow Mathematical Journal **2** (2002), no. 2, 329–402, <https://doi.org/10.17323/1609-4514-2002-2-2-329-402>.

Email address: `naslund.math@gmail.com`