

# AN EXPONENT OF 1.043 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  $u(U_j)/|U_j|^{1.043171} \rightarrow \infty$ . The largest exponent previously claimed, apart from preliminary versions of the present work, is 1.0358, in the author's unpublished manuscript. The method is the number-field construction of OpenAI and Sawin. Here unit distances come from elements of relative norm one in quadratic extensions  $K/F$  in which  $F$  has both real and complex places, and the fields come from an infinite pro-2 tower over  $\mathbb{Q}(\sqrt{241})$ , ramified only above 2, 3 and 5, with Frobenius conditions at the two primes above 29 and at one prime above 41. The relative zeta value is bounded through the dihedral quotients of the tower group: the tower group has 27 quotients isomorphic to the dihedral group of order 8; fifteen of them detect, by a census, the residue degree of the primes that split completely in the Kummer field up to norm  $4 \cdot 10^{13}$ , and seven of them generate a field  $E_{W''}$  of degree 8192 contained in every field of the tower. We write  $\zeta_{E_{W''}}$  as a product of  $L$ -functions of degrees 2, 4 and 8, evaluate the 576 of degrees 4 and 8 rigorously at 21 real points near 1, and combine the values through a kernel inequality with coefficients of both signs. Finite facts and numerical inequalities are certified by exact computation and interval arithmetic. Partial formalization PALOMAR-2026-10-01-000018 v2 [21].

**\*AI Methodology.** This work was done with extensive AI use, with agents developing the mathematics, writing the programs and writing the paper; I supervised, prompted, and coordinated them. The choice of the Frobenius condition at a prime above 41, rather than at the prime 7 (Section 2), was found in an agent run of the Muse Spark system. The refinements of the bound for the relative zeta value (Sections 4–7), the general shell weights, the certificates and this paper were produced with Claude Opus 5.5 working as an agent in Claude Code. Preliminary versions of this work, on which the construction builds, were produced with Claude Opus 5.5, ChatGPT Sol 5.6 and ChatGPT Astra 6. The reviews mentioned in Subsection 1.5 are automated reviews by AI agents in fresh contexts, not human peer review. I have had the agents provide a clearer introduction, and a dependency graph on page 4 to help navigate the paper and the proof, and make it easier to read. However I still recommend that the reader navigate this paper with their AI model of choice, and to ask the paper questions.

## 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 [5] 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*

$$\frac{u(U_j)}{|U_j|^{1.043171}} \rightarrow \infty.$$

*In particular,  $u(n) \geq n^{1.043171}$  for arbitrarily large integers  $n$ .*

---

*Date:* October 8, 2026.

The theorem concerns an unbounded sequence of cardinalities; it asserts nothing for every sufficiently large  $n$ . Its proof uses no unproved hypothesis, such as the generalized Riemann hypothesis, but it is computer-assisted: finite facts about the tower, a census of primes, and many numerical inequalities, among them enclosures of the values of 576  $L$ -functions near  $s = 1$ , are verified by exact computation and interval arithmetic (Subsection 1.8).

The largest exponent previously claimed, apart from preliminary versions of the present work, is 1.0358, in the author’s unpublished manuscript [22]. The method is the number-field construction of OpenAI [26] and Sawin [32]. Subsection 1.4 describes the ingredients that give the present exponent: fields of mixed signature from a tower over  $\mathbb{Q}(\sqrt{241})$ , the local conditions of that tower, a bound for the relative zeta value through the dihedral quotients of the tower group, and general weights at the selected primes (the primes used for equal-norm choices, Subsection 1.2). The paper is self-contained, apart from the cited standard results and the supplementary programs.

**1.1. Background.** Erdős [5] 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 [5, 6]. The best upper bound,

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

is due to Spencer, Szemerédi and Trotter [35]; Székely [37] gave a proof by crossing numbers.

In 2026 a team at OpenAI [26] 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  $\text{rd}(M) = |\Delta_M|^{1/[M:\mathbb{Q}]}$  ( $\Delta_M$  the discriminant). Alon, Bloom, Gowers, Litt, Sawin, Shankar, Tsimmerman, Wang and Wood [1] simplified the argument, and Sawin [32] made every step explicit and reached the exponent 1.014114. Improvements followed in online discussions [19, 36, 20], and the author’s manuscript [22] recorded 1.0358324. The present paper uses a tower over  $\mathbb{Q}(\sqrt{241})$  and quadratic extensions  $K/F$  of *mixed signature*, that is, with  $F$  having both real and complex places. Table 1 lists the explicit exponents, and the repository [27] 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. 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 [5]              | integer lattice                                                                               | journal                    |
| $1 + \delta, \delta > 0$ | OpenAI [26]            | 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 [3]           | optimized parameters                                                                          | preprint                   |
| 1.031185                 | Emmerich, Cordella [4] | extended range of primes                                                                      | online certificate         |
| 1.031849                 | mlewko [19]            | finite data found by ChatGPT                                                                  | forum post                 |
| 1.0333487                | spiderduckpig [36]     | weighted Zassenhaus count                                                                     | online post                |
| 1.0358324                | Naslund [22, 20]       | covolume counting, dyadic<br>ramification, fixed-subfield Euler products                      | manuscript,<br>online post |
| 1.043171                 | this paper             | tower over $\mathbb{Q}(\sqrt{241})$ , mixed signature,<br>dihedral quotients (Subsection 1.4) |                            |

**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  $\iota$  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  $\iota$  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  $\mathfrak{p}^k$ ; the primes used in this way are the *selected primes* (they lie above the selected primes of  $B$  of Definition 4.16). Second, ideal classes: keeping the products of such ideals that lie in one class of  $\text{Cl}(K)$  modulo the image of  $\text{Cl}(F)$  loses at most a factor equal to the order of that quotient (Lemma 8.11). Through the class-number formula, this loss is governed by the root discriminant  $\lambda = \text{rd}(K)$  of  $K$  (Definition 2.44), which equals that of  $F$  because  $K/F$  will be unramified at the finite places, 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  $k$  makes the ideal lattice denser by the factor  $N\mathfrak{p}^k$ , which costs  $\delta k \log N\mathfrak{p}$  before division by  $d$ .

Quantitatively, suppose that such fields exist with  $d \rightarrow \infty$ , a fixed root discriminant  $\lambda$ , and selected primes of fixed local types (ramification index and residue degree, Definition 2.45). Let  $(b, c)$  be the signature of  $F$ , so that  $d = b + 2c$ , and put  $\theta = c/d$ . If  $C$  is an upper bound for  $d^{-1} \log L_F(1)$ , then the exponent  $1 + \delta$  is attained when the *margin*

$$(1.2) \quad \frac{1}{d} \sum_{\mathfrak{p}} \log \mathcal{F}_{\delta, \mathfrak{p}} - \left( \frac{1}{2} - \delta \right) \log \lambda - C + (1 - \delta) \log 2 + (1 - \theta) \log \pi + (1 - 2\theta) J_{\mathbb{R}} + \theta J_{\mathbb{C}}$$

is bounded below by a positive constant. Here the sum runs over the selected primes of  $F$ , and  $\mathcal{F}_{\delta, \mathfrak{p}}$  is the value of the local functional of Definition 9.3 at the weight function placed at  $\mathfrak{p}$ , a *shell profile* (Definition 9.7); for an unweighted profile used with exponent  $k$  at a prime of norm  $Q$  it is  $(k+1)Q^{-\delta k}$ . The numbers  $J_{\mathbb{R}}$  and  $J_{\mathbb{C}}$  are functionals of the profiles at the real and complex places of  $F$  (Definition 8.28). This is Proposition 9.26, the geometric transfer with shell profiles; Section 11 proves that the margin is positive at  $\delta = 0.043171$ .

The fields come from a tower: a pro-2 extension of  $B = \mathbb{Q}(\sqrt{241})$  with restricted ramification and prescribed local Galois groups. Its Galois group is the *tower group*  $G_B$  (Definition 2.23), a pro-2 group; we write  $(D_n G_B)_{n \geq 1}$  for its Zassenhaus filtration and  $\text{gr}_n G_B = D_n G_B / D_{n+1} G_B$  for its graded pieces (recalled at the start of Section 2). The tower is infinite because its Golod–Shafarevich function  $P_B$  of (2.41) takes a negative value [9, 10]. Its fields have  $\lambda = 2^{9/4} \sqrt{3615} \approx 286.0$ , the field  $F$  is the fixed field of one complex conjugation  $\iota_1$ , whose conjugacy class in  $G_B / D_4 G_B$  has  $2^{15}$  elements (Lemma 2.30(c)), which forces  $b/d \leq 2^{-16}$  and  $\theta \geq \theta_* = 65535/131072$  (Theorem 2.46).

**1.3. The structure of the proof.** Figure 1 shows how the main statements depend on each other. The proof has four parts: Parts (II)–(IV) apply to the fields of Part (I); Parts (II) and (III) are independent of each other and meet in the final inequality of Part (IV).

- (I) *The fields* (Section 2). A presentation of the Galois group of the maximal pro-2 extension of  $B$  unramified outside 2, 3, 5, the local conditions, and the Golod–Shafarevich criterion show that the tower is infinite (Proposition 2.43); the graded pieces of its Zassenhaus filtration (Lemmas 2.29 and 2.30) give the root discriminant, the local types and the signature of its fields (Theorem 2.46).
- (II) *The relative zeta value* (Sections 3–7). A limit lemma (Lemma 4.13) and the signed kernel inequality (Proposition 4.19) reduce  $d^{-1} \log L_F(1)$  to values of a zeta function at real points  $\sigma_j > 1$  and to *floors*: lower bounds for the residue degrees of the *free* primes of  $B$ , those other than the selected ones (Definitions 4.16 and 4.18). The dihedral quotients of  $G_B$  supply

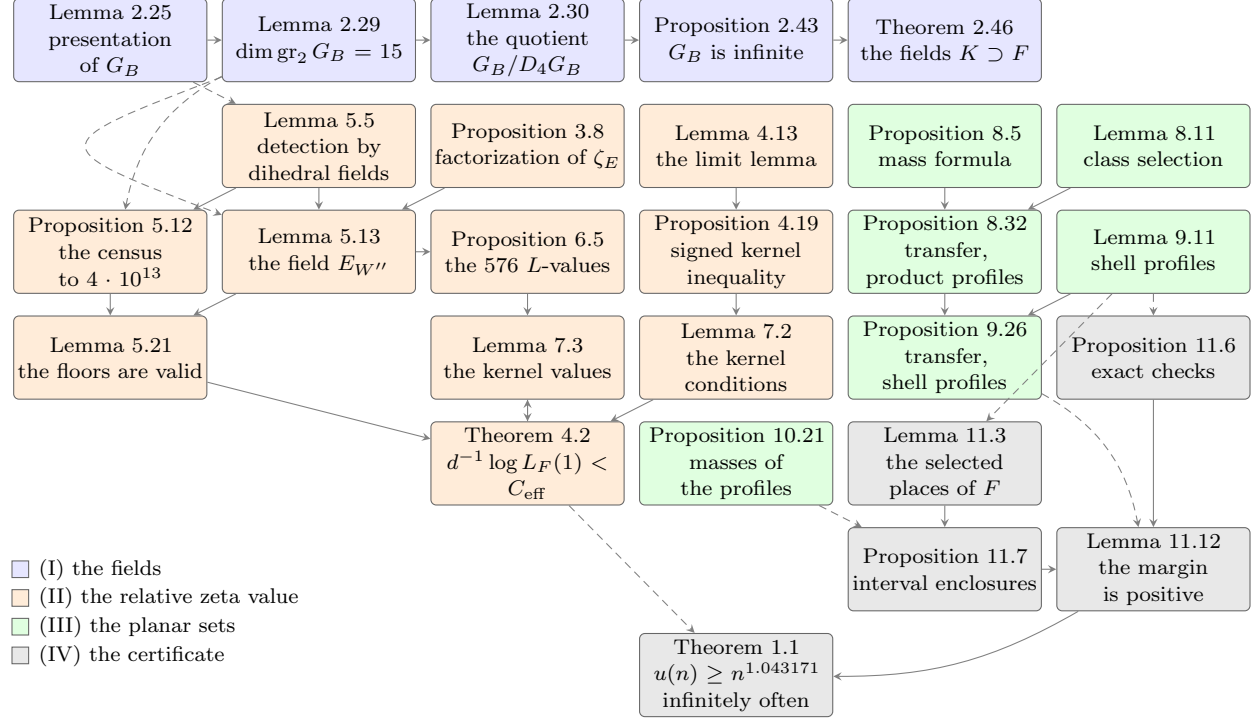


FIGURE 1. The structure of the proof (Subsection 1.3). Each box is a numbered statement, coloured by the part of the proof it belongs to. An arrow goes from a statement to each statement whose proof uses it, directly or through statements not shown, except that arrows implied by a chain of drawn arrows are left out; dashed arrows join different parts. The arrows from Theorem 2.46, which supplies the fields to which Parts (II)–(IV) apply, are also left out. Appendix B lists the citations between all numbered statements; the notation is collected in Subsection 1.7.

the floors, through a census of primes (Proposition 5.12), and a field  $E_{W''}$  of degree 8192 (Definition 5.7), whose zeta function factors into the  $L$ -functions of Lemma 5.13. Their values (Proposition 6.5) and the kernel (Lemmas 7.2 and 7.3) give the bound  $C_{\text{eff}} = 0.0422764$  for  $d^{-1} \log L_F(1)$  (Theorem 4.2).

- (III) *The planar sets* (Sections 8–10). A mass formula for ideal lattices (Proposition 8.5), the class selection (Lemma 8.11) and local and archimedean profiles give the transfer Proposition 9.26: for fields as in (I), the exponent  $1 + \delta$  is attained when the margin (1.2) is positive.
- (IV) *The certificate* (Section 11). Exact checks and interval enclosures of the local functionals, the profile integrals and the margin at  $\delta = 0.043171$ , with  $C = C_{\text{eff}}$  from (II) (Theorem 4.2), complete the proof of Theorem 1.1.

The dependency index (Appendix B) lists, for each numbered statement, the numbered statements that it or its proof cites and the statements that cite it.

**1.4. The main ingredients.** *The base field and the signature.* In the construction of Sawin [32], and in [22], the field  $K$  is a CM field:  $F$  is totally real, so  $\theta = 0$ , and the norm-one units are finite. Sawin’s fields come from an unramified pro-2 tower over a real quadratic field ramified at 2 and at the thirteen odd primes up to 43, and their root discriminant is about  $1.6 \cdot 10^8$ . Here the base field is  $B = \mathbb{Q}(\sqrt{241})$ , the real quadratic field of smallest discriminant in which 2, 3 and 5 all split. The tower is ramified only at the six primes of  $B$  above 2, 3 and 5, with prescribed local Galois groups there, and is still infinite (Proposition 2.43); its fields have root discriminant  $\lambda \approx 286$ . The field  $K$

is totally imaginary and Galois over  $B$ , and  $F$  is the fixed field of one complex conjugation, which is not central, so that almost every place of  $F$  is complex and  $\theta \geq \theta_*$ . Above a complex place of  $F$  the two coordinates of a norm-one element can have different moduli, and the norm-one units, of rank  $c$ , move them along a lattice; averaging over a fundamental domain of that lattice counts the resulting pairs exactly, and the class-number formula cancels the regulator of these units (Proposition 8.5). By (1.2), mixed signature adds  $\theta(J_{\mathbb{C}} - 2J_{\mathbb{R}} - \log \pi)$  to the margin: with the profiles of Section 11, the lower bound for the margin proved there is positive for  $\theta \geq \theta_*$ , but would be below  $-0.312$  at  $\theta = 0$  (Remark 11.13).

*The caps.* The local conditions of the tower bound the order of the Frobenius elements by four (a *cap*) at the two primes above 29 and at one of the two primes of  $B$  above 41 (the prime 41 splits in  $B$ ). The capped primes are selected (Definition 4.16): the primes of  $F$  above them that split in  $K$  are used for equal-norm choices. A cap at the prime 7, the smallest prime inert in  $B$ , would cost the same in the Golod–Shafarevich function and would give the same quotient  $G_B/D_4G_B$  of the tower group, because every fourth power lies in  $D_4G_B$ . But the selected primes above 41 have residue field of order  $41^4$  instead of  $7^8$ , and their contribution to the margin is about twice as large.

*The relative zeta value.* The simplest bound for  $d^{-1} \log L_F(1)$ ,  $C = 0.04871285$  (Remark 4.36), compares  $\zeta_K$  prime by prime with the zeta function of the Kummer field  $E$ , the maximal elementary abelian subextension of the tower, with  $[E : \mathbb{Q}] = 512$ . With this bound the construction gives the exponent 1.042901. A prime of  $B$  that splits completely in  $E$  is then counted as if it split completely in  $K$ ; such primes carry about 0.005 of  $C$ . We recover most of this through the second graded piece  $\text{gr}_2 G_B = D_2G_B/D_3G_B$  of the Zassenhaus filtration, a vector space over  $\mathbb{F}_2$  of dimension 15 (Lemma 2.29):

- (a) Exactly 27 linear forms on it are of *dihedral type* (Definition 5.2): they come from quotients of  $G_B$  isomorphic to the dihedral group of order 8, each realized by an explicit field of degree 8 over  $B$  that lies in every field of the tower (Lemmas 5.5 and 5.6). Fifteen of them, with independent forms, detect the residue degree of every prime of degree one that splits completely in  $E$  up to norm  $4 \cdot 10^{13}$ , except those whose Frobenius lies in  $D_3G_B$  (Subsection 5.4).
- (b) The census cannot reach the infinite tail. Seven of the dihedral forms span a space  $W''$  of dimension four (Subsection 5.3), and the corresponding field  $E_{W''}$ , with  $[E_{W''} : \mathbb{Q}] = 8192$ , lies in every field of the tower (Subsection 5.5). Its zeta function is the product of  $\zeta_E$ , of the squares of 448 Hecke  $L$ -functions of quadratic characters of quartic fields, and of the fourth powers of 128 Hecke  $L$ -functions of quadratic characters of octic fields (Lemmas 5.13 and 5.16). Comparing with  $E_{W''}$  instead of  $E$  moves fifteen sixteenths of the remaining primes, at all norms, from residue degree one to two. No larger space of this kind has  $L$ -functions of degree at most 8.
- (c) We evaluate these  $L$ -functions rigorously at real points  $\sigma$  near 1, with approximate functional equations whose cut-off functions are certified for the four gamma factors that occur (Section 6); the octic  $L$ -functions have conductors up to  $7.2 \cdot 10^{20}$  and need Dirichlet coefficients up to  $1.06 \cdot 10^{11}$ .
- (d) The step from  $\sigma > 1$  to  $s = 1$  goes through the Tsfasman–Vlăduț inequality [42, Proposition 3.1] (Lemma 4.13(b)). Instead of one abscissa, we use a kernel  $K = \sum_j c_j g_{\sigma_j}$ , where  $g_{\sigma}(q) = -\log(1 - q^{-\sigma})$ , over 21 abscissae  $\sigma_j$  with coefficients  $c_j$  of both signs; it dominates the prime-by-prime contribution at  $s = 1$  up to a multiple of the Tsfasman–Vlăduț weight  $w(q) = 2 \log q \sum_{m \geq 1} (q^m + 1)^{-1}$  (Proposition 4.19).

Together these lower the bound for  $d^{-1} \log L_F(1)$  from 0.04871285 to  $C_{\text{eff}} = 0.0422764$  (Theorem 4.2). Since the margin falls by about 23.8 per unit of  $\delta$  and by 1 per unit of  $C$ , this is worth about 0.00027 in the exponent.

*General shell weights.* The shell profiles are weighted sums  $\sum_{i,j} w_{ij} \mathbf{1}_{\mathcal{S}_i \times \varpi^{-k} \mathcal{S}_j}$  over products of *shells*: in a local field with ring of integers  $\mathcal{O}$  and uniformizer  $\varpi$ ,  $\mathcal{S}_0 = \mathcal{O}$  and  $\mathcal{S}_i$  ( $i \geq 1$ ) is the set of elements of valuation  $-i$ , and  $k$  is the exponent used at the prime (Definition 9.7). Product weights  $w_{ij} = x_i x_j$  suffice for the exponent 1.043170; the local lemma allows any nonnegative weights (Lemma 9.11), and optimized symmetric  $10 \times 10$  matrices at the primes above 2, 3 and 5 add  $1.5 \cdot 10^{-5}$  to the margin.

Table 2 shows the successive certified exponents. Section 12 describes the steps that are not needed for Theorem 1.1, and what is known about the limits of the method.

TABLE 2. Successive exponents.  $C_{\text{eff}}$  is the bound for  $d^{-1} \log L_F(1)$  in force; each step keeps the previous ones, and the profiles are re-optimized at each exponent. Rows marked \* are intermediate certificates, described in Section 12; the proof of Theorem 1.1 uses the census, the signed kernel and the field  $E_{W''}$ , but not the adaptive dichotomy or the single-abscissa step. The row marked † was computed during the search, with product shell weights, and has no witness of its own; every other row has a witness (Subsection 1.8) and a replay program in the repository.  $E_W$  and  $E_{W'}$  are the fields of the spaces  $W \subset W' \subset W''$  of Section 12, and “ceiling over  $M$ ” means the bound for  $d^{-1} \log L_F(1)$  obtained with  $M$  as comparison field.

| step                                                                                    | $C_{\text{eff}}$ | exponent |
|-----------------------------------------------------------------------------------------|------------------|----------|
| caps above 29 and 41, comparison field $E$                                              | 0.04871285       | 1.042901 |
| *adaptive dichotomy (Propositions 12.4, 12.8)                                           | 0.048134265      | 1.042925 |
| *dihedral census to $10^{12}$                                                           | 0.0471692613     | 1.042965 |
| *ceiling over $E_W$ , $[E_W : \mathbb{Q}] = 2048$ , census to $10^{13}$                 | 0.0436495        | 1.043113 |
| *refined Tsfasman–Vlăduț step, one abscissa                                             | 0.0435763        | 1.043116 |
| *signed kernel, census to $8.5 \cdot 10^{14}$                                           | 0.0433891        | 1.043124 |
| *ceiling over $E_{W'}$ , $[E_{W'} : \mathbb{Q}] = 4096$                                 | 0.0427163        | 1.043152 |
| †ceiling over $E_{W''}$ , $[E_{W''} : \mathbb{Q}] = 8192$ , census to $4 \cdot 10^{13}$ | 0.0422764        | 1.043170 |
| general shell weights at 2, 3, 5                                                        | 0.0422764        | 1.043171 |

**1.5. Status.** The proof of Theorem 1.1 is complete as written, but parts of it rest on computations. Each computation is done by a supplementary program, named where it is used, in exact arithmetic or in outward-rounded interval arithmetic, and a replay program reruns the certificate (Subsection 1.8). The dihedral refinements, the signed kernel, the general shell weights and the intermediate certificates were checked by ten independent reviews by AI agents in fresh contexts, each given the statements, the arguments and the programs but not the author’s confidence or earlier verdicts. One review found a material error in an intermediate certificate: thirteen primes had been credited twice. It was corrected; the exponent of that step did not change. The other reviews found no error affecting the bounds; their minor points, among them gaps in the error accounting of the numerical programs, were fixed. No reviewer recomputed the octic  $L$ -values independently, since general-purpose software cannot reach their conductors; they rest on the method of Section 6 and its checks. The cap above 41 (Section 2) has had two fresh-context reviews of its argument, but its finite computations have not had a full independent review. The manuscript as a whole had three further fresh-context reviews, which found no error affecting the theorem or any constant, and an audit of the floating-point arithmetic of the  $L$ -value programs found every bound rigorous. These are automated reviews, not human peer review.

A Lean formalization [21] of the tower of the present paper proves the planar conclusion with the exponent 1.04315 from one explicit inequality for  $\zeta_{E_{W''}}$  (Remark 4.38). The inequality is not proved in Lean, and the formalization does not cover the census beyond norm 1000, the signed kernel or the general shell weights, so it does not prove Theorem 1.1, even conditionally.

**1.6. Organization.** Section 2 constructs the tower and proves Theorem 2.46, which supplies the fields. Section 3 describes the Kummer field  $E$  and its quadratic  $L$ -functions. Section 4 reduces the relative zeta value to the primes of the fields of the tower, and proves the signed kernel inequality (Proposition 4.19). Section 5 treats the dihedral quotients, the census and the field  $E_{W''}$ ; Section 6 evaluates the  $L$ -functions of  $E_{W''}$ ; and Section 7 proves the bound  $C_{\text{eff}}$  (Theorem 4.2). Sections 8–10 carry out the geometric construction, with general shell weights. Section 11 proves the final inequality at  $\delta = 0.043171$  and completes the proof of Theorem 1.1. Section 12 records refinements that are not used, and the limits of the method. Appendix A lists the optimized shell weights, and the dependency index (Appendix B) lists, for every numbered statement, the statements it cites and those that cite it.

**1.7. Notation.** The following symbols keep one meaning throughout the paper. Other letters ( $H$ ,  $N$ ,  $\tau$ ,  $\beta$ ,  $\gamma$ ,  $\sigma$ ,  $\nu$ ,  $q$ ,  $s$ ,  $t$ , ...) are reused in different sections with local meanings, which are defined where they are introduced.

| symbol                                  | meaning                                                                                                                                 | defined in                    |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| $B, S$                                  | $B = \mathbb{Q}(\sqrt{241})$ ; $S$ the primes of $B$ above 2, 3, 5                                                                      | Section 2                     |
| $N$                                     | the absolute norm of an ideal                                                                                                           | Section 2                     |
| $\mathfrak{t}_1, \dots, \mathfrak{t}_4$ | the primes of $B$ above 29 and 41; the capped primes are $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$                               | Lemma 2.5, Definition 2.13    |
| $v_1, v_2, \Sigma$                      | the real places of $B$ ; $\Sigma = S \cup \{v_1, v_2\}$                                                                                 | Section 2                     |
| $B_S, G_S$                              | the maximal pro-2 extension of $B$ unramified at the finite primes outside $S$ , and its Galois group                                   | Section 2                     |
| $E$                                     | the Kummer field: the maximal elementary abelian 2-extension of $B$ in $B_S$ , $[E : \mathbb{Q}] = 512$                                 | Section 2                     |
| $\chi_e, \kappa_a$                      | the characters of $\text{Gal}(E/B)$ , with values $\pm 1$ and in $\mathbb{F}_2$                                                         | Definitions 3.1, 2.12         |
| $D_n G, \text{gr}_n G$                  | the Zassenhaus filtration of a pro-2 group $G$ and its graded pieces $D_n G / D_{n+1} G$                                                | Section 2                     |
| $G_B, B_G, \overline{G}_B$              | the tower group; the field $B_G \subset B_S$ of the tower, with $\text{Gal}(B_G/B) = G_B$ ; and $\overline{G}_B = G_B / D_4 G_B$        | Definition 2.23               |
| $\iota_1$                               | a complex conjugation at a place above $v_1$                                                                                            | Definition 2.13               |
| $\text{rd}(M), \lambda, \ell$           | root discriminant; $\lambda = 2^{9/4} \sqrt{3615}$ , the root discriminant of the fields of the tower; $\ell = \log \lambda$            | Definition 2.44, Theorem 2.46 |
| $\mathcal{K}, K, F, d$                  | the fields of the tower used; $K \in \mathcal{K}$ , $F = K^{\langle \iota_1 \rangle}$ , $d = [F : \mathbb{Q}]$                          | Definition 4.1                |
| $(b, c), \theta, \theta_*$              | the signature of $F$ ( $d = b + 2c$ ), $\theta = c/d$ , and the lower bound $\theta_* = 65535/131072$                                   | Theorem 2.46                  |
| $L_F(s)$                                | the relative zeta function $\zeta_K(s)/\zeta_F(s)$                                                                                      | Subsection 1.2                |
| $C, C_{\text{eff}}$                     | an upper bound for $d^{-1} \log L_F(1)$ ; the bound $C_{\text{eff}} = 0.0422764$ proved here                                            | Theorem 4.2                   |
| $e_K(\mathfrak{p}), f_K(\mathfrak{p})$  | ramification index and residue degree of a prime $\mathfrak{p}$ of $B$ in $K/B$                                                         | Section 4                     |
| $g_s(q), w(q), \kappa_\infty$           | $g_s(q) = -\log(1 - q^{-s})$ ; $w(q)$ the Tsfasman–Vlăduț weight, and $2\kappa_\infty$ the right side of the Tsfasman–Vlăduț inequality | Subsection 4.2                |
| $\beta_q, Z(s)$                         | limiting densities of primes of norm $q$ , and $Z(s) = \sum_q \beta_q g_s(q)$                                                           | Lemma 4.13                    |
| $Z_{\text{sel}}, T_{\text{sel}}$        | the parts of $Z$ and of the Tsfasman–Vlăduț sum from the selected primes                                                                | Subsection 4.3                |
| selected, free                          | the selected primes of $B$ (above 2, 3, 5 and the capped primes); the other primes of $B$                                               | Definition 4.16               |

| symbol                                              | meaning                                                                                                                               | defined in                       |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| $f_{\mathfrak{p}}^0, Y_{\mathfrak{H}}$              | floors: lower bounds for the residue degrees of the free primes, conditions (F11), (F12); the floor sum                               | Definition 4.18                  |
| $K, \sigma_j, c_j, b_{TV}$                          | the signed kernel $\sum_j c_j g_{\sigma_j}$ with its 21 abscissae and coefficients, and its multiplier of $w$                         | Proposition 4.19, Definition 7.1 |
| $\text{Dih}_4, \psi_o$                              | the dihedral group of order 8; the 27 forms of dihedral type on $\text{gr}_2 G_B$                                                     | Definition 5.2, Lemma 5.4        |
| $\psi_1^c, \dots, \psi_{15}^c$                      | the census basis of dihedral forms                                                                                                    | Definition 5.9                   |
| $W'', E_{W''}$                                      | the span of seven dihedral forms, $\dim W'' = 4$ , and its field, $[E_{W''} : \mathbb{Q}] = 8192$                                     | Definition 5.7                   |
| $\delta, p$                                         | the exponent is $1 + \delta$ ; $p = 2/(1 + \delta)$ is a Lebesgue exponent                                                            | Definition 8.28                  |
| $\mathcal{S}_i, \mathcal{F}_{\delta, \mathfrak{p}}$ | the shells of a local field; the local functional of the shell profile at $\mathfrak{p}$                                              | Definitions 9.3, 9.7             |
| $J_{\mathbb{R}}, J_{\mathbb{C}}$                    | the archimedean functionals of the profiles                                                                                           | Definition 8.28                  |
| $(e_r, f_r)$                                        | for $r = 2, 3, 5, 29$ the type of the selected places above $r$ ; for $r = 41$ the <i>effective type</i> $(2, 4)$ , a counting device | Definition 11.2                  |

**1.8. Computations and data.** The proof uses finite computations: linear algebra over  $\mathbb{F}_2$  for the tower and its quotients, exact rational arithmetic for the Golod–Shafarevich function, a census of primes in  $\mathbb{C}$ , rigorous evaluations of  $L$ -functions in the ball arithmetic of Arb, now part of FLINT [15, 39], 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.

The programs and their data are in the directory `papers/0.043171/certificates` of the repository [23]. They import, without modifying them, programs in the directories `papers/0.04273/certificates` and `papers/0.042901/certificates` of the same repository (the arithmetic of  $B$  and of  $E$ , the analytic ceiling with  $E$  as comparison field, and the geometric margin) and some routines of the data archive in `papers/0.0418235/certificates`, whose members are checked against their SHA-256 hashes when the archive is unpacked. A *witness* is a JSON file that records the exact data of one certificate (the exponent, the bound  $C$ , the kernel abscissae and coefficients, the profile parameters and the shell weights) together with the SHA-256 hashes of the data files it reads; its replay program recomputes every certified inequality from it. The witness of Theorem 1.1 is `certificates/dihedral/witness_0.043171.json`; it pins the SHA-256 hashes of 683 data files, among them all 356 files that the certification reads. The replay program `certificates/dihedral/reproduce_w3.py` regenerates the exports of the number fields with PARI/GP, recomputes the  $L$ -values at three of the abscissae and checks the others by hash, repeats the census on sample ranges and checks the census bins against an independent classification, reruns the kernel checks and the bound for the relative zeta value, and recomputes the margin. It takes about two hours on a machine with sixteen cores. The computations were run with PARI/GP 2.17.2, python-flint 0.9.0 (FLINT 3.6.0), mpmath 1.3.0, numpy 2.5.3 and scipy 1.18.1; the census programs need an x86-64 processor with the AVX-512 IFMA instructions.

## CONTENTS

|                                                            |    |
|------------------------------------------------------------|----|
| 1. Introduction                                            | 1  |
| 2. The Tower over $\mathbb{Q}(\sqrt{241})$                 | 9  |
| 3. The Kummer Field and Its Quadratic $L$ -Functions       | 27 |
| 4. The Relative Zeta Value                                 | 31 |
| 5. Dihedral Quotients of the Tower and the Field $E_{W''}$ | 44 |
| 6. Values of the $L$ -Functions of $E_{W''}$               | 53 |

|                                                        |     |
|--------------------------------------------------------|-----|
| 7. Proof of the Bound for the Relative Zeta Value      | 58  |
| 8. Units of Relative Norm One and Planar Point Sets    | 60  |
| 9. Shell Profiles at Split Finite Places               | 69  |
| 10. Archimedean Profiles                               | 77  |
| 11. Proof of Theorem 1.1                               | 84  |
| 12. Other Refinements, Intermediate Results and Limits | 89  |
| Appendix A. The Shell Weights                          | 93  |
| Appendix B. Dependency Index                           | 94  |
| References                                             | 100 |

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

This section constructs the number fields of Theorem 2.46 as finite subextensions of an infinite pro-2 extension of  $B = \mathbb{Q}(\sqrt{241})$  with prescribed local Galois groups: ramification is allowed only above 2, 3 and 5, and the order of the Frobenius is bounded by four at the two primes  $\mathfrak{t}_1, \mathfrak{t}_2$  above 29 and at one of the two primes  $\mathfrak{t}_3, \mathfrak{t}_4$  above 41, namely  $\mathfrak{t}_3$  (Lemma 2.5). 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 2.20). Subsection 2.4 imposes the local conditions and defines the quotient  $G_B$  of  $G_S$  (Definition 2.23). 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  $\iota_1$  (Definition 2.13) has  $2^{15}$  conjugates in  $G_B/D_4 G_B$  (Lemma 2.30). Subsections 2.6 and 2.7 prove that  $G_B$  is infinite, by a filtered Fox calculus and the Golod–Shafarevich method [9]: the Golod–Shafarevich function  $P_B$  of (2.41) takes a negative value (Lemma 2.42). Subsection 2.8 proves Theorem 2.46. Later sections use Theorem 2.46 (the fields, their root discriminant, signature and local types), the elementary images of Table 5 (Section 3 and the census of Section 4), and the description  $\text{gr}_2 G_B = \mathfrak{L}_2/R_2$  of Lemmas 2.27 and 2.29 (Sections 4 and 5).

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  $\Delta$  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, 30, 7]. By Lazard’s formula [7, Proposition 3.2],  $D_n = \prod_{i \geq n} \gamma_i^{2^i}$ , where  $\gamma_i$  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  $\mathfrak{F}$  of rank  $n$  (free pro-2 groups are written in fraktur:  $\mathfrak{F}, \mathfrak{F}_k, \mathfrak{F}'$ ),  $\text{gr } \mathfrak{F}$  is the free restricted Lie algebra on  $\mathfrak{F}/D_2 \mathfrak{F} \cong \mathbb{F}_2^n$  [30, 7]. 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  $M = \text{Fil}^0 M \supseteq \text{Fil}^1 M \supseteq \dots$  such that  $\text{Fil}^m M = 0$  for large  $m$ . Its *Hilbert polynomial* is  $h_M(t) = \sum_{m \geq 0} \dim(\text{Fil}^m M / \text{Fil}^{m+1} M) t^m$ . For a finite 2-group  $\Delta$  we filter  $\mathbb{F}_2[\Delta]$  by the powers  $\mathfrak{I}^m$  of its augmentation ideal  $\mathfrak{I}$ , so that  $h_{\mathbb{F}_2[\Delta]}(t) = \sum_{m \geq 0} \dim(\mathfrak{I}^m / \mathfrak{I}^{m+1}) t^m$ .

**Theorem 2.2** (Jennings [13]; see also [30]). *Let  $\Delta$  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  $(g_1 - 1)^{a_1} \cdots (g_m - 1)^{a_m}$  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  $\mathfrak{I}^n$ . The same holds with the factors taken in any other fixed order (Remark 2.3). Consequently*

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

*Remark 2.3.* The form of Theorem 2.2 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  $\text{gr } \Delta$  [30] and the restricted Poincaré–Birkhoff–Witt theorem. We use this freedom in Lemma 2.38(a), where the elements of a subgroup are placed last.

**2.1. The Base Field.** This subsection fixes the  $\{2, 3, 5\}$ -units  $\alpha_0, \dots, \alpha_7$  of  $B$ , the primes above 2, 3, 5, 29, 41 and their square classes (Lemma 2.5, Table 4); every later Kummer-theoretic computation reads off these data.

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

$$(2.4) \quad \begin{aligned} \alpha_0 &= -1, & \alpha_1 &= \varepsilon = -71011068 + 4574225\sqrt{241}, \\ \alpha_2 &= \frac{-6101-393\sqrt{241}}{2}, & \alpha_3 &= \frac{6101-393\sqrt{241}}{2}, \\ \alpha_4 &= 31 - 2\sqrt{241}, & \alpha_5 &= 31 + 2\sqrt{241}, & \alpha_6 &= 326 - 21\sqrt{241}, & \alpha_7 &= 326 + 21\sqrt{241}. \end{aligned}$$

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 2.5.** (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  $\varepsilon$  has norm  $N_{B/\mathbb{Q}}(\varepsilon) = -1$ , and the classes of  $-1$  and  $\varepsilon$  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. Likewise  $41 = \mathfrak{t}_3\mathfrak{t}_4$  with  $\mathfrak{t}_3 = (621 + 40\sqrt{241})\mathcal{O}_B$  and  $\mathfrak{t}_4 = (621 - 40\sqrt{241})\mathcal{O}_B$ , two distinct primes 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 ten primes of degree one above  $p \in \{2, 3, 5, 29, 41\}$  listed here, 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 4.

(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 element  $\alpha_i$  is a square modulo  $\mathfrak{t}_3$  exactly for  $i = 0, 1, 5, 6, 7$ , and modulo  $\mathfrak{t}_4$  exactly for  $i = 0, 1, 4, 6, 7$ . The residue field of  $\mathfrak{t}_0$  is  $\mathbb{F}_{49}$ , and  $\alpha_i$  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  $\eta$ , and  $\varepsilon = \pm \eta^k$ . Since  $N_{B/\mathbb{Q}}(\varepsilon) = -1$ , the exponent  $k$  is odd, so  $-1$  and  $\varepsilon$  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  $241 \equiv 1 \pmod{8}$ ,  $241 \equiv 1 \pmod{3}$ ,  $241 \equiv 1 \pmod{5}$ ,  $241 \equiv 9 \pmod{29}$ ,  $241 \equiv 36 \pmod{41}$  and  $241 \equiv 3 \pmod{7}$ , and 3 is not a square modulo 7. Hence 2, 3, 5, 29, 41 split, 7 is inert and 241 ramifies. The listed generators have norms  $\pm 2, \pm 3, \pm 5, 29, 41$  (for instance  $621^2 - 241 \cdot 40^2 = 41$ ), 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 and 41 the product of the two generators is  $p$ . 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 4.

(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) At  $\mathfrak{t}_3$  and  $\mathfrak{t}_4$  the residue field is  $\mathbb{F}_{41}$  and  $\sqrt{241} \mapsto 6$ , respectively 35, since  $621 + 40 \cdot 6 = 21 \cdot 41$  and  $621 - 40 \cdot 35 = -19 \cdot 41$ ; the statement is a computation of Legendre symbols modulo 41, repeated by the supplementary programs `kummer41.gp` and `check41.py`. 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 (2.4), this holds for  $\alpha_i$  exactly when  $i = 0, 4, 5, 6, 7$ .  $\square$

TABLE 4. 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  $u = -1, 2, 2, 3$  is a nonsquare unit for  $p = 3, 5, 29, 41$ .

| place            | $\sqrt{241} \mapsto$ | $\alpha_0$ | $\alpha_1$ | $\alpha_2$ | $\alpha_3$ | $\alpha_4$ | $\alpha_5$ | $\alpha_6$ | $\alpha_7$ |
|------------------|----------------------|------------|------------|------------|------------|------------|------------|------------|------------|
| $\mathfrak{p}_1$ | 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          |
| $\mathfrak{t}_3$ | 6 mod 41             | 1          | 1          | 3          | 3          | 3          | 1          | 1          | 1          |
| $\mathfrak{t}_4$ | 35 mod 41            | 1          | 1          | 3          | 3          | 1          | 3          | 1          | 1          |
| $v_1$            | $+\sqrt{241}$        | -          | +          | -          | -          | -          | +          | -          | +          |
| $v_2$            | $-\sqrt{241}$        | -          | -          | +          | +          | +          | -          | +          | -          |

The classes in Table 4 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 2.5(e); the prime  $\mathfrak{t}_0$  carries no condition in this paper.

**2.2. Local Galois Groups.** This subsection gives presentations of the local pro-2 Galois groups, with the quadratic initials of their relators (Lemma 2.8), and constructs the dyadic local field  $L_2$  with Galois group  $\mathcal{D}$  (Lemma 2.9). These are the local conditions of the tower and the local inputs of the Golod–Shafarevich estimate of Subsections 2.6 and 2.7.

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  $\nu$  of  $B$  let  $\mathcal{G}_\nu$  be the Galois group of the maximal pro-2 extension of the completion  $B_\nu$ ; 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 [18, Chapter III, Section 4]. For odd  $p$  and  $p$ -adic units  $u, w$ , and for 2-adic units  $u, w$ ,

$$(2.6) \quad (p^a u, p^b w)_p = (-1)^{ab(p-1)/2} \left(\frac{u}{p}\right)^b \left(\frac{w}{p}\right)^a, \quad (2^a u, 2^b w)_2 = (-1)^{\frac{u-1}{2} \frac{w-1}{2} + a \frac{w^2-1}{8} + b \frac{u^2-1}{8}}$$

[33, Chapter III, Theorem 1], [18, Chapter VIII, Section 5].

**Definition 2.7.** Let  $g_1, \dots, g_k$  generate a pro-2 group  $G$ , and let  $\mathfrak{F}_k$  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  $\mathfrak{F}_k$  whose normal closure is the kernel of  $\mathfrak{F}_k \rightarrow G$ . If a defining relator  $r$  lies in  $D_2 \mathfrak{F}_k$ , its *quadratic initial* is its class in  $\text{gr}_2 \mathfrak{F}_k$ .

**Lemma 2.8.** (a) If  $\nu$  is real, then  $\mathcal{G}_\nu = \langle \iota \rangle \cong C_2$  with the single defining relator  $\iota^2$ , and  $\iota(\sqrt{b}) = -\sqrt{b}$  exactly when  $b < 0$ .

(b) Let  $p$  be an odd prime and  $\varpi$  a uniformizer of  $\mathbb{Q}_p$ . Then  $\mathcal{G}_{\mathbb{Q}_p}$  is generated by a generator  $\tau$  of its inertia group and a Frobenius lift  $\varphi$  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 [25, Theorem 7.5.3], the Galois group of the maximal tamely ramified extension of  $\mathbb{Q}_p$  is generated by a Frobenius lift  $\varphi'$  and a generator  $\tau$  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  $\tau$  moves  $\sqrt{\varpi}$ ; replacing  $\varphi'$  by  $\varphi'\tau$  if necessary gives  $\varphi$ . 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  $\varphi$  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  $\tau^{1-p}$  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 [25, 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 (2.6). By [25, 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  $\kappa_b$  be the character with  $g(\sqrt{b}) = (-1)^{\kappa_b(g)} \sqrt{b}$ . The characters dual to  $x, y, z$  are  $\kappa_2, \kappa_{-5}, \kappa_5$ . Inflation identifies  $H^2(\mathcal{G}_{\mathbb{Q}_2}, \mathbb{F}_2)$  with  $H^2$  of the absolute Galois group of  $\mathbb{Q}_2$  [25, Proposition 7.5.8], and there the invariant of  $\kappa_a \cup \kappa_b$  is given by the Hilbert symbol  $(a, b)_2$  [18, Chapter III, Section 4]. By (2.6), 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  $\text{tr}_r$  of the transgression at  $r$  is an isomorphism  $H^2(\mathcal{G}_{\mathbb{Q}_2}, \mathbb{F}_2) \rightarrow \mathbb{F}_2$  [25, Proposition 3.9.12(iii)], and so is the invariant, so the two coincide. We now apply the relation–cup identity [25, Proposition 3.9.13(ii)], see also [29, 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  $\text{tr}_r$  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  $\mathbb{Z}_2^\times \times \mathbb{Z}/2$ . 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  $\text{gr}_2$  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  $\kappa \cup \kappa$ , 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 [25, 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  $\text{Fr}$ ; let  $i = \sqrt{-1}$ ,  $k_2 = \mathbb{Q}_2(i)$ , and let  $\pi_5 = 1 + 2i$ , a prime element of  $\mathbb{Z}[i]$  above 5. Put

$$M_8 = \mathbb{Q}_2(i, \sqrt{5}, \sqrt{\pi_5}), \quad M_{16} = M_8(\sqrt{2}), \quad L_2 = M_{16}U_4.$$

Since  $\pi_5 \bar{\pi}_5 = 5$  with  $\bar{\pi}_5 = 1 - 2i$ , the field  $M_8$  contains  $\sqrt{\pi_5} = \sqrt{5}/\sqrt{\pi_5}$ . Let  $\sigma_y$  and  $\sigma_z$  be the automorphisms of  $M_8$  given by

$$\sigma_y : i \mapsto -i, \sqrt{5} \mapsto \sqrt{5}, \sqrt{\pi_5} \mapsto \sqrt{5}/\sqrt{\pi_5}; \quad \sigma_z : i \mapsto -i, \sqrt{5} \mapsto -\sqrt{5}, \sqrt{\pi_5} \mapsto \sqrt{5}/\sqrt{\pi_5}.$$

**Lemma 2.9.** (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  $\sigma_y$  on  $M_8$ , fixes  $\sqrt{2}$  and is trivial on  $U_4$ ; and  $z$  restricts to  $\sigma_z$  on  $M_8$ , fixes  $\sqrt{2}$  and restricts to  $\text{Fr}$  on  $U_4$ . They act on  $E_2 \subset L_2$  as in Lemma 2.8(c), and the map sending the generators of*

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

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

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

(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  $\text{ord}_2$  is the valuation of  $L_2$  normalized by  $\text{ord}_2(2) = 1$ .*

*Proof.* Quadratic extensions of  $k_2$ . Let  $\text{ord}_{k_2}$  be the normalized valuation of  $k_2$ . Put  $\varpi = 1 + i$ , a uniformizer of  $k_2$ , so that  $\text{ord}_{k_2}(2) = 2$ , and for  $b \in k_2^\times$  let  $c(b)$  be the exponent of the conductor of  $k_2(\sqrt{b})/k_2$ , 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  $\pi_5 = 1 + \varpi^2$ , the element  $\varpi' = (\sqrt{\pi_5} - 1 - \varpi)/\varpi$  is a root of the Eisenstein polynomial  $X^2 + \frac{2(1+\varpi)}{\varpi}X + \frac{2}{\varpi}$ ; its derivative at  $\varpi'$  is the sum of terms of valuations 5 and 2 in  $k_2(\sqrt{\pi_5})$ , so  $c(\pi_5) = 2$ . Next  $2\pi_5 = \varpi^2 u'$  with  $u' = 2 - i$ , and  $\sqrt{u'} - 1$  is a root of  $X^2 + 2X + 1 - u'$ , which is Eisenstein since  $\text{ord}_{k_2}(1 - u') = 1$ ; its derivative  $2\sqrt{u'}$  has valuation 4, so  $c(2\pi_5) = 4$ . 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  $b \notin k_2^{\times 2} \cup 5k_2^{\times 2}$ : the field  $k_2(\sqrt{5}, \sqrt{b})$  is unramified over both  $k_2(\sqrt{b})$  and  $k_2(\sqrt{5b})$ , so the two ways of computing its discriminant over  $k_2$  give  $2c(b) = 2c(5b)$ .

(a) Since  $k_2(\sqrt{5})/k_2$  is unramified and  $k_2(\sqrt{\pi_5})/k_2$  is ramified,  $\pi_5$  is not a square in  $k_2(\sqrt{5})$ , so  $[M_8 : \mathbb{Q}_2] = 8$ . The field  $M_8$  contains the conjugate  $\sqrt{\pi_5}$  of  $\sqrt{\pi_5}$ , 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  $\pi_5$ ; in particular  $\sigma_y$  and  $\sigma_z$  exist. Now  $\sigma_y^2 = 1$ ,  $\sigma_z^2$  fixes  $i, \sqrt{5}$  and negates  $\sqrt{\pi_5}$ ,  $\sigma_z$  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  $(\sigma, s, \mu)$ , where  $\sigma \in \text{Gal}(M_8/\mathbb{Q}_2)$ ,  $s = \pm 1$  is the sign by which the element multiplies  $\sqrt{2}$ , and  $\mu \in \text{Gal}(U_4/\mathbb{Q}_2)$  agrees with  $\sigma$  on  $\sqrt{5}$ ; both sets have 32 elements. Since  $\text{Fr}$  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  $\mathcal{D}$  hold. Conversely, in  $\mathcal{D}$  these relations make  $w = [y, z]$  central:  $w^y = w^{-1} = w$ , and  $[w, z] = 1$  is imposed. Since  $zy = yzw$ , every element of  $\mathcal{D}$  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

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

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  $\mathcal{D} \cong \text{Gal}(L_2/\mathbb{Q}_2)$ . The inertia group consists of the elements trivial on  $U_4$ , namely  $\langle x, y, w \rangle$ .

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

(d) The extension  $M_{16}/k_2$  is abelian with group  $C_2^3$ , generated by  $\sqrt{5}, \sqrt{\pi_5}, \sqrt{2}$ . We apply the conductor–discriminant formula for abelian extensions [18, 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  $M_{16}/k_2$ . Taking  $(1+i)$ -adic valuations gives

$$\text{ord}_{k_2}(\mathfrak{d}_{M_{16}/k_2}) = \sum_b c(b) = 0 + 0 + 2 + 2 + 4 + 4 + 4 + 4 = 20,$$

the sum over the classes  $b = 1, 5, \pi_5, 5\pi_5, 2, 10, 2\pi_5, 10\pi_5$ . Hence

$$\text{ord}_2(\mathfrak{d}_{M_{16}/\mathbb{Q}_2}) = [M_{16} : k_2] \text{ord}_2(\mathfrak{d}_{k_2/\mathbb{Q}_2}) + 20 = 8 \cdot 2 + 20 = 36.$$

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 2.10.* 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  $\mathcal{D}$  and generates, so it also defines an isomorphism  $\mathcal{D} \cong \text{Gal}(L_2/\mathbb{Q}_2)$ . The description of the inertia group, however, refers to the triple of Lemma 2.9(b).

**2.3. The Global Group and Its Complete Presentation.** This subsection introduces the Galois group  $G_S$  of the maximal pro-2 extension of  $B$  unramified outside  $2, 3, 5$ , its local generators and their elementary images (Lemma 2.14), and shows that  $G_S$  has 8 generators and 7 relations, given by local relators (Lemma 2.20). The presentation is the starting point of Subsections 2.4–2.7.

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 2.11.** *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 2.5(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 2.12.** 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*  $\kappa_a$  is defined by  $g(\sqrt{a}) = (-1)^{\kappa_a(g)} \sqrt{a}$ ; its values lie in  $\mathbb{F}_2$ . (The  $\pm 1$ -valued characters  $\chi_e$  of Section 3 are  $\chi_e = (-1)^{\kappa_a}$  with  $a = \prod_i \alpha_i^{e_i}$ .)

By Lemmas 2.5(d) and 2.11,  $g \mapsto \bar{g}$  identifies  $G_S/D_2G_S = \text{Gal}(E/B)$  with  $\mathbb{F}_2^8$ , and  $a \mapsto \kappa_a$  identifies  $V$  with the dual of  $\mathbb{F}_2^8$ , with  $\kappa_{\alpha_i}(g) = \bar{g}_i$ . We write vectors in  $\mathbb{F}_2^8$  as strings  $c_0c_1 \cdots c_7$  of their coordinates.

For a place  $\nu$  of  $B$ , a choice of a place of  $B_S$  above  $\nu$  gives a homomorphism  $\mathcal{G}_\nu \rightarrow G_S$ , the *local map* at  $\nu$ ; 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  $\text{Frob}_\nu$ . Let  $\Sigma = S \cup \{v_1, v_2\}$ .

**Definition 2.13.** 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  $G_S$ :  $\iota_j$  at  $v_j$  (Lemma 2.8(a)), so that  $\iota_1, \iota_2$  are complex conjugations;  $\tau_\nu, \varphi_\nu$  at  $\nu \in \{q_1, q_2, t_1, t_2\}$ , with the generator  $\alpha_i$  of  $\nu$  as uniformizer  $\varpi$  in Lemma 2.8(b); and  $x_j, y_j, z_j$  at  $p_j$ , the images of one fixed triple  $x, y, z \in \mathcal{G}_{\mathbb{Q}_2} = \mathcal{G}_{p_j}$  lifting the elements  $x, y, z$  of Lemma 2.9(b). We also write  $\text{Frob}_{t_k}$  for  $k = 1, 2, 3$ . These elements are the *local generators*: those at  $\nu \in \Sigma$  are the generators just fixed, and the local generator at  $t_k$ ,  $k = 1, 2, 3$ , is  $\text{Frob}_{t_k}$ . We call  $t_1, t_2, t_3$  the *capped primes*.

The triple  $x, y, z$  satisfies the hypothesis of Lemma 2.8(c). For a finite place  $\nu \notin \Sigma$ , in particular for  $\nu = t_4$ , the elementary image of  $\text{Frob}_\nu$  does not depend on the place of  $B_S$  chosen above  $\nu$ , because  $\text{Gal}(E/B)$  is abelian; it is the elementary image of the Frobenius of  $\nu$  in  $E/B$ .

**Lemma 2.14.** *The elementary images of the local generators are those of Table 5. More precisely, for each local generator  $g$  at a place  $\nu$ , the column “action” gives an element  $c \in B_\nu^\times$  ( $c = -1$  at a real place, where  $(-1, a)_\nu$  is the sign of  $a$ ) such that  $g(\sqrt{a}) = (c, a)_\nu \sqrt{a}$  for every  $a \in V$ ; hence  $\bar{g} = (\frac{1}{2}(1 - (c, \alpha_i)_\nu))_{0 \leq i \leq 7}$ . The elementary image of the Frobenius  $\text{Frob}_{t_4}$  of the uncapped prime  $t_4$  above 41 is 00110100.*

*Proof.* The actions in the column “action” follow from Lemma 2.8 and (2.6). At a real place,  $\iota_j$  negates  $\sqrt{a}$  exactly when  $a < 0$  there, that is, when  $(-1, a)_{v_j} = -1$ . At a place  $\nu$  above  $p \in \{3, 5\}$ , by Lemma 2.8(b),  $\tau_\nu$  negates  $\sqrt{a}$  exactly when  $\text{ord}_\nu(a)$  is odd, that is, when  $(u, a)_\nu = -1$  for the nonsquare unit  $u$  of Table 4; and  $\varphi_\nu$  fixes the square root of the generator  $\alpha_i$  of  $\nu$  and negates the square root of a unit exactly when it is not a square modulo  $\nu$ , which is the action of  $(-\alpha_i, \cdot)_\nu$ . At  $p_j$  the actions are those of Lemma 2.8(c). At a capped prime  $\nu$  above  $p$ , every  $a \in V$  is a unit, and the Frobenius negates  $\sqrt{a}$  exactly when  $a$  is not a square modulo  $\nu$ , that is, when  $(p, a)_\nu = -1$ . These Hilbert symbols are the local Artin symbols [18, Chapter III, Remark 4.5]. The vector  $\bar{g}$  is then read off from the square classes of the  $\alpha_i$  in Table 4 and (2.6), and at the primes  $t_3, t_4$  above 41 also from Lemma 2.5(e). For example, at the places above 3 and 5 the vector of  $\tau_\nu$  marks the odd valuations, and that of  $\varphi_\nu$  marks the units that are not squares modulo  $\nu$ , with a zero at the

TABLE 5. 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                            |
|--------------------------------|----------|----------------------------|--------------------------------|----------|-----------------------------------|
| $\iota_1$                      | 10111010 | sign at $v_1$              | $\iota_2$                      | 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 | $(29, b)_{\mathfrak{t}_2}$        |
| $\text{Frob}_{\mathfrak{t}_3}$ | 00111000 | $(41, b)_{\mathfrak{t}_3}$ |                                |          |                                   |

generator of  $\nu$ . By Lemma 2.5(e), the  $\alpha_i$  that are not squares modulo  $\mathfrak{t}_4$  are those with  $i = 2, 3, 5$ , which gives 00110100 for  $\text{Frob}_{\mathfrak{t}_4}$ . The supplementary program `kummer241.gp` checks the norms of the  $\alpha_i$ , the generators of the primes in Lemma 2.5(c) and the residues of  $\sqrt{241}$  in Table 4, and recomputes Table 5 from these Hilbert symbols, except the row of  $\mathfrak{t}_3$ , which `kummer41.gp` computes in the same way; it also computes the elementary image of  $\text{Frob}_{\mathfrak{t}_4}$ .  $\square$

Fix a minimal presentation  $1 \rightarrow R \rightarrow \mathfrak{F} \rightarrow G_S \rightarrow 1$ , where  $\mathfrak{F}$  is a free pro-2 group of rank 8. Minimality means  $R \subset D_2\mathfrak{F}$ , so  $\mathfrak{F}/D_2\mathfrak{F} = \mathbb{F}_2^8$  with the coordinates above. Put  $\mathfrak{L} = \text{gr } \mathfrak{F}$ , so that  $\dim \mathfrak{L}_1 = 8$ ,  $\dim \mathfrak{L}_2 = 36$  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  $\mathfrak{F}$  with image  $v$  has class  $v^{[2]}$ . For each local generator  $g$  above choose a lift  $\hat{g} \in \mathfrak{F}$ , and define the local relators

$$(2.15) \quad \rho_{v_j} = \hat{\iota}_j^2, \quad \rho_\nu = \hat{\varphi}_\nu \hat{\tau}_\nu \hat{\varphi}_\nu^{-1} \hat{\tau}_\nu^{-p} \quad (\nu \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2\}), \quad \rho_{\mathfrak{p}_j} = r(\hat{x}_j, \hat{y}_j, \hat{z}_j),$$

where  $p \in \{3, 5\}$  is the rational prime below  $\nu$ , 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 2.8:

$$(2.16) \quad \bar{\iota}_j^{[2]}, \quad [\bar{\tau}_\nu, \bar{\varphi}_\nu] + \frac{p-1}{2} \bar{\tau}_\nu^{[2]}, \quad \bar{y}_j^{[2]} + [\bar{x}_j, \bar{y}_j] + [\bar{x}_j, \bar{z}_j].$$

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

The classes (2.16) have an arithmetic meaning, which we now describe (Lemmas 2.17 and 2.19). 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  $\mathfrak{L}_1 = \mathbb{F}_2^8$ . Through the identification of  $\mathfrak{L}_1$  with  $\text{Gal}(E/B)$ , the Kummer characters  $\kappa_a$ ,  $a \in V$ , are linear forms on  $\mathfrak{L}_1$ , with  $\kappa_{\alpha_i}(X_j) = 1$  exactly when  $i = j$ .

**Lemma 2.17.** *There is a unique linear isomorphism  $\beta$  from  $\mathfrak{L}_2$  onto the space of symmetric bilinear forms on  $V$  such that*

$$\beta(v^{[2]})(a, b) = \kappa_a(v)\kappa_b(v), \quad \beta([v, w])(a, b) = \kappa_a(v)\kappa_b(w) + \kappa_a(w)\kappa_b(v)$$

for all  $v, w \in \mathfrak{L}_1$  and  $a, b \in V$ . If  $\xi \in \mathfrak{L}_2$  is written in the free algebra as  $\sum_{i,j} n_{ij} X_i X_j$ , then  $\beta(\xi)(\alpha_i, \alpha_j) = n_{ij}$ .

*Proof.* 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  $\mathfrak{L}_2$ . Define  $\beta$  on this basis by the displayed formulas for basis vectors  $v, w$ ; it sends  $X_i^{[2]}$  to the form that is 1 at

$(\alpha_i, \alpha_i)$  and 0 at the other pairs of basis vectors, and  $[X_i, X_j]$  to the form that is 1 at  $(\alpha_i, \alpha_j)$  and  $(\alpha_j, \alpha_i)$  and 0 elsewhere. These 36 forms are a basis of the symmetric bilinear forms on  $V$ , so  $\beta$  is an isomorphism, and it is the only linear map satisfying the formulas on basis vectors. 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  $\mathbb{F}_2$ . The last statement holds for the basis elements  $X_i^2$  and  $X_i X_j + X_j X_i$  by the description of their images, and both sides are linear in  $\xi$ .  $\square$

**Definition 2.18.** For  $\nu \in \Sigma$ , the *local Hilbert form*  $H_\nu$  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 2.19.** For every  $\nu \in \Sigma$ ,  $\beta$  maps the class of  $\rho_\nu$  to  $H_\nu$ . The eight classes (2.16), 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  $\nu$ ,  $\kappa_a(\bar{g})$  is the value at  $g$  of the local Kummer character of the image of  $a$  in  $B_\nu$ . Hence  $\beta$  (Lemma 2.17) of the class of  $\rho_\nu$  is the pullback to  $V$  of a symmetric bilinear form on  $B_\nu^\times/B_\nu^{\times 2}$ , as is  $H_\nu$ , 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  $\nu$  above  $p \in \{3, 5\}$ , take the basis  $\varpi, u$  with  $\varpi$  the generator of  $\nu$  and  $u$  a nonsquare unit. By Lemma 2.8(b),  $\kappa_\varpi(\tau) = \kappa_u(\varphi) = 1$  and  $\kappa_\varpi(\varphi) = \kappa_u(\tau) = 0$ , 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 (2.6) 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  $\kappa_2, \kappa_{-5}, \kappa_5$  are dual to  $x, y, z$ , as in the proof of Lemma 2.8(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  $\nu'$  is finite and not above 2, and  $a, b$  are units at  $\nu'$ , so  $(a, b)_{\nu'} = 1$  [18, Chapter VIII, 5.8]. By the product formula for the Hilbert symbol [18, Chapter V, Example 5.4],  $\sum_{\nu \in \Sigma} H_\nu = 0$ , so the eight classes sum to zero.

Finally, by Table 4 and (2.6), 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 2.20.** The group  $G_S$  has generator rank 8 and relation rank 7. The seven relators  $\rho_\nu$  with  $\nu \in \Sigma \setminus \{\mathfrak{p}_1\}$  form a minimal system of defining relations: their normal closure in  $\mathfrak{F}$  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 2.11 and [25, 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  $\mu_2$  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 [16, 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 [28, 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 2.19, the classes in  $\mathfrak{L}_2$  of the seven relators  $\rho_\nu$ ,  $\nu \neq \mathfrak{p}_1$ , are linearly independent. Since  $R \subset D_2\mathfrak{F}$ , we have  $R^2[R, \mathfrak{F}] \subset D_3\mathfrak{F}$ , so the classes of these seven relators in  $R/R^2[R, \mathfrak{F}]$  are independent. On the other hand  $\dim R/R^2[R, \mathfrak{F}] = \dim H^2(G_S, \mathbb{F}_2) \leq 7$  by the five-term exact sequence of the presentation [25, Proposition 3.9.5], [29, (3.3)–(3.4)]. Hence the seven classes form a basis, the relation rank is 7, and by the pro-2 Nakayama lemma [25, Corollary 3.9.3] the seven relators generate  $R$  as a normal subgroup. Finally  $\rho_{\mathfrak{p}_1} \in R$ .  $\square$

**Corollary 2.21.** *Any seven of the eight local relators  $\rho_\nu$ ,  $\nu \in \Sigma$ , generate  $R$  as a normal subgroup.*

*Proof.* By Lemma 2.19, the only linear relation among the eight classes (2.16) 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 2.20 applies to any seven of the eight local relators.  $\square$

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

*Remark 2.22.* By Lemma 2.20, 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  $\kappa_a \cup \kappa_b$  maps to the class of the quaternion algebra  $(a, b)$ , whose invariant at  $\nu$  is given by  $(a, b)_\nu$  [18, Chapter III, Remark 4.7], and the seven pairs in the proof of Lemma 2.19 give seven classes with independent invariant vectors. The supplementary program `cup241.gp` computes the invariant vectors at the eight places of  $\Sigma$  of all 36 algebras  $(\alpha_i, \alpha_j)$ .

**2.4. The Prescribed Local Groups.** This subsection defines the quotient  $G_B$  of  $G_S$  with prescribed local groups and the tower  $B_G/B$  (Definition 2.23), and gives a presentation of  $G_B$  by eight generators and thirty relators (Lemma 2.25), from which Subsections 2.5–2.7 compute.

We now cut  $G_S$  down to prescribed local groups. At the dyadic places we use the restriction  $\mathcal{G}_{\mathfrak{p}_j} = \mathcal{G}_{\mathbb{Q}_2} \rightarrow \text{Gal}(L_2/\mathbb{Q}_2) = \mathcal{D}$  of Lemma 2.9. At a place  $\nu$  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 the capped primes  $\mathfrak{t}_1, \mathfrak{t}_2$  and  $\mathfrak{t}_3$ , whose completions are  $\mathbb{Q}_{29}$ ,  $\mathbb{Q}_{29}$  and  $\mathbb{Q}_{41}$ , we bound the order of the Frobenius by four. (A variant of the construction caps the inert prime  $\mathfrak{t}_0$  instead of  $\mathfrak{t}_3$ ; see Remark 2.47.)

**Definition 2.23.** Let  $N$  be the normal closure in  $G_S$  of the images of  $\ker(\mathcal{G}_{\mathfrak{p}_j} \rightarrow \mathcal{D})$  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  $k = 1, 2, 3$ . 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  $\nu$ : 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 2.24.** (a) *The image of  $\mathcal{G}_{\mathfrak{p}_j}$  in  $G_B$  is a quotient of  $\mathcal{D}$ , the image of  $\mathcal{G}_\nu$  for  $\nu$  above 3 or 5 is a quotient of  $C_2 \times C_2$  in which inertia maps to the image of  $\tau_\nu$ , and  $\text{Frob}_{\mathfrak{t}_k}^4$  has order dividing four in  $G_B$  for  $k = 1, 2, 3$ .*

(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 2.23, the maps  $\mathcal{G}_{\mathfrak{p}_j} \rightarrow G_B$  and  $\mathcal{G}_\nu \rightarrow G_B$  kill  $\ker(\mathcal{G}_{\mathfrak{p}_j} \rightarrow \mathcal{D})$  and  $D_2\mathcal{G}_\nu$ , and  $\text{Frob}_{\mathfrak{t}_k}^4 \in N$ . For  $\nu$  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  $\tau_\nu$  (Lemma 2.8(b)).

(b) Since  $\mathcal{D}$  and  $\mathcal{G}_{\mathbb{Q}_2}$  both have generator rank three,  $\ker(\mathcal{G}_{\mathfrak{p}_j} \rightarrow \mathcal{D})$  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 2.11.  $\square$

By Lemma 2.30(b) below, the quotients in Lemma 2.24(a) are  $\mathcal{D}$  and  $C_2 \times C_2$ , and  $\text{Frob}_{t_k}$  has order exactly four in  $G_B$ .

**Lemma 2.25.** *The kernel  $N_B$  of  $\mathfrak{F} \rightarrow G_S \rightarrow G_B$  is the normal closure of the following thirty elements:*

- (i) *the seven relators  $\rho_\nu$ ,  $\nu \in \Sigma \setminus \{\mathfrak{p}_1\}$ ;*
- (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  $k = 1, 2, 3$ :  $\widehat{\text{Frob}_{t_k}}^4$ , where  $\widehat{\text{Frob}_{t_k}}$  is the chosen lift of  $\text{Frob}_{t_k}$ .*

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

*Proof.* By Lemma 2.20, it suffices to show that the images in  $G_S$  of the elements (ii)–(iv) generate  $N$  as a normal subgroup. Let  $\mathfrak{F}_3$  be free on  $x, y, z$ , and let  $N_{\mathcal{D}}$  be the normal closure of the seven relators of  $\mathcal{D}$  in Lemma 2.9, so that  $\mathfrak{F}_3/N_{\mathcal{D}} = \mathcal{D}$ . The relator  $r$  maps to 1 in  $\mathcal{D}$ , so  $r \in N_{\mathcal{D}}$ , and  $\ker(\mathcal{G}_{\mathbb{Q}_2} \rightarrow \mathcal{D})$  is the image of  $N_{\mathcal{D}}$ . Since  $N_{\mathcal{D}} \subset D_2\mathfrak{F}_3$ , we have  $N_{\mathcal{D}}^2[N_{\mathcal{D}}, \mathfrak{F}_3] \subset D_3\mathfrak{F}_3$ . The seven relators of  $\mathcal{D}$  span  $N_{\mathcal{D}}/N_{\mathcal{D}}^2[N_{\mathcal{D}}, \mathfrak{F}_3]$  [25, Corollary 3.9.3]; write the class of  $r$  as a combination of them. The classes in  $\text{gr}_2 \mathfrak{F}_3$  of  $x^2, y^2, [x, y], [x, z]$  are independent, the relators  $z^4, [y, z]^2$  and  $[[y, z], z]$  lie in  $D_3\mathfrak{F}_3$ , 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 [25, Corollary 3.9.3] the elements  $r, x^2, [x, y], [x, z], [[y, z], z], z^4, [y, z]^2$  generate  $N_{\mathcal{D}}$  as a normal subgroup. Since  $r = 1$  in  $\mathcal{G}_{\mathbb{Q}_2}$ , the other six generate  $\ker(\mathcal{G}_{\mathbb{Q}_2} \rightarrow \mathcal{D})$ . For  $\nu$  above  $p \in \{3, 5\}$ , the quotient of  $\mathcal{G}_\nu$  by the normal closure of  $\tau^2, \varphi^2$  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 2.24(b)) and  $R \subset D_2\mathfrak{F}$  give  $N_B \subset D_2\mathfrak{F}$ , and  $\rho_{\mathfrak{p}_1} \in R \subset N_B$ .  $\square$

**2.5. The Quotient  $G_B/D_4G_B$ .** This subsection computes  $\text{gr}_1, \text{gr}_2$  and  $\text{gr}_3$  of  $G_B$  (of dimensions 8, 15 and 26), shows that the prescribed local groups inject into  $G_B/D_3G_B$ , and counts the conjugates of  $\iota_1$  in  $G_B/D_4G_B$  (Lemmas 2.27–2.30). These results give the hypotheses of Lemma 2.38 in the proof of Proposition 2.43, the bound  $\theta \geq \theta_*$  of Theorem 2.46, and the space  $\text{gr}_2 G_B$  used in Sections 4 and 5. Throughout,  $\mathfrak{F}$ ,  $R$  and  $\mathfrak{L} = \text{gr } \mathfrak{F}$  are as in Subsection 2.3, and  $N_B$  is the kernel of  $\mathfrak{F} \rightarrow G_B$  (Lemma 2.25).

**Definition 2.26.** For  $n \geq 1$ , the *relation space*  $R_n \subseteq \mathfrak{L}_n$  of  $G_B$  in degree  $n$  is the image of  $N_B \cap D_n\mathfrak{F}$  in  $\mathfrak{L}_n = D_n\mathfrak{F}/D_{n+1}\mathfrak{F}$ .

**Lemma 2.27.** *For every  $n \geq 1$ ,  $D_nG_B$  is the image of  $D_n\mathfrak{F}$ , and the induced map  $\mathfrak{L}_n \rightarrow \text{gr}_n G_B$  is surjective with kernel  $R_n$ ; these maps respect brackets and restricted squares. In particular  $\text{gr}_1 G_B = \mathbb{F}_2^8$  and  $\text{gr}_n G_B \cong \mathfrak{L}_n/R_n$ .*

*Proof.* The map  $\mathfrak{F} \rightarrow G_B$  is surjective, and a surjection maps  $D_n$  onto  $D_n$ , so  $D_nG_B$  is the image of  $D_n\mathfrak{F}$ . The kernel of  $D_n\mathfrak{F} \rightarrow D_nG_B$  is  $N_B \cap D_n\mathfrak{F}$ , and the preimage of  $D_{n+1}G_B$  in  $D_n\mathfrak{F}$  is  $(N_B D_{n+1}\mathfrak{F}) \cap D_n\mathfrak{F} = (N_B \cap D_n\mathfrak{F}) D_{n+1}\mathfrak{F}$ . Hence  $\text{gr}_n G_B = D_nG_B/D_{n+1}G_B$  is the quotient of  $\mathfrak{L}_n$  by the image of  $N_B \cap D_n\mathfrak{F}$ , which is  $R_n$ . Brackets and restricted squares are induced by commutators and squares, which the homomorphism  $\mathfrak{F} \rightarrow G_B$  preserves. Finally  $N_B \subset D_2\mathfrak{F}$  (Lemma 2.25), so  $R_1 = 0$  and  $\text{gr}_1 G_B = \mathfrak{L}_1 = \mathbb{F}_2^8$ .  $\square$

Consider the following 22 elements of  $\mathfrak{L}_2$ , written with the vectors of Table 5:

$$(2.28) \quad \begin{aligned} & \bar{\iota}_1^{[2]}, \bar{\iota}_2^{[2]}, \quad [\bar{\tau}_\nu, \bar{\varphi}_\nu] + \bar{\tau}_\nu^{[2]} \quad (\nu = \mathfrak{q}_1, \mathfrak{q}_2), \quad [\bar{\tau}_\nu, \bar{\varphi}_\nu] \quad (\nu = \mathfrak{r}_1, \mathfrak{r}_2); \\ & \bar{y}_j^{[2]} + [\bar{x}_j, \bar{y}_j] + [\bar{x}_j, \bar{z}_j], \quad \bar{x}_j^{[2]}, \quad [\bar{x}_j, \bar{y}_j], \quad [\bar{x}_j, \bar{z}_j] \quad (j = 1, 2); \\ & \bar{\tau}_\nu^{[2]}, \bar{\varphi}_\nu^{[2]} \quad (\nu = \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2). \end{aligned}$$

They are the classes of the eight local relators (2.16) 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 2.25.

**Lemma 2.29.** *The space  $R_2$  is spanned by the 22 elements (2.28), and  $\dim R_2 = 21$ ; their only linear relation is that the eight classes of local relators sum to zero. Hence  $\dim \text{gr}_2 G_B = 15$ . 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  $D_2\mathfrak{F}$  have the same class modulo  $D_3\mathfrak{F}$ , classes of products add, and  $\mathfrak{L}_2$  is finite. Hence, by Lemma 2.25,  $R_2$  is spanned by the classes of the thirty generators of  $N_B$ . Those in (i) have the classes (2.16), 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  $D_3\mathfrak{F}$ . The class of  $\rho_{\mathfrak{p}_1}$  also lies in  $R_2$ , since  $\rho_{\mathfrak{p}_1} \in N_B$ . 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 2.19, 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. By Lemma 2.27,  $\dim \text{gr}_2 G_B = 36 - 21 = 15$ . For the last statement,  $g^2 \in D_2G_B$  has class  $v^{[2]}$  in  $\text{gr}_2 G_B = \mathfrak{L}_2/R_2$  (Lemma 2.27), so  $g^2 \in D_3G_B$  exactly when  $v^{[2]} \in R_2$ .  $\square$

**Lemma 2.30.** (a)  $\dim \text{gr}_3 G_B = 26$ , so  $|\overline{G}_B| = 2^{8+15+26} = 2^{49}$ .

- (b) For  $j = 1, 2$ , the local map induces an injection  $\mathcal{D} \rightarrow G_B/D_3G_B$ , and  $\text{gr}_n \mathcal{D} \rightarrow \text{gr}_n G_B$  is injective for  $n = 1, 2$ . For  $\nu$  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  $k = 1, 2, 3$ ,  $\text{Frob}_{\mathfrak{t}_k}$  has order exactly four in  $G_B$  and in  $G_B/D_3G_B$ . For  $j = 1, 2$ ,  $\iota_j$  has order two in  $G_B/D_2G_B$ .
- (c) The conjugacy class of  $\iota_1$  in  $\overline{G}_B$  has  $2^{15}$  elements.
- (d) We have  $\bar{\iota}_1 \neq \bar{\iota}_2$ . For each  $\nu \in \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3\}$ , neither  $\bar{\iota}_1$  nor  $\bar{\iota}_2$  lies in the span of the elementary images of the local generators at  $\nu$ .

*Proof.* (a) Work in  $\mathfrak{F}/D_4\mathfrak{F}$ , in which  $D_2\mathfrak{F}/D_4\mathfrak{F}$  is elementary abelian and  $D_3\mathfrak{F}/D_4\mathfrak{F}$  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 2.25. They lie in  $D_2\mathfrak{F}$ , and their classes in  $\mathfrak{L}_2$  are the elements of (2.28) other than the class of  $\rho_{\mathfrak{p}_1}$ , which are independent by Lemma 2.29. The generators  $\omega_j = [[\hat{y}_j, \hat{z}_j], \hat{z}_j]$  lie in  $D_3\mathfrak{F}$ , and the remaining generators of  $N_B$  lie in  $D_4\mathfrak{F}$ . For  $\rho \in D_2\mathfrak{F}$  and  $g \in \mathfrak{F}$  we have  $g^{-1}\rho g = \rho[\rho, g]$ , and modulo  $D_4\mathfrak{F}$  the commutator  $[\rho, g]$  is central and depends only, and linearly, on the classes of  $\rho$  in  $\mathfrak{L}_2$  and of  $g$  in  $\mathfrak{L}_1$ . Hence the image of  $N_B$  in  $\mathfrak{F}/D_4\mathfrak{F}$  is the subgroup generated by the  $\rho_i$ , the  $[\rho_i, f]$  for  $f$  in a basis of  $\mathfrak{F}$ , and the  $\omega_j$ . An element  $\prod_i \rho_i^{a_i}$  times an element of  $D_3\mathfrak{F}$  lies in  $D_3\mathfrak{F}$  only if all  $a_i = 0$ . Therefore  $R_3$  is spanned by the brackets  $[\bar{\rho}_i, \xi]$ , for  $\xi$  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  $\dim \text{gr}_3 G_B = 26$  by Lemma 2.27, and  $|\overline{G}_B| = 2^{8+15+26}$  by Lemmas 2.27 and 2.29.

(b) The local map  $\mathcal{G}_{\mathfrak{p}_j} \rightarrow G_B$  factors through  $\mathcal{D}$  by Definition 2.23, and the induced map  $\mathcal{D} \rightarrow G_B$  preserves the Zassenhaus filtrations. It is injective on  $\text{gr}_1$  because  $\bar{x}_j, \bar{y}_j, \bar{z}_j$  are independent, and on  $\text{gr}_2$  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  $1 \neq g \in \mathcal{D}$ , let  $n \leq 2$  be maximal with  $g \in D_n(\mathcal{D})$ ; then the image of  $g$  is nonzero in  $\text{gr}_n G_B$ , so it is not in  $D_3G_B$ . For  $\nu$  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  $\overline{\text{Frob}}_{\mathfrak{t}_k}^{[2]} \notin R_2$  for  $k = 1, 2$ , and `check41.py` checks it for  $k = 3$  (and for the elementary image of  $\text{Frob}_{\mathfrak{t}_4}$  in Lemma 2.14), using the space  $R_2$  of `lie241.py`; so Lemma 2.29 gives order at least four in  $G_B/D_3G_B$ , while Definition 2.23 gives order at most four in  $G_B$ . Finally  $\bar{\iota}_j \neq 0$ .

(c) Write  $\overline{G} = \overline{G}_B$  and  $\iota = \iota_1$ . The map  $\mathfrak{L}_1 \rightarrow \text{gr}_2 \overline{G}$ ,  $v \mapsto [\bar{\iota}, v]$ , has rank 7 by `lie241.py`, so its kernel is the line through  $\bar{\iota}$ . The map  $\text{gr}_2 \overline{G} \rightarrow \text{gr}_3 \overline{G}$ ,  $u \mapsto [u, \bar{\iota}]$ , has rank 8 by `lie241c.py`. Since  $D_2\overline{G}$  is abelian and  $D_3\overline{G}$  is central in  $\overline{G}$ , the map  $h \mapsto [h, \bar{\iota}]$  is a homomorphism  $D_2\overline{G} \rightarrow D_3\overline{G}$ ; it factors through  $\text{gr}_2 \overline{G}$  and equals the second map. Its kernel is  $C_{\overline{G}}(\bar{\iota}) \cap D_2\overline{G}$ , where  $C_{\overline{G}}(\bar{\iota}) = \{g \in$

$\bar{G} : g\iota = \iota g$  is the centralizer of  $\iota$ . The kernel therefore has order  $2^{15+26-8} = 2^{33}$ . If  $g \in C_{\bar{G}}(\iota)$ , then  $[\bar{\iota}, \bar{g}] = 0$  in  $\text{gr}_2 \bar{G}$ , so  $\bar{g} \in \{0, \bar{\iota}\}$ ; conversely  $\iota \in C_{\bar{G}}(\iota)$ . Hence  $|C_{\bar{G}}(\iota)| = 2^{34}$ , and the class of  $\iota$  has  $2^{49-34} = 2^{15}$  elements.

(d) This is a finite check on Table 5, carried out by `lie241.py`; at  $t_3$  the span is  $\{0, 00111000\}$ , which contains neither 10111010 nor 11000101 (`check41.py`).  $\square$

**2.6. Filtered Fox Calculus.** This subsection and the next prove that  $G_B$  is infinite (Proposition 2.43) by the Golod–Shafarevich method. Suppose that  $G_B$  is finite, and let  $\Lambda = \mathbb{F}_2[G_B]$ . The rows (Definition 2.34) of the relators of  $G_B$  in a presentation with eight generators (Lemma 2.25) span a  $\Lambda$ -module  $\mathcal{M}$  whose Hilbert polynomial is  $1 - (1 - 8t)h_\Lambda$  (Lemma 2.36). The module  $\mathcal{M}$  is also the sum of the modules spanned by the rows of the relations of the eleven local groups  $\Gamma$ , each isomorphic to  $C_2$ ,  $C_2 \times C_2$ ,  $C_4$  or  $\mathcal{D}$ ; for  $0 < t < 1$  the Hilbert polynomial of each of these modules is at most  $\psi_\Gamma(t)h_\Lambda(t)$ , with  $\psi_\Gamma$  as in Definition 2.37 (Lemma 2.38). The row of the dyadic relator  $\rho_{\mathfrak{p}_1}$  of (2.15) 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  $s_{\mathcal{D}}h_\Lambda$ , with  $s_{\mathcal{D}}$  as in Lemma 2.39. Comparing these bounds gives  $1 \leq h_\Lambda(t)P_B(t)$  for  $0 < t < 1$ , with  $P_B$  as in (2.41); this fails at  $t = 34/117$  (Lemma 2.42).

Let  $\Delta$  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  $\text{Fil}^m \Lambda = \mathfrak{I}^m$ . In this subsection  $n$  denotes the rank of a free pro-2 group (Definition 2.34), and filtration indices are written  $m$ . For an integer  $c \geq 1$ ,  $\Lambda^c(-1)$  denotes  $\Lambda^c$  with  $\text{Fil}^0 = \Lambda^c$  and  $\text{Fil}^m = (\mathfrak{I}^{m-1})^c$  for  $m \geq 1$ , so that  $h_{\Lambda^c(-1)} = ct h_\Lambda$ . Subspaces carry the induced filtration unless stated otherwise. A linear map  $f : M \rightarrow M'$  of filtered spaces is *strict* if  $f(\text{Fil}^m M) = \text{Fil}^m M'$  for all  $m$ . For  $0 < t < 1$ ,

$$(2.31) \quad h_M(t) = (1 - t) \sum_{m \geq 1} \dim(M / \text{Fil}^m M) t^{m-1}.$$

**Lemma 2.32.** *Let  $0 < t < 1$ .*

- (h1) *If  $f : M \rightarrow M'$  is surjective with  $f(\text{Fil}^m M) \subset \text{Fil}^m M'$  for all  $m$ , 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  $f : M \rightarrow M'$  is surjective and strict, then  $h_M = h_{\ker f} + h_{M'}$ .*
- (h4) *For subspaces  $U_1, U_2$  of a filtered space,*

$$(2.33) \quad h_{U_1+U_2}(t) \leq h_{U_1}(t) + h_{U_2}(t) - h_{U_1 \cap U_2}(t).$$

*Proof.* Statements (h1)–(h3) follow from the definitions and (2.31). 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  $\text{Fil}^m U_1 + \text{Fil}^m U_2$  on  $U_1 + U_2$ ; this filtration is contained in the induced one, and (h1) applies to the identity map.  $\square$

**Definition 2.34.** Let  $\mathfrak{F}$  be a free pro-2 group with basis  $f_1, \dots, f_n$  and  $\pi : \mathfrak{F} \rightarrow \Delta$  a surjection. Since  $\Lambda^n \rtimes \Delta$ , with  $\Delta$  acting by left multiplication, is a finite 2-group, there is a unique homomorphism  $\mathfrak{F} \rightarrow \Lambda^n \rtimes \Delta$  sending  $f_i$  to  $(e_i, \pi(f_i))$ , where  $e_1, \dots, e_n$  is the standard basis of  $\Lambda^n$ . 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  $w$  [8, Section 2].

**Lemma 2.35.** (F1)  $\partial(w w') = \partial w + \pi(w) \partial w'$ .

(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  $\partial$  restricts to a continuous homomorphism on  $\ker \pi$ .*

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

*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  $\mathfrak{F}' \rightarrow \Lambda^n \rtimes \Delta$  that agree on the basis.  $\square$

**Lemma 2.36.** *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  $\rho$  lies in the normal closure of a set  $Y \subset \ker \pi$ , then  $\partial\rho$  lies in the  $\Lambda$ -span of  $\partial Y$ . In particular,  $\mathcal{M}$  is the  $\Lambda$ -span of the rows of any set of normal generators of  $\ker \pi$ .*

*Proof.* Since the  $\pi(f_i)$  generate  $\Delta$ , 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  $\mathfrak{F}^\circ \subset \mathfrak{F}$  be the dense subgroup generated by the  $f_i$ , which is a free group on them. Then  $\pi(\mathfrak{F}^\circ) = \Delta$ , and the kernel of  $\mathbb{F}_2[\mathfrak{F}^\circ] \rightarrow \Lambda$  is  $\mathbb{F}_2[\mathfrak{F}^\circ] (\mathfrak{F}^\circ \cap \ker \pi - 1)$ . Lift  $a \in \mathcal{M}$  to  $\tilde{a} \in \mathbb{F}_2[\mathfrak{F}^\circ]^n$ . Then  $\sum_i \tilde{a}_i(f_i - 1) = \sum_l \zeta_l(q_l - 1)$  with  $q_l \in \mathfrak{F}^\circ \cap \ker \pi$  and  $\zeta_l \in \mathbb{F}_2[\mathfrak{F}^\circ]$ . By Fox's fundamental formula  $q_l - 1 = \sum_i (\partial q_l / \partial f_i)(f_i - 1)$ , where the  $\partial / \partial f_i$  are the free derivatives [8, 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  $\zeta'_j$ . So  $\tilde{a}_i = \sum_l \zeta_l \partial q_l / \partial f_i$ . On  $\mathfrak{F}^\circ$  the rows are the images of the vectors of free derivatives, so  $a = \sum_l \zeta_l \partial q_l$  lies in  $\Lambda \partial(\ker \pi)$ , which equals  $\partial(\ker \pi)$  by (F3). For the remaining statements, let  $M_Y$  be the  $\Lambda$ -span of  $\partial Y$ . By (F3), the elements  $q \in \ker \pi$  with  $\partial q \in M_Y$  form a closed normal subgroup of  $\mathfrak{F}$  containing  $Y$ .  $\square$

The next lemma bounds, in terms of the function  $\psi_\Gamma$  below, the Hilbert polynomial of the  $\Lambda$ -module spanned by the rows of all relations of one local group  $\Gamma$ . The groups  $\Gamma$  below are  $C_2$ ,  $C_2 \times C_2$ ,  $C_4$  and  $\mathcal{D}$ , with standard generators  $\iota$ ;  $\tau, \varphi$ ; 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  $h_{\mathbb{F}_2[\mathcal{D}]}$  (Theorem 2.2), and  $D_3(\Gamma) = 1$  in each case.

**Definition 2.37.** For each of these groups  $\Gamma$ , put

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

**Lemma 2.38.** *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 the maps  $\text{gr}_1 \Gamma \rightarrow \text{gr}_1 \Delta$  and  $\text{gr}_2 \Gamma \rightarrow \text{gr}_2 \Delta$  are injective. 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  $\Lambda$ -module  $\Lambda \mathcal{M}_\Gamma \subset \Lambda^k(-1)$  has  $h_{\Lambda \mathcal{M}_\Gamma} = \psi_\Gamma h_\Lambda$ .*
- (c) *Let  $\mathfrak{F}$  and  $\pi$  be as above, let  $u_1, \dots, u_k \in \mathfrak{F}$  with  $\pi(u_l) = g_l$ , and let  $\mathfrak{F}_k$  be free on  $k$  letters, mapping to  $\Gamma$  by the standard generators. Let  $U \subset \Lambda^n(-1)$  be the  $\Lambda$ -span of the rows  $\partial W(u_1, \dots, u_k)$  for all  $W$  in the kernel of  $\mathfrak{F}_k \rightarrow \Gamma$ . 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  $\Gamma$  whose classes form a homogeneous basis of  $\text{gr } \Gamma$ , and extend them by elements of  $\Delta$  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  $\Gamma$  last, form a basis of  $\Lambda$ , 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  $\Lambda_\Gamma$  and the elements of  $\Gamma$  alone. Let the  $\eta_j$  be the ordered products of the other elements, and  $w_j$  the weight of  $\eta_j$ . The empty product  $\eta_j = 1$  has weight 0, so  $\mathfrak{I}^m \cap \Lambda_\Gamma = \mathfrak{I}_\Gamma^m$ : the filtration of  $\Lambda_\Gamma$  induced from  $\Lambda$  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 2.36, 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  $\text{Fil}^m = \bigoplus_j \eta_j \text{Fil}^{m-w_j}$ , 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  $\partial u_l \in \Lambda^n = \text{Fil}^0 \Lambda^n$ . 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 2.43, 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 2.39.** *In the situation of Lemma 2.38 with  $\Gamma = \mathcal{D}$ , suppose that  $u_1, u_2, u_3$  are the basis elements  $f_1, f_2, f_3$  of  $\mathfrak{F}$ . Let  $r \in \mathfrak{F}_3$  map to 1 in  $\mathcal{D}$ , with class  $y^{[2]} + [x, y] + [x, z]$  in  $\text{gr}_2 \mathfrak{F}_3$ , and let  $\rho = r(f_1, f_2, f_3)$ . Then*

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

*Proof.* By (F4),  $\partial \rho = (\partial' r, 0, \dots, 0)$ , where  $\partial' r \in \Lambda_{\mathcal{D}}^3$  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 2.38(a),  $\Lambda^3 = \bigoplus_j \eta_j \Lambda_{\mathcal{D}}^3$  with  $\text{Fil}^m(\Lambda^3(-1)) = \bigoplus_j \eta_j \text{Fil}^{m-w_j}(\Lambda_{\mathcal{D}}^3(-1))$ , and  $b \mapsto \eta_j b$  is injective on  $\Lambda_{\mathcal{D}}^3$ . The submodule  $\Lambda \partial' r = \bigoplus_j \eta_j \Lambda_{\mathcal{D}} \partial' r$  decomposes in the same way, so  $\text{Fil}^m(\Lambda \partial' r) = \bigoplus_j \eta_j \text{Fil}^{m-w_j}(\Lambda_{\mathcal{D}} \partial' r)$  for the induced filtrations, and  $h_{\Lambda \partial \rho} = (h_\Lambda / h_{\mathbb{F}_2[\mathcal{D}]}) h_{\Lambda_{\mathcal{D}} \partial' r}$ . It therefore suffices to show that  $h_{\Lambda_{\mathcal{D}} \partial' r} = t^2(h_{\mathbb{F}_2[\mathcal{D}]} - t^7)$ , for the filtration induced from  $\Lambda_{\mathcal{D}}^3(-1)$ . Write  $\mathfrak{I}_{\mathcal{D}}$  for the augmentation ideal of  $\Lambda_{\mathcal{D}} = \mathbb{F}_2[\mathcal{D}]$ , 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  $\pi$  also denotes the map  $\mathfrak{F}_3 \rightarrow \mathcal{D}$ . For  $g, h \in \mathfrak{F}_3$ , (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  $\mathfrak{I}_{\mathcal{D}}$  to the image  $\bar{g} \in \mathbb{F}_2^3$  of  $g$  in  $\mathfrak{F}_3/D_2 \mathfrak{F}_3$ , and  $\pi(g) - 1 \equiv \sum_l \bar{g}_l X_l$  modulo  $\mathfrak{I}_{\mathcal{D}}^2$  by (F2). Hence, for  $q \in D_2 \mathfrak{F}_3$ , the row  $\partial' q$  has entries in  $\mathfrak{I}_{\mathcal{D}}$ , and modulo  $\mathfrak{I}_{\mathcal{D}}^2$  it is additive in  $q$ , because  $\pi(q) - 1 \in \mathfrak{I}_{\mathcal{D}}^2$ . It vanishes modulo  $\mathfrak{I}_{\mathcal{D}}^2$  on  $D_3 \mathfrak{F}_3 = (D_2 \mathfrak{F}_3)^2[D_2 \mathfrak{F}_3, \mathfrak{F}_3]$  (Lazard's formula): for  $q \in D_2 \mathfrak{F}_3$  the formulas above give  $\partial'(q^2), \partial'[q, h] \in \mathfrak{I}_{\mathcal{D}}^2$ , since  $\bar{q} = 0$  and  $\pi(q) - 1 \in \mathfrak{I}_{\mathcal{D}}^2$ . So the row modulo  $\mathfrak{I}_{\mathcal{D}}^2$  depends only on the class of  $q$  in  $\text{gr}_2 \mathfrak{F}_3$ , the classes  $v^{[2]}$  and  $[v, v']$  giving the rows with  $l$ -th entries  $v_l \sum_i v_i X_i$  and  $v_l \sum_i v'_i X_i + v'_l \sum_i v_i X_i$ . For the class  $y^{[2]} + [x, y] + [x, z]$  this gives

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

*Three facts about  $\Lambda_{\mathcal{D}}$ .* Let  $A = \bigoplus_m \mathfrak{I}_{\mathcal{D}}^m / \mathfrak{I}_{\mathcal{D}}^{m+1}$ , and write  $\bar{X}_1, \bar{X}_2, \bar{X}_3$  and  $\bar{X}_4$  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 2.9(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  $\mathfrak{I}_{\mathcal{D}}^m$ ; here  $X_3^2 = z^2 - 1$ . Hence the monomials  $\bar{X}_1^{a_1} \bar{X}_2^{a_2} \bar{X}_3^{a_3} \bar{X}_4^{a_4}$  form a basis of  $A$ , and, since the coefficients of  $h_{\mathbb{F}_2[\mathcal{D}]}$  are 1, 3, 5, 7, 7, 5, 3, 1,

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

Because  $x$  and  $w$  are central and  $x^2 = y^2 = w^2 = z^4 = 1$ , the elements  $\bar{X}_1$  and  $\bar{X}_4$  are central in  $A$  and  $\bar{X}_1^2 = \bar{X}_2^2 = \bar{X}_4^2 = \bar{X}_3^4 = 0$ . Moreover  $\bar{X}_3 \bar{X}_2 = \bar{X}_2 \bar{X}_3 + \bar{X}_4$ , because  $X_3 X_2 + X_2 X_3 = zy + yz = zy(w-1) \equiv X_4 \pmod{\mathfrak{I}_{\mathcal{D}}^3}$ ; by induction  $\bar{X}_3^j \bar{X}_2 = \bar{X}_2 \bar{X}_3^j + j \bar{X}_3^{j-1} \bar{X}_4$  for  $j \geq 1$ .

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

Second, for  $m < 7$  the map  $A_m \rightarrow A_{m+1}^3$ ,  $\xi \mapsto (\xi \bar{X}_1, \xi \bar{X}_2, \xi \bar{X}_3)$ , is injective. Let  $\xi = \sum_\mu b_\mu \mu$  over the basis monomials  $\mu = \bar{X}_1^{a_1} \bar{X}_2^{a_2} \bar{X}_3^{a_3} \bar{X}_4^{a_4}$  of degree  $m$ . Right multiplication by  $\bar{X}_1$  maps the

monomials with  $a_1 = 0$  to distinct basis monomials and kills the others, and right multiplication by  $\bar{X}_3$  maps those with  $a_3 \leq 2$  to distinct basis monomials and kills those with  $a_3 = 3$ . So  $\xi \bar{X}_1 = \xi \bar{X}_3 = 0$  forces  $\xi = \sum_{a_2, a_4} b_{a_2 a_4} \bar{X}_1 \bar{X}_2^{a_2} \bar{X}_3^3 \bar{X}_4^{a_4}$ . Then

$$\begin{aligned} \xi \bar{X}_2 &= b_{00}(\bar{X}_1 \bar{X}_2 \bar{X}_3^3 + \bar{X}_1 \bar{X}_3^2 \bar{X}_4) + b_{01} \bar{X}_1 \bar{X}_2 \bar{X}_3^3 \bar{X}_4 \\ &\quad + b_{10} \bar{X}_1 \bar{X}_2 \bar{X}_3^2 \bar{X}_4, \end{aligned}$$

a combination of distinct basis monomials, so  $\xi \bar{X}_2 = 0$  forces  $\xi = b_{11} \bar{X}_1 \bar{X}_2 \bar{X}_3^3 \bar{X}_4$ , which has degree 7. Hence  $\xi = 0$  when  $m < 7$ .

Third, the same holds for  $\xi \mapsto (\xi(\bar{X}_2 + \bar{X}_3), \xi(\bar{X}_2 + \bar{X}_1), \xi \bar{X}_1)$ , because this triple is obtained from  $(\bar{X}_1, \bar{X}_2, \bar{X}_3)$  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 2.8(c). So the injectivity used here, and with it the correction term  $s_{\mathcal{D}}$ , 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  $\Lambda_{\mathcal{D}}$ .

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

**2.7. Infinitude.** This subsection assembles the local bounds of Subsection 2.6 into the Golod–Shafarevich function  $P_B$  of (2.41), shows that  $P_B(34/117) < 0$  (Lemma 2.42), and concludes that  $G_B$  is infinite (Proposition 2.43). Theorem 2.46 uses this to obtain fields of every degree  $2^n$  over  $B$  with  $n \geq 49$ .

By Definition 2.37 and the Hilbert polynomials listed before it,

$$\begin{aligned} (2.40) \quad \psi_{C_2}(t) &= \frac{t^2}{1+t}, & \psi_{C_2 \times C_2}(t) &= 2t - 1 + \frac{1}{(1+t)^2}, \\ \psi_{C_4}(t) &= \frac{t^4}{(1+t)(1+t^2)}, & \psi_{\mathcal{D}}(t) &= 3t - 1 + \frac{1}{h_{\mathbb{F}_2[\mathcal{D}]}(t)}. \end{aligned}$$

With  $s_{\mathcal{D}}$  as in Lemma 2.39, the *Golod–Shafarevich function* of  $G_B$  is

$$(2.41) \quad P_B(t) = 1 - 8t + 2\psi_{C_2}(t) + 4\psi_{C_2 \times C_2}(t) + 2\psi_{\mathcal{D}}(t) - s_{\mathcal{D}}(t) + 3\psi_{C_4}(t).$$

In the proof of Proposition 2.43, the term  $-8t$  comes from the eight generators of a free group mapping onto  $G_B$ ; the terms in  $\psi_{C_2}$ ,  $\psi_{C_2 \times C_2}$ ,  $\psi_{\mathcal{D}}$  and  $\psi_{C_4}$  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  $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$ ; and  $-s_{\mathcal{D}}$  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 2.42.**

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

*Proof.* By (2.40), (2.41), the formula for  $s_{\mathcal{D}}$  in Lemma 2.39 and  $h_{\mathbb{F}_2[\mathcal{D}]}(t) = (1+t)^3(1+t^2)^2$  (Lemma 2.9(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 2.43.** *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 5,  $\bar{x}_1, \bar{y}_1, \bar{z}_1$  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  $\mathfrak{F}$  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  $\pi: \mathfrak{F} \rightarrow \Delta$  be the composite and  $\mathcal{M}$  as in Lemma 2.36, so that  $h_{\mathcal{M}} = 1 - (1 - 8t)h_{\Lambda}$ .

By Lemma 2.30(b), the image in  $\Delta$  of each local group is the prescribed group  $\Gamma$ , and  $\text{gr}_n \Gamma \rightarrow \text{gr}_n \Delta$  is injective for  $n = 1, 2$ ; this is the hypothesis of Lemma 2.38. Indeed, for  $\Gamma = \mathcal{D}$  this is stated in Lemma 2.30(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  $\text{Frob}_{t_k}$ ,  $k = 1, 2, 3$ , 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  $\Gamma = \mathcal{D}$ ; and  $t_1, t_2, t_3$ , with  $\Gamma = C_4$  generated by the Frobenius. For each of these places  $\nu$ , let  $U_\nu$  be the module  $U$  of Lemma 2.38(c) for this  $\Gamma$ , formed with the lifts of the local generators at  $\nu$ . Every generator of  $N_B$  in Lemma 2.25 is of the form  $W(u_1, \dots, u_k)$  for one of these places and some  $W$  in the kernel of  $\mathfrak{F}_k \rightarrow \Gamma$ , and conversely every such element lies in  $N_B$ . By Lemma 2.36,  $\mathcal{M} = \sum_\nu U_\nu$ . Let  $U'$  be the sum of the  $U_\nu$  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 2.25, its row also lies in the  $\Lambda$ -span of their rows (Lemma 2.36), which is contained in  $U'$ . Hence  $\Lambda \partial \rho_{\mathfrak{p}_1} \subset U_{\mathfrak{p}_1} \cap U'$ . By Lemma 2.32(h4) and (h2), Lemma 2.38(c) and Lemma 2.39, for  $0 < t < 1$ ,

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

that is,  $1 \leq h_{\Lambda}(t)P_B(t)$ . Since  $h_{\Lambda}(t) > 0$ , this contradicts  $P_B(34/117) < 0$  (Lemma 2.42).  $\square$

**2.8. The Fields.** This subsection proves Theorem 2.46: the existence of the fields  $K$ , their root discriminant  $\text{rd}(K) = \lambda$ , the bound  $\theta \geq \theta_*$  on the signature of  $F = K^{\langle \iota_1 \rangle}$ , and the splitting and local types at the selected primes. These are the properties of the fields used in Sections 3–5, in Section 8 and in Section 11.

**Definition 2.44.** The *root discriminant* of a number field  $M$  with discriminant  $\Delta_M$  is  $\text{rd}(M) = |\Delta_M|^{1/[M:\mathbb{Q}]}$ .

**Definition 2.45.** 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 2.46.** *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  $\iota_1$  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  $\iota_1$  of Definition 2.13, 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  $\iota_1$  in  $\text{Gal}(K/B)$ . The extension  $K/F$  is quadratic and unramified at every finite place. Let  $\mathfrak{p} \in S \cup \{\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3\}$ . Every prime of  $F$  above  $\mathfrak{p}$  splits in  $K$ , the primes of  $K$  and of  $F$  above  $\mathfrak{p}$  have the absolute type of Table 6, and the completions of  $K$  at the primes above  $\mathfrak{p}$  are the local extensions listed there. The type of  $\mathfrak{p}$  in  $K/B$  is  $(8, 4)$  if  $\mathfrak{p}$  lies above 2,  $(2, 2)$  if it lies above 3 or 5, and  $(1, 4)$  if it is a capped prime. In particular  $K/F$  has uniform local types  $(e_r, f_r)_{r \in \{2, 3, 5, 29\}}$  in the sense of Definition 8.7.

TABLE 6. Absolute types of the places of  $K$  and  $F$  above 2, 3, 5, 29 and above the prime  $\mathfrak{t}_3$  of  $B$  above 41, 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 $\mathcal{D}$                                  | $2^{9/4}$                |
| 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 $C_2 \times C_2$  | $5^{1/2}$                |
| 29                           | $(1, 4)$     | unramified of degree 4 over $\mathbb{Q}_{29}$                             | 1                        |
| 41 (above $\mathfrak{t}_3$ ) | $(1, 4)$     | unramified of degree 4 over $\mathbb{Q}_{41}$                             | 1                        |
| 241                          | $e = 2$      | unramified                                                                | $241^{1/2}$              |

*Proof. Existence.* By Proposition 2.43,  $G_B$  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  $\bar{\sigma} \circ h = (\sigma \circ h) \circ (h^{-1}\iota_\sigma h)$ , 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  $\iota_j$  in  $H$  is the complex conjugation at the place of  $K$  below the place of  $B_S$  fixed in Definition 2.13. Hence every complex conjugation at a place of  $K$  above  $v_j$  is conjugate in  $H$  to the image of  $\iota_j$ , and has elementary image  $\bar{\iota}_j$ , since conjugation preserves elementary images. In particular, two choices of  $\iota_1$  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  $h$  lies in the centralizer  $C_H(\iota_1) = \{h \in H : h\iota_1 = \iota_1 h\}$ . Similarly, if  $\iota'$  is complex conjugation for an embedding  $\sigma_2$  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 2.30(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  $N_\iota$  of the conjugacy class of  $\iota_1$  in  $H$ , that is,  $b/d = 1/(2N_\iota)$ . This class maps onto the class in  $\bar{G}_B$

of the element  $\iota_1$  of Definition 2.13, which has  $2^{15}$  elements by Lemma 2.30(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  $\mathfrak{p} \in S \cup \{\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3\}$ . 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 2.30(b) shows that this image is  $\mathcal{D}$ ,  $C_2 \times C_2$  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  $B_{\mathfrak{t}_1} = B_{\mathfrak{t}_2} = \mathbb{Q}_{29}$  and  $B_{\mathfrak{t}_3} = \mathbb{Q}_{41}$ , the places of  $K$  above  $\mathfrak{p}$  have the absolute types of Table 6, and the types in  $K/B$  stated in the theorem. 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  $\iota_1$  has elementary image  $\bar{\iota}_1$ . By Lemma 2.30(d),  $\iota_1$  lies in no decomposition group of a prime above  $S \cup \{\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3\}$ , so the decomposition group of  $\mathfrak{P}$  in  $\text{Gal}(K/F) = \langle \iota_1 \rangle$  is trivial. Hence the places of  $F$  above  $\mathfrak{p}$  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 2.9(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 2.47.* Consider the variant of the construction in which the third cap is placed at the inert prime  $\mathfrak{t}_0 = 7\mathcal{O}_B$  instead of at  $\mathfrak{t}_3$ . Its quotient by the fourth Zassenhaus term, its relation spaces  $R_2$  and  $R_3$ , and the class of  $\iota_1$  are the same as here: the proof of Lemma 2.30(a) uses only the generators of  $N_B$  in (i)–(iii) of Lemma 2.25 and the commutators  $[[\hat{y}_j, \hat{z}_j], \hat{z}_j]$ , since a fourth power lies in  $D_4 \mathfrak{F}$ . The two towers also have the same Golod–Shafarevich function, since both impose three conditions of type  $C_4$ . They differ at the primes above 7 and 41.

*Remark 2.48.* The Lean formalization [21] formalizes the present tower, with its caps at  $\mathfrak{t}_1, \mathfrak{t}_2$  and  $\mathfrak{t}_3$ . Remark 4.38 states what it proves.

### 3. THE KUMMER FIELD AND ITS QUADRATIC $L$ -FUNCTIONS

The analytic estimate of Sections 4–7 compares every field of Theorem 2.46 with a fixed subfield. The simplest choice of this subfield is 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 (2.4) and  $V$  as in Lemma 2.5(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. Here the comparison field is a larger field  $E_{W''} \supset E$  (Section 5), whose zeta function contains  $\zeta_E$  as a factor. This section shows that  $E$  lies in every field of Theorem 2.46. It then writes  $\zeta_E$  as the product of  $\zeta_B$  and 255 quadratic Hecke  $L$ -functions of  $B$ , and determines their conductors, gamma factors, root numbers and Euler factors. The field  $E$  does not depend on the choice of the capped primes.

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  $\tau(n)$ ; it is not to be confused with the inertia generators  $\tau_{\mathfrak{p}}$  of Definition 2.13, whose elementary images  $\bar{\tau}_{\mathfrak{p}}$  appear in Lemma 3.5.

**3.1. The Characters of the Kummer Field.** This subsection fixes the characters  $\chi_e$  of  $\text{Gal}(E/B) \cong \mathbb{F}_2^8$  (Definition 3.1) and shows that  $E$  lies in every field of the tower (Lemma 3.2).

By Lemma 2.11,  $[E : B] = 256$ , and the elementary image  $\bar{g} \in \mathbb{F}_2^8$  of Definition 2.12, 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  $\chi_e$  be the character  $g \mapsto (-1)^{\langle \bar{g}, e \rangle}$  of  $\text{Gal}(E/B)$ .

The character  $\chi_e$  takes the values  $\pm 1$ ; in terms of the  $\mathbb{F}_2$ -valued Kummer characters  $\kappa_a$  of Definition 2.12,  $\chi_e(g) = (-1)^{\kappa_{\alpha_e}(g)}$ . Since  $g(\sqrt{\alpha_e}) = \chi_e(g) \sqrt{\alpha_e}$ , the character  $\chi_e$  cuts out  $B_e$ , and the 256 characters  $\chi_e$  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 2.5(d)).

**Lemma 3.2.** *The fixed field of the Frattini subgroup  $D_2 G_B$  of  $G_B$  is  $E$ . Consequently  $E$  is contained in every field  $K$  of Theorem 2.46.*

*Proof.* Let  $G_S$  be the group of Subsection 2.3, so that  $G_S/D_2 G_S = \text{Gal}(E/B)$  (Lemma 2.11), and let  $G_B = G_S/N$  as in Definition 2.23. By Lemma 2.24(b),  $N \subseteq D_2 G_S$ , so  $G_B/D_2 G_B = G_S/D_2 G_S = \text{Gal}(E/B)$ . A field  $K$  of Theorem 2.46 contains the fixed field of  $D_4 G_B \subseteq D_2 G_B$ , and hence contains  $E$ .  $\square$

**3.2. Local Data.** This subsection computes the conductor exponents and the Frobenius values of every character  $\chi_e$  (Proposition 3.4), expresses them through the elementary images of the local generators (Lemma 3.5), and records the types of the primes of  $B$  in  $E/B$  (Corollary 3.7). They give the Euler factors and conductors of Subsection 3.3, and the Frobenius vectors used by the census of Section 4.

**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  $\mathfrak{p} = \mathfrak{t}_k$ ,  $k = 1, 2, 3$ , it is the vector of  $\text{Frob}_{\mathfrak{t}_k}$  in Table 5, and for  $\mathfrak{p} = \mathfrak{t}_4$  it is 00110100 (Lemma 2.14). By Euler's criterion,  $(\overline{\text{Frob}}_{\mathfrak{p}})_i = 1$  exactly when  $\alpha_i$  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  $\chi_e$ , and if  $c_{\mathfrak{p}}(e) = 0$ , let  $\chi_e(\mathfrak{p}) \in \{\pm 1\}$  be the value of  $\chi_e$  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  $\alpha_i$  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  $\alpha_i$  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 2.13, which fixes  $\sqrt{\alpha_i}$ , acts on square roots by  $(-\alpha_i, \cdot)_{\mathfrak{p}}$  (Table 5).*
- (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,  $\chi_e$  is nontrivial at  $v_k$ , exactly when  $\alpha_e < 0$  at  $v_k$ .
- (5) The conductor of  $\chi_e$  is the ideal  $\mathfrak{f}_e = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{c_{\mathfrak{p}}(e)}$  of  $\mathcal{O}_B$ .

*Proof.* For (1),  $\mathfrak{p}$  is odd and  $\alpha_e$  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  $\alpha_e$  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  $U^{(n)} = 1 + p^n \mathbb{Z}_p$  [18].

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  $v_k$ . For (5),  $c_{\mathfrak{p}}(e) = 0$  for  $\mathfrak{p} \notin S$  by (1).  $\square$

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  $\alpha_i$  the generator of  $\mathfrak{p}$ ,  $(u, \alpha_e)_{\mathfrak{p}} = (-1)^{\langle \bar{v}_{\mathfrak{p}}, e \rangle}$  and  $(-\alpha_i, \alpha_e)_{\mathfrak{p}} = (-1)^{\langle \bar{v}_{\mathfrak{p}}, e \rangle}$ . 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 5: 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  $\iota_k$  negates  $\sqrt{\alpha_e}$  exactly when  $\alpha_e < 0$  at  $v_k$  (Lemma 2.8(a)), and it multiplies  $\sqrt{\alpha_e}$  by  $(-1)^{\langle \bar{v}_k, e \rangle}$ .  $\square$

**Definition 3.6.** For  $e \in \mathbb{F}_2^8$  and  $k = 1, 2$  put  $\nu_k(e) = \langle \bar{v}_k, e \rangle \in \{0, 1\}$ , where  $\bar{v}_k$  is the elementary image of the complex conjugation  $\iota_k$  (Table 5).

By Proposition 3.4(4) and Lemma 3.5, for  $e \neq 0$  we have  $\nu_k(e) = 1$  exactly when the real place  $v_k$  becomes complex in  $B_e$ , that is, when  $\chi_e$  is nontrivial at  $v_k$ .

**Corollary 3.7.** *The type (Definition 2.45) 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 the capped primes  $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$  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 5), 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  $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$  are nonzero (Table 5).  $\square$

**3.3. The Zeta Function of the Kummer Field.** This subsection factors  $\zeta_E$  into  $\zeta_B$  and 255 quadratic Hecke  $L$ -functions (Proposition 3.8), and records their coefficients, completed forms, functional equations and conductors (Proposition 3.9, Corollary 3.11). These are the input of the approximate functional equation in Section 4.

Let  $\chi_B$  be the Dirichlet character  $n \mapsto (n/241)$ .

**Proposition 3.8.** *For  $\operatorname{Re} s > 1$ ,*

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

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

*Proof.* Compare Euler factors at a prime  $\mathfrak{p}$  of  $B$ . Let  $T_{\mathfrak{p}} \subseteq Z_{\mathfrak{p}} \subseteq G = \operatorname{Gal}(E/B)$  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  $\zeta_E$  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  $\zeta_{B_e}/\zeta_B$ . 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  $\chi_B$ .  $\square$

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  $\Delta_M$  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 3.9.** *Let  $e \neq 0$ , write  $L(s, \chi_e) = \sum_{n \geq 1} a_n(e) n^{-s}$ , and put*

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

- (1) *The coefficients  $a_n(e)$  are integers with  $|a_n(e)| \leq \tau(n)$ . The Euler factor at a rational prime  $p$  is  $\prod_{\mathfrak{p}|p} (1 - \chi_e(\mathfrak{p}) N\mathfrak{p}^{-s})^{-1}$ , 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 3.8 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  $\chi_e$  is nontrivial [11, 38]. The discriminants satisfy  $|\Delta_{B_e}| = |\Delta_B|^2 N\mathfrak{d}_{B_e/B}$ , 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  $|\Delta_{B_e}|/|\Delta_B| = 241 N\mathfrak{f}_e = Q_e$ . By Definition 3.6, Proposition 3.4(4) and Lemma 3.5, 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  $\chi_e$ , which is entire of order at most one [11, 38].

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 3.10.** Let  $e \neq 0$ . The *gamma factor* of  $\chi_e$  is  $\Gamma_{\mathbb{R}}(s + \nu_1(e))\Gamma_{\mathbb{R}}(s + \nu_2(e))$ , the factor in the definition of  $\Lambda(s, \chi_e)$  in Proposition 3.9. It is *pure* if  $\nu_1(e) = \nu_2(e)$ ; writing  $\nu$  for the common value, it then 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 3.11.** For  $e \neq 0$ ,  $Q_e = 241 \cdot 2^i \cdot m$ , where  $2^i = 2^{c_{p_1}(e) + c_{p_2}(e)} \in \{1, 4, 8, 16, 32, 64\}$  and  $m = 3^{c_{q_1}(e) + c_{q_2}(e)} 5^{c_{r_1}(e) + c_{r_2}(e)}$  divides 225. The number of characters  $\chi_e$  with given  $2^i$  and  $m$  is given by the table

|        |                    |    |    |    |    |    |    |    |    |     |              |
|--------|--------------------|----|----|----|----|----|----|----|----|-----|--------------|
| (3.12) | $2^i \backslash m$ | 1  | 3  | 5  | 9  | 15 | 25 | 45 | 75 | 225 | <i>total</i> |
|        | 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           |
|        | <i>total</i>       | 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 (Proposition 3.4(5)), so  $Q_e = 241 \text{Nf}_e$  with

$$\text{Nf}_e = 2^{c_{p_1}(e) + c_{p_2}(e)} 3^{c_{q_1}(e) + c_{q_2}(e)} 5^{c_{r_1}(e) + c_{r_2}(e)}.$$

By Proposition 3.4,  $c_{p_j}(e) \in \{0, 2, 3\}$  and  $c_{q_j}(e), c_{r_j}(e) \in \{0, 1\}$ , and by Lemma 3.5 these exponents are determined by the vectors of Table 5; counting the 255 vectors  $e \neq 0$  gives the table, which the supplementary program `check255.gp` also prints (Remark 3.13). No nontrivial character has  $\text{Nf}_e = 1$ , since  $B$  has class number one and a unit of norm  $-1$  (Lemma 2.5(a),(b)), so that its narrow class number is one. The range of  $Q_e$  can be read off from the table.  $\square$

*Remark 3.13.* The supplementary program `lfun241.py` (directory `papers/0.04273/certificates` of [23]) 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  $n \leq N_e = 4\lfloor\sqrt{Q_e}\rfloor + 1$ , from Propositions 3.4 and 3.9(1). For the values used here (Subsection 4.7), the program `ye_hp.py` computes the coefficients up to the larger truncation point  $8\lfloor\sqrt{Q_e}\rfloor + 1$  of that subsection. The supplementary program `check255.gp`, in the same directory, 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  $\zeta_{B_e}/\zeta_B$ . All agree. It also prints the table (3.12), the counts of Proposition 3.9(3) and the range of  $Q_e$ . These comparisons check the implementation; the identification of the  $L$ -functions rests on Propositions 3.4 and 3.9.

#### 4. THE RELATIVE ZETA VALUE

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 2.23). These are the fields  $K$  of Theorem 2.46.

For  $K \in \mathcal{K}$  we use the notation of Theorem 2.46:  $\iota_1$  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  $\iota_1$  are conjugate in  $\text{Gal}(K/B)$  and give conjugate fields  $F$ ; hence  $b, c, \theta$  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  $\gamma$  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 2.45).

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

$$\frac{1}{d} \log L_F(1) < C_{\text{eff}} := 0.0422764.$$

The proof of Theorem 4.2 is completed in Section 7. This section proves the general criterion, Proposition 4.19, and encloses  $\zeta_E$  at real points (Proposition 4.31); Sections 5 and 6 supply the other inputs of the criterion.

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 four steps. Monotonicity of the completion of  $L_F$  reduces the value at  $s = 1$  to  $\zeta_K$  at real points  $\sigma > 1$  (Subsection 4.1). Along a sequence of fields of growing degree, the normalized numbers of primes of each prime power norm  $q$  converge to limiting densities  $\beta_q$  (Lemma 4.13), and  $d^{-1} \log L_F(1)$  is bounded in the limit by  $Z(1) = \sum_q \beta_q g_1(q)$ , where  $g_s(q) = -\log(1 - q^{-s})$ ; the Tsfasman–Vlăduț inequality bounds a weighted sum of the  $\beta_q$  (Subsection 4.2). The *selected primes* of  $B$ , those above 2, 3, 5 and the capped primes, have the same type in every field of the tower, so their part of  $Z(1)$  is known exactly (Subsection 4.3). For each other prime of  $B$  we use a lower bound for its residue degree, a *floor*, and a kernel inequality with several abscissae bounds the rest of  $Z(1)$  by a combination, with coefficients of both signs, of *floor sums*: the sums of the terms of these primes at residue degree equal to the floor, evaluated at real points  $\sigma_j > 1$  (Proposition 4.19). Sections 5–7 supply the floors and the values: the floors come from a field  $E_{W''}$  contained in every field of the tower and from a census, and the values come from the factorization of  $\zeta_{E_{W''}}$  into  $L$ -functions. Throughout,  $\sigma$  denotes a real number greater than 1 and  $\varepsilon = \sigma - 1$ ; in this section  $\varepsilon$  is this positive number, not the unit  $\alpha_1$  of (2.4).

**4.1. Reduction to  $s > 1$ .** This subsection shows that  $L_F(1) > 0$ , by the class-number formula, and that the completion  $\mathcal{L}_F$  of  $L_F$ , defined in (4.5) below, is positive and nondecreasing on  $[1, \infty)$  (Lemma 4.6). Together with a comparison of Euler products they bound  $L_F(1)$  by  $\zeta_K$  at a real point  $1 + \varepsilon$  (Lemma 4.8), which Lemma 4.13 uses.

For a number field  $A$ , write  $h_A$ ,  $\text{Reg}_A$ ,  $w_A$  and  $\Delta_A$  for its class number, regulator, number of roots of unity and discriminant. The residue of  $\zeta_A$  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  $\zeta_K$ , 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  $\Lambda_A$  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 [11, 38],  $\mathcal{L}_F$  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  $\rho$  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  $\Xi$  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  $\Xi$  is even,  $\Xi'/\Xi$  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  $\Upsilon$  is affine in  $\theta$ ,  $\Upsilon(\varepsilon, \theta) \rightarrow 0$  as  $\varepsilon \downarrow 0$ , uniformly for  $0 \leq \theta \leq \frac{1}{2}$ .  $\square$

The term  $\Upsilon$  does not appear in the final estimate. With  $\varepsilon = 1/300$ , (4.9) would add  $\Upsilon(1/300, \theta) \approx 0.0054$  for  $\theta$  near  $\frac{1}{2}$ . Instead, the proof of Lemma 4.13 applies (4.9) with  $s - 1$  in place of  $\varepsilon$  for each fixed  $s \in (1, 2]$ , passes to the limit along a sequence of fields, and then lets  $s \downarrow 1$ , so that  $\Upsilon$  vanishes in the limit; the change from the real points  $\sigma > 1$  back to 1 is then paid for through the Tsfasman–Vlăduț inequality (Propositions 4.15 and 4.19). This limit is also the reason why  $m_0$  is not effective.

**4.2. The Tsfasman–Vlăduț Inequality over  $B$ .** This subsection passes to limits along sequences of fields of  $\mathcal{K}$  (Lemma 4.13). The limit densities  $\beta_q$  and the function  $Z(s)$  defined there are the quantities that Propositions 4.15 and 4.19 bound, and the Tsfasman–Vlăduț inequality bounds  $\sum_q \beta_q w(q)$ . Lemma 4.10 first writes the normalized logarithm of a Dedekind zeta function as a sum over the primes of  $B$ .

For real  $q > 1$  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*

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

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

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  $N\mathfrak{p}^f$ , and  $[M : \mathbb{Q}] = 2[M : B]$ . This gives both formulas. The first equality in (4.12) follows from  $-\zeta'_M/\zeta_M(s) = \sum_{\mathfrak{p}} \log N\mathfrak{p}/(N\mathfrak{p}^s - 1)$ . 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.

**Lemma 4.13.** *Let  $C' \in \mathbb{R}$ , and let  $K^{(j)} \in \mathcal{K}$ ,  $j \geq 1$ , be fields of strictly increasing degree. Let  $F^{(j)}$  and  $d_j = [F^{(j)} : \mathbb{Q}]$  be the field  $F$  and the number  $d$  attached to  $K^{(j)}$  above, so that  $[K^{(j)} : \mathbb{Q}] = 2d_j$ , and suppose that  $d_j^{-1} \log L_{F^{(j)}}(1) \geq C'$  for every  $j$ . For a prime power  $q$  let  $N_q(K)$  be the number of primes of  $K$  of norm  $q$ . After passing to a subsequence, the limit  $\beta_q = \lim_j N_q(K^{(j)})/(2d_j)$  exists for every prime power  $q$ , and  $Z(s) = \sum_q \beta_q g_s(q)$ , for real  $s \geq 1$ , satisfies:*

- (a)  $Z(s) = \lim_j [K^{(j)} : \mathbb{Q}]^{-1} \log \zeta_{K^{(j)}}(s)$  for every real  $s > 1$ ;
- (b)  $\sum_q \beta_q w(q) \leq 2\kappa_\infty$ ;
- (c)  $C' \leq Z(1) < \infty$ .

*Proof.* If  $q = p^f$ , then  $N_q(K) \leq [K : \mathbb{Q}]/f$ , since the local degrees above  $p$  add up to  $[K : \mathbb{Q}]$ . So  $N_q(K^{(j)})/(2d_j) \leq 1$ , and a diagonal argument gives a subsequence along which  $\beta_q$  exists for every  $q$ . The fields  $K^{(j)}$  have strictly increasing degrees, so they are pairwise non-isomorphic.

(a) 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  $\sum_q q^{-s} < \infty$ .

(b) 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  $\mathfrak{g}(K^{(j)}) = d_j \ell$  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

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

(c) 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  $Z(1) < \infty$  by (b). By Lemma 4.8 with  $s-1$  in place of  $\varepsilon$ , and by (a), 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  $Z(1)$  by monotone convergence, and the supremum tends to zero. Hence  $C' \leq Z(1)$ .  $\square$

The next proposition is the form of this argument with one abscissa. Here it serves only for comparison (Remark 4.36 and Section 12) and for the Lean formalization (Remark 4.38).

**Proposition 4.15.** *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  $K \in \mathcal{K}$ , and let  $Y'_*$  be a real number with*

$$Y'_* \geq \sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{2e_{\mathfrak{p}}^0(N\mathfrak{p}^{2f_{\mathfrak{p}}^0} - 1)}.$$

*Then every  $C' > Y_* + \varepsilon(\kappa_{\infty} + Y'_*)$  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.* Suppose not, and let  $K^{(j)}$ ,  $\beta_q$  and  $Z$  be as in Lemma 4.13. 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  $Z(1) \leq Z(1 + \varepsilon) + \varepsilon(\kappa_{\infty} + \sum_q \beta_q \log q/(q^2 - 1))$ . By Fatou's lemma, (4.12) for  $M = K^{(j)}$ , and the monotonicity in Lemma 4.10,

$$\sum_q \beta_q \frac{\log q}{q^2 - 1} \leq \liminf_j \sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{2e_{K^{(j)}}(\mathfrak{p})(N\mathfrak{p}^{2f_{K^{(j)}}(\mathfrak{p})} - 1)} \leq Y'_*.$$

Finally  $Z(1 + \varepsilon) \leq Y_*$  by Lemma 4.13(a). Thus  $C' \leq Z(1) \leq Y_* + \varepsilon(\kappa_{\infty} + Y'_*)$ , a contradiction.  $\square$

By (4.12) and the monotonicity in Lemma 4.10,  $Y'_*$  bounds  $-[K : \mathbb{Q}]^{-1}(\zeta'_K/\zeta_K)(2)$  for every  $K \in \mathcal{K}$ , as  $Y_*$  bounds  $[K : \mathbb{Q}]^{-1} \log \zeta_K(\sigma)$ .

**4.3. Selected Primes and Floors.** This subsection separates the primes of  $B$  whose type is the same in every  $K \in \mathcal{K}$ , the selected primes, whose contribution  $Z_{\text{sel}}(1)$  to  $Z(1)$  is computed exactly (Lemma 4.17), from the free primes, which enter Proposition 4.19 only through lower bounds for their residue degrees, the floors of Definition 4.18.

**Definition 4.16.** The *selected primes* of  $B$  are the six primes of  $S$ , which lie above 2, 3 and 5 (Lemma 2.5(c),(d)), and the capped primes  $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$  (Definition 2.13). The other primes of  $B$  are *free*. For a prime power  $q$  put

$$\beta_q^{\text{sel}} = \sum_{\mathfrak{p}} \frac{1}{2e_K(\mathfrak{p})f_K(\mathfrak{p})},$$

the sum over the selected primes  $\mathfrak{p}$  with  $N\mathfrak{p}^{f_K(\mathfrak{p})} = q$ , where  $(e_K(\mathfrak{p}), f_K(\mathfrak{p}))$  is the type of  $\mathfrak{p}$  in  $K/B$  given by Theorem 2.46; it is the same for every  $K \in \mathcal{K}$ . Put

$$Z_{\text{sel}}(s) = \sum_q \beta_q^{\text{sel}} g_s(q) \quad (s \geq 1), \quad T_{\text{sel}} = \sum_q \beta_q^{\text{sel}} w(q).$$

The places of  $F$  above the selected primes of  $B$  form the set of finite places used in the geometric construction (Section 11); in Subsection 1.2 they are also called selected.

**Lemma 4.17.** *The numbers  $\beta_q^{\text{sel}}$  are  $1/32$  for  $q = 16$ ,  $1/4$  for  $q = 9, 25, 29^4$ ,  $1/8$  for  $q = 41^4$ , and 0 for every other prime power  $q$ . For every  $K \in \mathcal{K}$  and every prime power  $q$ , the number  $N_q^{\text{sel}}(K)$  of primes of  $K$  of norm  $q$  above selected primes of  $B$  satisfies  $N_q^{\text{sel}}(K)/[K : \mathbb{Q}] = \beta_q^{\text{sel}}$ . Moreover*

$$0.0416684840321404 < Z_{\text{sel}}(1) < 0.0416684840321405, \\ 0.2004555342790642 < T_{\text{sel}} < 0.2004555342790643.$$

*Proof.* By Theorem 2.46 the types are  $(8, 4)$  at  $\mathfrak{p}_1, \mathfrak{p}_2$ , which have norm 2;  $(2, 2)$  at the two primes above 3 and the two above 5, which have norms 3 and 5; and  $(1, 4)$  at  $\mathfrak{t}_1, \mathfrak{t}_2$ , of norm 29, and at  $\mathfrak{t}_3$ , of norm 41. The definition then gives the values of  $\beta_q^{\text{sel}}$ . A prime  $\mathfrak{p}$  of  $B$  of type  $(e, f)$  in the Galois extension  $K/B$  has  $[K : B]/(ef) = d/(ef)$  primes of  $K$  above it, each of norm  $N\mathfrak{p}^f$ , and  $[K : \mathbb{Q}] = 2d$ ; this gives  $N_q^{\text{sel}}(K)/[K : \mathbb{Q}] = \beta_q^{\text{sel}}$ . The two numbers are evaluated in Arb interval arithmetic by the supplementary program `signed.py` (its functions `zsel` and `B_r`).  $\square$

Since  $K/B$  is unramified outside  $S$ , every free prime has  $e_K(\mathfrak{p}) = 1$ .

**Definition 4.18.** Put  $q_{\min} = 41^4 = 2825761$ . A *system of floors* is a choice of an integer  $f_{\mathfrak{p}}^0 \geq 1$ , the *floor* of  $\mathfrak{p}$ , for every free prime  $\mathfrak{p}$  of  $B$  such that

$$(F11) \quad f_{\mathfrak{p}}^0 \text{ divides } f_K(\mathfrak{p}) \text{ for every } K \in \mathcal{K};$$

$$(F12) \quad N\mathfrak{p}^{f_{\mathfrak{p}}^0} \geq q_{\min}.$$

Its *floor sum* is

$$Y_{\text{fl}}(\sigma) = \sum_{\mathfrak{p} \text{ free}} \frac{g_{\sigma}(N\mathfrak{p}^{f_{\mathfrak{p}}^0})}{2f_{\mathfrak{p}}^0} \quad (\sigma > 1).$$

The series converges, since  $g_{\sigma}(x^f)/f \leq g_{\sigma}(x)$  for  $x > 1$  and  $f \geq 1$ , and  $\sum_{\mathfrak{p}} g_{\sigma}(N\mathfrak{p}) = \log \zeta_B(\sigma)$ . By (F11), the floors are an admissible choice, at the free primes, of the lower bounds  $f_{\mathfrak{p}}^0$  of Proposition 4.15; this is why the same symbol is used.

By (4.11), the floor sum is the part of the termwise bound for  $[K : \mathbb{Q}]^{-1} \log \zeta_K(\sigma)$  that comes from the free primes, for a hypothetical field in which every free prime has residue degree equal to its floor. The floors used in this paper are those of Definition 5.20.

**4.4. A Signed Kernel.** Proposition 4.15 passes from  $1 + \varepsilon$  to 1 through the uniform bound  $g_1(q) - g_{1+\varepsilon}(q) \leq \varepsilon \log q/(q - 1)$ . The next proposition, the criterion that proves Theorem 4.2 in Section 7, replaces it by a kernel inequality between  $g_1$ , a combination  $\mathbf{K}$  of several functions  $g_{\sigma_i}$  with coefficients of either sign, and the weight  $w$  of the Tsfasman–Vlăduț inequality. Such a combination can follow the function  $(g_1 - b_{\text{TV}}w)_+$ , where  $b_{\text{TV}} \geq 0$  is the multiplier of  $w$  in the proposition, far more closely than a single multiple of  $g_{\sigma}$ .

**Proposition 4.19.** *Let  $(f_{\mathfrak{p}}^0)$  be a system of floors (Definition 4.18), with floor sum  $Y_{\text{fl}}$ , and let  $Z_{\text{sel}}$  and  $T_{\text{sel}}$  be as in Definition 4.16 and  $\kappa_{\infty}$  as in Subsection 4.2. Let  $1 < \sigma_1 < \dots < \sigma_n$ , let  $c_1, \dots, c_n$  be real numbers of either sign, let  $b_{\text{TV}} \geq 0$ , and define the kernel  $\mathbf{K}(q) = \sum_i c_i g_{\sigma_i}(q)$  for real  $q > 1$ . Suppose that, for every real  $q \geq q_{\min}$ ,*

$$(i) \quad \mathbf{K}(q) \geq g_1(q) - b_{\text{TV}} w(q), \quad (ii) \quad \mathbf{K}(q) \geq 0, \quad (iii) \quad \mathbf{K} \text{ is non-increasing on } [q_{\min}, \infty).$$

*Then every*

$$C' > Z_{\text{sel}}(1) + \sum_{i=1}^n c_i Y_{\text{fl}}(\sigma_i) + b_{\text{TV}} (2\kappa_{\infty} - T_{\text{sel}})$$

*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.* Suppose not, and let  $K^{(j)}$ ,  $\beta_q$  and  $Z$  be as in Lemma 4.13, applied with this  $C'$ . Write  $N_q(K) = N_q^{\text{sel}}(K) + N_q^{\text{free}}(K)$ , where  $N_q^{\text{free}}(K)$  counts the primes of  $K$  of norm  $q$  above free primes of  $B$ , and put  $\mu_j(q) = N_q^{\text{free}}(K^{(j)})/(2d_j)$ . By Lemma 4.17,  $\beta_q^{\text{free}} = \beta_q - \beta_q^{\text{sel}} = \lim_j \mu_j(q)$  for every  $q$ , and  $\beta_q^{\text{free}} \geq 0$ .

*One field.* Fix  $j$  and write  $K = K^{(j)}$  and  $d = d_j$ . A free prime  $\mathfrak{p}$  of  $B$  with  $f = f_K(\mathfrak{p})$  has  $d/f$  primes of  $K$  above it, each of norm  $\text{Np}^f$ . By (F11),  $f$  is a multiple of  $f_{\mathfrak{p}}^0$ , so  $1/(2f) \leq 1/(2f_{\mathfrak{p}}^0)$ , and  $\text{Np}^f \geq \text{Np}^{f_{\mathfrak{p}}^0} \geq q_{\min}$  by (F12). By (ii) and (iii), the primes of  $K$  above  $\mathfrak{p}$  contribute

$$\frac{d/f}{2d} \text{K}(\text{Np}^f) = \frac{\text{K}(\text{Np}^f)}{2f} \leq \frac{\text{K}(\text{Np}^{f_{\mathfrak{p}}^0})}{2f_{\mathfrak{p}}^0}$$

to  $\sum_q \mu_j(q) \text{K}(q)$ . Summing over the free primes,

$$\sum_q \mu_j(q) \text{K}(q) \leq \Sigma_{\text{K}} := \sum_{\mathfrak{p} \text{ free}} \frac{\text{K}(\text{Np}^{f_{\mathfrak{p}}^0})}{2f_{\mathfrak{p}}^0} = \sum_{i=1}^n c_i Y_{\text{fl}}(\sigma_i),$$

where the series defining  $\Sigma_{\text{K}}$  converges absolutely, since  $|\text{K}| \leq \sum_i |c_i| g_{\sigma_i}$ , and may be summed term by term. Note also that  $\mu_j$  is supported on  $[q_{\min}, \infty)$ , hence so is  $\beta^{\text{free}}$ .

*The limit.* Since  $\text{K} \geq 0$  on  $[q_{\min}, \infty)$ , Fatou's lemma gives  $\sum_q \beta_q^{\text{free}} \text{K}(q) \leq \liminf_j \sum_q \mu_j(q) \text{K}(q) \leq \Sigma_{\text{K}}$ . By (i) at every  $q$  in the support of  $\beta^{\text{free}}$ , by  $b_{\text{TV}} \geq 0$ , and by Lemma 4.13(b),

$$\sum_q \beta_q^{\text{free}} g_1(q) \leq \sum_q \beta_q^{\text{free}} \text{K}(q) + b_{\text{TV}} \sum_q \beta_q^{\text{free}} w(q) \leq \Sigma_{\text{K}} + b_{\text{TV}} (2\kappa_{\infty} - T_{\text{sel}}),$$

where we used  $\sum_q \beta_q^{\text{free}} w(q) = \sum_q \beta_q w(q) - T_{\text{sel}}$ . With Lemma 4.13(c),

$$C' \leq Z(1) = Z_{\text{sel}}(1) + \sum_q \beta_q^{\text{free}} g_1(q) \leq Z_{\text{sel}}(1) + \sum_i c_i Y_{\text{fl}}(\sigma_i) + b_{\text{TV}} (2\kappa_{\infty} - T_{\text{sel}}),$$

which contradicts the choice of  $C'$ .  $\square$

*Remark 4.20.* Condition (ii) follows from (iii), since  $\text{K}(q) \rightarrow 0$  as  $q \rightarrow \infty$ ; it is checked separately. The proof uses the floors only through (F11) and (F12), and the selected primes only through their exact types. The right-hand side of the proposition is at least  $Z_{\text{sel}}(1)$ , since  $\Sigma_{\text{K}} \geq 0$  by (ii) and  $2\kappa_{\infty} > T_{\text{sel}}$  (Remark 4.37). With  $n = 1$  and  $c_1 \geq 1$  it is the refined Tsfasman–Vlăduț step of Proposition 12.9, without the adaptive credits  $R_{\mathfrak{p}}(f_K(\mathfrak{p})) + \rho_K(\mathfrak{p}) I_{\mathfrak{p}}(f_K(\mathfrak{p}))$  of Definition 12.2 and Proposition 12.4.

**4.5. An Approximate Functional Equation for Two Gamma Factors.** This subsection and the next two enclose  $\zeta_E(\sigma)$  at the abscissae of Section 7 (Proposition 4.31), through the factorization of Proposition 3.8. The factors  $L(\sigma, \chi_e)$  are computed from an approximate functional equation (Lemma 4.21), whose kernels are bounded by envelopes (Lemmas 4.22 and 4.23) and enclosed on a grid (Subsection 4.6). For real  $\mu$  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 4.22(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 [2]. 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 4.21.** *Let  $a_n$  be real numbers with  $|a_n| \leq \tau(n)$ , where  $\tau(n)$  is the number of divisors of  $n$ , 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  $\operatorname{Re} w > 0$  [24, 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 4.22.** *Let  $\mu \in \mathbb{R}$ .*

- (1) *The functions  $H_\mu$  and  $I_\mu$  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  $H_\mu$  as the Laplace transform of  $u^{\mu-1} du$  on  $[1, \infty)$ . Taking the order 0 in [24, 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  $I_\mu$ , 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  $I_\mu$  we use  $K_0(x) \leq K_{1/2}(x) = \sqrt{\pi/(2x)} e^{-x}$  [24, 10.39.2]. It holds because the modified Bessel function of order  $\eta \geq 0$  is  $\int_0^\infty e^{-x \cosh r} \cosh(\eta r) dr$  [24, 10.32.9], which increases with  $\eta$ . 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 [24, 10.25.1, 10.29.3].  $\square$

The next lemma bounds the tails of the two series of Lemma 4.21. In the application  $1 < \sigma \leq 101/100$ , so its hypothesis  $1 < \sigma \leq 3/2$  holds.

**Lemma 4.23.** *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.* Since  $1 < \sigma \leq 3/2$  and  $\nu \in \{0, 1\}$ , every  $\mu \in \{\sigma, 1 - \sigma\}$  satisfies  $\mu \leq 2$  and every  $\mu \in \{\sigma + \nu - 1, \nu - \sigma\}$  satisfies  $\mu \leq 3/2$ ; so Lemma 4.22(2) gives  $H_\mu \leq \mathcal{V}_1$  in (1) and  $I_\mu \leq \mathcal{V}_2$  in (2). 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  $n > N$ . Hence

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

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  $y \geq \omega + \nu - \frac{3}{2}$ .  $\square$

**4.6. Enclosures of  $H_\mu$  and  $I_\mu$ , and Finite Sums.** This subsection encloses the kernels  $H_\mu$  and  $I_\mu$  on a geometric grid (Lemma 4.25) and bounds the error of the resulting approximation of the finite sums of Lemma 4.21 (Lemma 4.26); Lemma 4.29 uses the second, which rests on the first. An *enclosure* of a real number is an interval that contains it. Let  $H$  be  $H_\mu$  or  $I_\mu$  with  $\mu$  as in Lemma 4.23, 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 4.24.** *Let  $\xi > 0$  and let  $h_j = H^{(j)}(\xi)/j!$  be the Taylor coefficients of  $H$  at  $\xi$ .*

(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  $\xi$  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 4.22. 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 4.22(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 4.24 are enclosed with the rigorous exponential and Bessel functions of Arb [15], which is now part of FLINT [39] and is called through its Python interface.

**Lemma 4.25.** *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  $\xi_i$  by the recurrences of Lemma 4.24(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 4.22,  $H(\xi_0) \in [0, \mathcal{V}(64)]$ . Suppose that the enclosure of  $H(\xi_i)$  contains  $H(\xi_i)$ . The true Taylor coefficients at  $\xi_i$  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 4.24(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  $\operatorname{Bin}_i = \{n : 1 \leq n \leq N, \xi_{i+1} < tn \leq \xi_i\}$ . These sets partition  $\{1, \dots, N\}$ . For nonempty  $\operatorname{Bin}_i$ , let  $\bar{n}_i$  be the integer part of the average of its least and largest elements, and put

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

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

**Lemma 4.26.** *With this notation,*

$$(4.27) \quad \left| \sum_{n=1}^N a_n n^\nu H(tn) - \sum_i \sum_{j=0}^J P_{i,j} M_{i,j} \right| \leq \sum_i \rho_J(\xi_i) A_i,$$

*where  $i$  runs over the indices with  $\operatorname{Bin}_i$  nonempty.*

*Proof.* Let  $n \in \text{Bin}_i$ . Then  $|tn - \xi_i| < \xi_i/32$ , so by Lemma 4.24(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  $n \in \text{Bin}_i$  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 3.11). So every argument  $tn$  exceeds 0.0033, and the part of the grid below that point is not used.

**4.7. The Values of  $\zeta_E$ .** This subsection encloses  $Y_E(\sigma) = \log \zeta_E(\sigma)/512$  at the abscissae of Table 9 (Proposition 4.31); these values enter  $Y_{W''}$  through (5.14).

Let  $\sigma \in (1, 101/100]$  be rational, and let  $e \in \mathbb{F}_2^8 \setminus \{0\}$ . By Proposition 3.9,  $L(s, \chi_e) = \sum_n a_n(e) n^{-s}$  satisfies the hypotheses of Lemma 4.21 with  $Q = Q_e$  and  $\nu_k = \nu_k(e)$  (Definition 3.6). Put  $t = 2\pi/\sqrt{Q_e}$  and let the truncation point be

$$N_e^{\text{afe}} = 8\lfloor \sqrt{Q_e} \rfloor + 1,$$

about twice the number  $N_e = 4\lfloor \sqrt{Q_e} \rfloor + 1$  of coefficients computed in Remark 3.13, so that the enclosures are narrow enough for Proposition 4.19.

**Lemma 4.28.** *For every  $e \in \mathbb{F}_2^8 \setminus \{0\}$ , with  $t = 2\pi/\sqrt{Q_e}$  and  $N = N_e^{\text{afe}}$ ,*

$$tN < 50.6 < \xi_0, \quad t > 0.0033 > \xi_{i_1}, \quad 49.0 < t(N+1) < 50.6.$$

*Hence Lemma 4.26 applies with this  $t$  and  $N$ , and for  $\nu \in \{0, 1\}$  the conditions on  $t(N+1)$  in Lemma 4.23 hold for every  $\omega$  in the list  $\frac{101}{100}, \frac{21}{20}, \frac{11}{10}, \frac{9}{8}, \frac{6}{5}, \frac{5}{4}, \frac{4}{3}, \frac{3}{2}, 2$ .*

*Proof.* By Corollary 3.11,  $723 \leq Q_e \leq 3470400$ . Since  $\sqrt{Q_e} - 1 < \lfloor \sqrt{Q_e} \rfloor \leq \sqrt{Q_e}$ ,

$$tN \leq 2\pi \left( 8 + \frac{1}{\sqrt{Q_e}} \right) \leq 2\pi \left( 8 + \frac{1}{\sqrt{723}} \right) < 50.6, \quad t(N+1) > 2\pi \left( 8 - \frac{6}{\sqrt{Q_e}} \right) \geq 2\pi \left( 8 - \frac{6}{\sqrt{723}} \right) > 48.8,$$

and  $t \geq 2\pi/\sqrt{3470400} > 0.0033$ . Moreover  $\xi_0 = 64$  and  $\xi_{i_1} \leq 2^{-80}$ . The conditions on  $t(N+1)$  in Lemma 4.23 are  $t(N+1) \geq \omega - 1$  and  $t(N+1) \geq \omega + \nu - \frac{3}{2}$ , whose right sides are at most  $\frac{3}{2}$  for  $\omega \leq 2$  and  $\nu \leq 1$ . Finally,  $Q_e$  takes the 53 values  $241 \cdot 2^i \cdot m$  with a nonzero entry in (3.12), and evaluating  $t(N+1)$  at these values gives  $49.0 < t(N+1) < 50.6$ ; the extremes, 49.07 and 50.59, occur at  $Q_e = 723$  and  $Q_e = 964$ .  $\square$

Let  $\Pi_e$  be the prefactor of Lemma 4.21:  $\Pi_e = t^\sigma/\Gamma(\sigma)$  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  $S^{(1)}$  and  $S^{(2)}$  be the sums  $\sum_i \sum_{j=0}^{20} P_{i,j} M_{i,j}$  of Lemma 4.26, with  $N = N_e^{\text{afe}}$ ,  $a_n = a_n(e)$  and  $J = 20$ , for the two functions of the series of Lemma 4.21:  $H = H_\sigma$  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. By Lemma 4.28, Lemma 4.26 applies, and Lemma 4.23 applies with every  $\omega$  in the list above; the value of  $\omega$  in this list is chosen to minimize the bound

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

**Lemma 4.29.** *For rational  $\sigma \in (1, 101/100]$  and every  $e \in \mathbb{F}_2^8 \setminus \{0\}$ ,*

$$(4.30) \quad |L(\sigma, \chi_e) - \Pi_e(S^{(1)} + S^{(2)})| \leq 2\Pi_e \mathcal{T}_e.$$

*Proof.* Split each of the two series of Lemma 4.21 at  $N_e^{\text{afe}}$ . By Lemma 4.26, each finite part differs from its approximation  $S^{(1)}$  or  $S^{(2)}$  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 4.23, each tail is at most  $\zeta(\omega)^2 (N_e^{\text{afe}} + 1)^{\omega+\nu} \mathcal{V}(t(N_e^{\text{afe}} + 1))$ . Multiplying by  $\Pi_e$  gives (4.30).  $\square$

**Proposition 4.31.** *Put  $Y_E(\sigma) = \log \zeta_E(\sigma)/512$ . For each of the abscissae  $\sigma$  of Table 9, the supplementary program `ye_hp.py` computes an enclosure of  $Y_E(\sigma)$  of width less than  $1.3 \cdot 10^{-19}$ , by (4.30) and*

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

For example,

$$0.085358048288873992 < Y_E(1001/1000) < 0.085358048288873993.$$

*Proof (computer-assisted).* The factorization is Proposition 3.8. The coefficients  $a_n(e)$  for  $n \leq N_e^{\text{afe}}$  are computed exactly from the Euler factors of Proposition 3.4 by the functions of the supplementary program `lfun241.py`, and the program `afe241.py`, both in the directory `papers/0.04273/certificates` of [23] and called unchanged by `ye_hp.py`, evaluates (4.30) in Arb midpoint-radius interval arithmetic [15, 39] with 256 bits of precision, rounding every quantity outward. Its routines for Lemmas 4.21–4.26 are taken unchanged from the data archive in `papers/0.0418235/certificates` of [23], whose members are checked against their SHA-256 hashes when it is unpacked, 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].  $\square$

**4.8. Frobenius Vectors and the Set  $\mathcal{P}_4$ .** This subsection defines a set  $\mathcal{P}_4$  of free primes of norm at most  $10^6$  by a condition on their Frobenius vectors (Definition 4.32), and shows that their residue degree in every  $K \in \mathcal{K}$  is divisible by 4 (Lemma 4.33); these primes receive the floor  $f_{\mathfrak{p}}^0 = 4$  in Definition 5.20. We use the group  $G_B$  of Definition 2.23 and its Zassenhaus filtration  $D_n G_B$ , the relation space  $R_2$  in degree two (Definition 2.26), which Lemma 2.29 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 4.32.** Let  $\Sigma_2 = \{v \in \mathbb{F}_2^8 : v^{[2]} \in R_2\}$ , and let  $\mathcal{P}_4$  be the set of free primes  $\mathfrak{p}$  of  $B$  with  $N_{\mathfrak{p}} \leq 10^6$  and  $\overline{\text{Frob}}_{\mathfrak{p}} \notin \Sigma_2$ .

**Lemma 4.33.** *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  $f_K(\mathfrak{p})$  is a power of two and at least 4, so 4 divides  $f_K(\mathfrak{p})$ .*

*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 2.29, which uses the complete list of generators of  $N_B$  in Lemma 2.25, 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, and this order is a power of two because  $\text{Gal}(K/B)$  is a 2-group.  $\square$

**Lemma 4.34.** *The set  $\Sigma_2$  of Definition 4.32 has exactly 21 elements: zero and the following twenty vectors, written as strings  $c_0 c_1 \cdots c_7$  of their coordinates, as in Section 2:*

|          |          |          |          |           |
|----------|----------|----------|----------|-----------|
| 00100000 | 11110010 | 11010010 | 00010000 | 10000001  |
| 10010001 | 00001000 | 10100111 | 10101111 | 00000100  |
| 11101011 | 11101111 | 00000010 | 01100101 | 01100111  |
| 00000001 | 01011010 | 01011011 | 10111010 | 11000101. |

In the notation of Table 5, 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  $\iota_1$  and  $\iota_2$ .

*Proof.* Each of these images lies in  $\Sigma_2$  by Lemma 2.29, since an involution has trivial square. The supplementary program `census241.py` computes  $\Sigma_2$  by linear algebra over  $\mathbb{F}_2$  from the relations of Lemma 2.29, and finds no other vectors.  $\square$

**Proposition 4.35** (Frobenius vectors of the primes of norm at most  $10^6$ ). *Among the 78616 free primes  $\mathfrak{p}$  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` (directory `papers/0.04273/certificates` of [23]) 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  $\Sigma_2$  (Lemma 4.34). It was written for the variant of the construction with the cap at  $\mathfrak{t}_0$  instead of  $\mathfrak{t}_3$  (Remark 2.47), whose free primes differ from the present ones only in that  $\mathfrak{t}_3$  is free and  $\mathfrak{t}_0$  is not; both have Frobenius vectors outside  $\Sigma_2$ , so the three counts are the same for both. The program `adaptive41.py` enumerates the free primes of the present tower and reproduces the three counts.  $\square$

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

*Remark 4.36.* With  $E$  as the comparison field, Proposition 4.15 at  $\sigma = 301/300$  gives the bound  $C = 0.04871285$  for the present tower. Its lower bounds  $(e_{\mathfrak{p}}^0, f_{\mathfrak{p}}^0)$  are the types in  $K$  at the selected primes,  $(1, 4)$  at the primes of  $\mathcal{P}_4$  (Lemma 4.33), and the types in  $E$  at the other free primes. By (4.11) and Lemma 4.10 one may take  $Y_* = Y_E(\sigma) - \Delta_{\text{sel}}^E(\sigma) - \Delta_4^E(\sigma)$ , where  $\Delta_{\text{sel}}^E(\sigma)$  is the sum over the selected primes of the difference between the terms in (4.11) for  $M = E$  and for  $M = K$ , and  $\Delta_4^E(\sigma) = \sum_{\mathfrak{p} \in \mathcal{P}_4} (g_{\sigma}(N\mathfrak{p}^2)/4 - g_{\sigma}(N\mathfrak{p}^4)/8)$ ;  $Y_*$  is bounded from the same lower bounds. Compared with the variant with the cap at  $\mathfrak{t}_0$  (Remark 2.47), the terms of  $\mathfrak{t}_0$  and of  $\mathfrak{t}_3$  change places between  $\Delta_{\text{sel}}^E$  and  $\Delta_4^E$ , with the same formula  $g_{\sigma}(N\mathfrak{p}^2)/4 - g_{\sigma}(N\mathfrak{p}^4)/8$ , so the totals are the same for both; the supplementary program `ceiling41.py` (directory `papers/0.042901/certificates` of [23]) computes the upper bound  $0.04871284289\dots$ . With this  $C$ , the margin of Section 11 with re-optimized profiles gives the exponent 1.042901 (Table 2). This bound is not used in the proof of Theorem 1.1.

*Remark 4.37.* The selected primes alone limit what Proposition 4.19 can give. In the notation of its proof,  $\Sigma_K \geq 0$  by condition (ii), and  $2\kappa_{\infty} - T_{\text{sel}} > 1.07 > 0$ . So no system of floors, abscissae and coefficients gives a bound below  $Z_{\text{sel}}(1) = 0.04166848403\dots$  (Lemma 4.17), the contribution of the selected primes to  $Z(1)$ . It exceeds the corresponding number for the variant with the cap at  $\mathfrak{t}_0$  by  $2.3 \cdot 10^{-8}$ , because the selected primes above 41 replace those above 7. The bound  $C_{\text{eff}} = 0.0422764$  exceeds  $Z_{\text{sel}}(1)$  by  $6.08 \cdot 10^{-4}$ ; Section 12 discusses what this means for the exponent.

*Remark 4.38* (The Lean formalization). The Lean formalization [21] proves a weaker form of Theorem 1.1, under one explicit hypothesis that it does not prove: for the fields of the present tower, there are finite planar sets  $U_j$  with  $|U_j| \rightarrow \infty$  and  $u(U_j)/|U_j|^{20863/20000} \rightarrow \infty$ , where  $20863/20000 = 1.04315$ , provided that

$$(4.39) \quad \frac{\log \zeta_{E_{W''}}(1 + \frac{1}{4411})}{8192} + \frac{1}{4411} \left( \frac{\ell - \gamma - \log(4\pi)}{4} - \frac{1}{8192} \frac{\zeta'_{E_{W''}}(2)}{\zeta_{E_{W''}}} \right) < 0.050969,$$

where  $E_{W''}$  is the field of Definition 5.7, given in the formalization by explicit generators  $\sqrt{\beta_i}$  over  $E$  for four dihedral forms that span  $W''$ . This is the bound of Proposition 4.15 at  $\sigma = 1 + 1/4411$  with comparison field  $E_{W''}$  in place of  $E$ . The formalization proves in Lean that  $[E_{W''} : \mathbb{Q}] = 8192$ , that  $E_{W''}$  lies in the fixed base of the tower, the local data of  $E_{W''}$  at 2 and at fifty split primes

below 1000, the resulting bound 0.0425 for  $d^{-1} \log L_F(1)$ , and the margin at the exponent 1.04315. The supplementary program `h.w.receipt.py` bounds the left side of (4.39) by 0.0509172, from the enclosures of Proposition 6.5 and an explicit bound for the logarithmic derivative. The formalization does not cover the census beyond norm 1000, the signed kernel or the general shell weights.

## 5. DIHEDRAL QUOTIENTS OF THE TOWER AND THE FIELD $E_{W''}$

Every field  $K \in \mathcal{K}$  contains the fixed field of  $D_3 G_B$  (Theorem 2.46), whose Galois group over  $B$  is the extension  $G_B/D_3 G_B$  of  $G_B/D_2 G_B = \text{Gal}(E/B) = \mathbb{F}_2^8$  by  $\text{gr}_2 G_B = D_2 G_B/D_3 G_B$ , of dimension 15 (Lemma 2.29). The Kummer field  $E$  sees only the quotient  $\mathbb{F}_2^8$ . In particular, a prime of  $B$  whose Frobenius vector is 0 splits completely in  $E$ , and the comparison with  $E$  treats it as if it split completely in  $K$ . This section uses the layer  $\text{gr}_2 G_B$ : through dihedral quotients of  $G_B$  it gives lower bounds for residue degrees, by a census for primes of norm at most  $4 \cdot 10^{13}$  and through the field  $E_{W''}$  for all norms, and it supplies the system of floors of Definition 5.20.

Subsection 5.1 identifies the linear forms on  $\text{gr}_2 G_B$  with quadratic forms and finds the 27 forms of dihedral type; Subsection 5.2 realizes each of them by a dihedral field contained in every  $K \in \mathcal{K}$ . Subsection 5.3 defines the space  $W''$  spanned by four of these forms. Subsection 5.4 reports the census of the primes of degree one with Frobenius vector 0. Subsection 5.5 studies the field  $E_{W''}$  and factors its zeta function into the  $L$ -functions evaluated in Section 6, and Subsection 5.6 defines the floors and expresses their floor sum through  $\zeta_{E_{W''}}$ , for use in Section 7.

In Sections 5–7, supplementary programs and data files are named by their paths relative to the directory `certificates/dihedral` if they lie in it, and relative to `certificates` otherwise; the names are unique.

For  $r, v \in \mathbb{F}_2^8$  we write  $r \cdot v = \sum_i r_i v_i \in \mathbb{F}_2$ , and, as in Definition 3.1,  $\alpha_r = \prod_i \alpha_i^{r_i}$  and  $\chi_r(g) = (-1)^{r \cdot \bar{g}}$ , where  $\bar{g} \in \mathbb{F}_2^8$  is the elementary image of  $g$  (Definition 2.12). We use the same symbol  $\chi_r$  for the inflation of this character to any Galois group over  $B$  that maps onto  $\text{Gal}(E/B)$ . We write  $\text{Dih}_4$  for the dihedral group of order 8.

**5.1. Linear forms on  $\text{gr}_2 G_B$ .** This subsection identifies the linear forms on  $\text{gr}_2 G_B$  with quadratic forms on  $\mathbb{F}_2^8$  (Lemma 5.1) and isolates the 27 forms whose polar form has rank 2 (Lemma 5.4). All of them are of dihedral type (Definition 5.2), and the next subsection realizes each of them by a dihedral field.

Recall (Lemma 2.27) that  $\text{gr}_2 G_B = \mathfrak{L}_2/R_2$ , where  $\mathfrak{L}_2$  is the degree-two part of the free restricted Lie algebra on  $\mathfrak{L}_1 = \mathbb{F}_2^8$  and  $R_2$  is the relation space (Definition 2.26). A *quadratic form* on  $\mathbb{F}_2^8$  is a function  $Q: \mathbb{F}_2^8 \rightarrow \mathbb{F}_2$  such that  $Q(v+w) - Q(v) - Q(w)$  is bilinear in  $v, w$ ; this bilinear form is its *polar form*. It is alternating, and its rank is even.

**Lemma 5.1.** *For a linear form  $\psi$  on  $\mathfrak{L}_2$  put  $q_\psi(v) = \psi(v^{[2]})$ . Then  $\psi \mapsto q_\psi$  is a linear bijection from the dual of  $\mathfrak{L}_2$  onto the space of quadratic forms on  $\mathbb{F}_2^8$ , and the polar form of  $q_\psi$  is  $\text{pol}_\psi(v, w) = \psi([v, w])$ . The linear forms on  $\text{gr}_2 G_B$  are the  $\psi$  that vanish on  $R_2$ .*

*Proof.* The identity  $(v+w)^{[2]} = v^{[2]} + w^{[2]} + [v, w]$  shows that  $q_\psi$  is a quadratic form with polar form  $\psi([v, w])$ . The map is injective, because  $\mathfrak{L}_2$  is spanned by the restricted squares  $v^{[2]}$ , the brackets being differences of them. Both spaces have dimension 36.  $\square$

**Definition 5.2.** A linear form  $\psi$  on  $\text{gr}_2 G_B$  is of *dihedral type* if there are linearly independent  $r_1, r_2 \in \mathbb{F}_2^8$  and  $\mathbf{r} \in \mathbb{F}_2^2 \setminus \{0\}$  such that, with  $\phi(v) = (r_1 \cdot v, r_2 \cdot v)$ ,

$$q_\psi(v) = \begin{cases} 1 & \text{if } \phi(v) = \mathbf{r}, \\ 0 & \text{otherwise.} \end{cases}$$

We call  $(r_1, r_2, \mathbf{r})$  *data* for  $\psi$ , and  $\phi$  its *associated map*  $\mathbb{F}_2^8 \rightarrow \mathbb{F}_2^2$ .

**Lemma 5.3.** *Let  $\psi$  be of dihedral type with data  $(r_1, r_2, \mathbf{r})$  and associated map  $\phi$ . Then  $\text{pol}_\psi(v, w) = \det(\phi(v), \phi(w))$ ; it has rank 2, and its radical is  $\ker \phi$ .*

*Proof.* The function  $x \mapsto [x = \mathbf{r}]$  on  $\mathbb{F}_2^2$  is  $x_1x_2$ ,  $x_1 + x_1x_2$  or  $x_2 + x_1x_2$  for  $\mathbf{r} = (1, 1), (1, 0), (0, 1)$ . The linear terms have polar form 0, and  $x_1x_2$  has polar form  $x_1y_2 + x_2y_1 = \det(x, y)$ . Since  $q_\psi(v) = [\phi(v) = \mathbf{r}]$  and  $\phi$  is linear,  $\text{pol}_\psi(v, w) = \det(\phi(v), \phi(w))$ . As  $r_1, r_2$  are linearly independent,  $\phi$  is surjective, and  $\det$  is nondegenerate on  $\mathbb{F}_2^2$ ; so the radical is  $\ker \phi$ , of codimension 2.  $\square$

**Lemma 5.4.** *Exactly 27 of the  $2^{15} - 1$  nonzero linear forms on  $\text{gr}_2 G_B$  have a polar form (Lemma 5.1) of rank 2. All of them are of dihedral type (Definition 5.2), and they span the dual of  $\text{gr}_2 G_B$ . The polar forms of the other nonzero forms have rank 4, 6 or 8. We number the 27 forms 0 to 26 as in the file `d4all27.json`, and write  $\psi_o$  for the form number  $o$ .*

*Proof (computer-assisted).* The supplementary programs `d4search.py` and `plane.py` enumerate the linear forms on  $\mathfrak{L}_2$  that vanish on the space  $R_2$  of `lie241.py` (Lemma 2.29), compute the ranks of their polar forms, and, for those of rank 2, find data  $(r_1, r_2, \mathbf{r})$ ; the 27 forms and their data are listed in `d4all27.json`.  $\square$

**5.2. Dihedral fields.** This subsection realizes each form of dihedral type by a Galois extension  $M/B$  with group  $\text{Dih}_4$ , contained in every  $K \in \mathcal{K}$ , and shows how  $M$  forces even residue degrees (Lemma 5.5); the elements that define these fields exist for all 27 forms (Lemma 5.6). The census and the field  $E_{W''}$  are built from these fields.

**Lemma 5.5.** *Let  $\psi$  be a form of dihedral type with data  $(r_1, r_2, \mathbf{r})$  (Definition 5.2). Put  $F_0 = B(\sqrt{\alpha_{r_1}}, \sqrt{\alpha_{r_2}})$ , a biquadratic extension of  $B$  contained in  $E$ , and identify  $\text{Gal}(F_0/B)$  with  $\mathbb{F}_2^2$  through the signs by which an element multiplies  $\sqrt{\alpha_{r_1}}$  and  $\sqrt{\alpha_{r_2}}$ . Let  $\beta \in F_0^\times$  be a unit outside the primes above  $S$  such that, for each  $\sigma \neq 1$  in  $\text{Gal}(F_0/B)$  (in this lemma  $\sigma$  denotes such an element):*

- (D1)  $\sigma(\beta)/\beta = u_\sigma^2$  for some  $u_\sigma \in F_0^\times$ ;
- (D2) the number  $t_\sigma = u_\sigma \sigma(u_\sigma)$ , which is  $\pm 1$ , is  $-1$  exactly when  $\sigma = \mathbf{r}$ .

Let  $M = F_0(\sqrt{\beta})$ . Then:

- (a)  $M$  is Galois over  $B$  with group isomorphic to  $\text{Dih}_4$ . The elements of  $\text{Gal}(M/B)$  with image  $\mathbf{r}$  in  $\text{Gal}(F_0/B)$  have order 4.
- (b)  $M$  lies in the fixed field of  $D_3 G_B$ , hence in every  $K \in \mathcal{K}$ . The quotient map  $\pi_M: G_B \rightarrow \text{Gal}(M/B)$  maps  $D_2 G_B$  to the center  $\langle z \rangle$  of  $\text{Gal}(M/B)$ , by  $g \mapsto z^{\psi([g]_2)}$ , where  $[g]_2$  is the class of  $g$  in  $\text{gr}_2 G_B$ .
- (c) Let  $\mathfrak{p} \notin S$  be a prime of  $B$  that splits completely in  $F_0$ , and suppose that  $\beta$  is not a square in the residue field of a prime of  $F_0$  above  $\mathfrak{p}$ . Then  $f_K(\mathfrak{p})$  is even for every  $K \in \mathcal{K}$ . The hypothesis does not depend on the prime of  $F_0$  above  $\mathfrak{p}$ .
- (d) Let  $\mathfrak{p} \notin S$  have Frobenius vector 0. Then the Frobenius elements in  $G_B$  of the primes of  $B_G$  above  $\mathfrak{p}$  lie in  $D_2 G_B$ , and they have the same class  $\overline{\text{Frob}}_{\mathfrak{p}}^{(2)} \in \text{gr}_2 G_B$ . The hypothesis of (c) holds exactly when  $\psi(\overline{\text{Frob}}_{\mathfrak{p}}^{(2)}) = 1$ .

*Proof.* Since  $\sigma^2 = 1$ ,  $t_\sigma^2 = (\sigma(\beta)/\beta) \cdot \sigma(\sigma(\beta)/\beta) = \sigma^2(\beta)/\beta = 1$ , so  $t_\sigma = \pm 1$ .

(a) Every conjugate of  $\beta$  over  $B$  is  $\beta$  times a square in  $F_0$ , so  $M$  is Galois over  $B$ . If  $\beta$  were a square in  $F_0$ , we could take  $u_\sigma = \sigma(\sqrt{\beta})/\sqrt{\beta}$ , and then  $t_\sigma = 1$  for every  $\sigma$ , contrary to (D2); so  $[M : B] = 8$ . Let  $\tilde{\sigma} \in \text{Gal}(M/B)$  lift  $\sigma \neq 1$ . Then  $\tilde{\sigma}(\sqrt{\beta}) = \eta u_\sigma \sqrt{\beta}$  with  $\eta = \pm 1$ , and  $\tilde{\sigma}^2(\sqrt{\beta}) = \eta \sigma(u_\sigma) \eta u_\sigma \sqrt{\beta} = t_\sigma \sqrt{\beta}$ . So  $\tilde{\sigma}^2$  is the generator  $z$  of  $\text{Gal}(M/F_0)$  exactly when  $\sigma = \mathbf{r}$ . The group  $\text{Gal}(M/B)$  has order 8, a central subgroup  $\langle z \rangle$  (a normal subgroup of order two), and quotient  $\mathbb{F}_2^2$ ; among such groups,  $C_2^3$  has no element of order four,  $C_4 \times C_2$  has elements of order four above two of the three nonzero classes of the quotient, the quaternion group above all three, and  $\text{Dih}_4$  above exactly one. Hence  $\text{Gal}(M/B) \cong \text{Dih}_4$ . In  $\text{Dih}_4$ , an element squares to  $z$  exactly

when its image in  $\mathbb{F}_2^2$  is  $\mathbf{r}$ , and two elements have commutator  $z$  exactly when their images are linearly independent.

(b) The field  $F_0$  lies in  $E$ , so it is unramified over  $B$  outside  $S$ , and  $\beta$  is a unit outside the primes above  $S$ , which include all primes above 2; so  $M/F_0$  is also unramified outside  $S$ . Since  $[M : B] = 8$ ,  $M$  lies in  $B_S$ , and restriction gives a surjection  $\pi_M : G_S \rightarrow \text{Gal}(M/B)$ . If  $g \in G_S$  has elementary image  $v$ , then  $\pi_M(g)$  has image  $\phi(v)$  in  $\text{Gal}(F_0/B)$ , because  $g(\sqrt{\alpha_r}) = (-1)^{r \cdot v} \sqrt{\alpha_r}$ . By (a) and Lemma 5.3, for  $g, h \in G_S$  with elementary images  $v, w$ ,

$$\pi_M(g^2) = z^{q_\psi(v)}, \quad \pi_M([g, h]) = z^{\text{pol}_\psi(v, w)}.$$

We check that  $\pi_M$  kills the generators (ii)–(iv) of  $N_B$  in Lemma 2.25, more precisely their images in  $G_S$ , which generate  $N$  as a normal subgroup. The elements  $x_j^2, [x_j, y_j], [x_j, z_j], \tau_\nu^2$  and  $\varphi_\nu^2$  map to  $z^{\psi(\xi)}$ , where  $\xi$  is respectively  $\bar{x}_j^{[2]}, [\bar{x}_j, \bar{y}_j], [\bar{x}_j, \bar{z}_j], \bar{\tau}_\nu^{[2]}$  and  $\bar{\varphi}_\nu^{[2]}$ ; these lie in  $R_2$  by (2.28), and  $\psi$  vanishes on  $R_2$ . The elements  $[y_j, z_j], z_j^4, [y_j, z_j]^2$  and  $\text{Frob}_{t_k}^4$  map to 1, since  $\text{Dih}_4$  has class two and exponent four and its commutators lie in  $\langle z \rangle$ . So  $\pi_M$  factors through  $G_B$ . Since  $D_3(\text{Dih}_4) = 1$  (its Frattini subgroup is  $\langle z \rangle$ , which is central of order two),  $\pi_M$  kills  $D_3G_B$ , and  $M$  lies in the fixed field of  $D_3G_B$ , which is contained in every  $K \in \mathcal{K}$ . On  $D_2G_B$ ,  $\pi_M$  is a homomorphism to  $\langle z \rangle$  that kills  $D_3G_B$ , hence factors through  $\text{gr}_2 G_B$ ; it agrees with  $g \mapsto z^{\psi([g]^2)}$  on squares and commutators, by the formulas above, and these classes span  $\text{gr}_2 G_B$ .

(c) The prime  $\mathfrak{p}$  is unramified in  $M$ . If it splits completely in  $F_0$ , then the Frobenius of a prime  $\mathfrak{P}_M$  of  $M$  above a prime  $\mathfrak{P}$  of  $F_0$  above  $\mathfrak{p}$  lies in  $\text{Gal}(M/F_0) = \langle z \rangle$ , and it is  $z$  exactly when  $\beta$ , a unit at  $\mathfrak{P}$ , is not a square modulo  $\mathfrak{P}$ . In that case  $f_M(\mathfrak{p}) = 2$ , and 2 divides  $f_K(\mathfrak{p})$  because  $M \subseteq K$  (Lemma 4.10). The primes of  $F_0$  above  $\mathfrak{p}$  are conjugate under  $\text{Gal}(F_0/B)$ , and  $\sigma(\beta)/\beta$  is a square, so the condition does not depend on  $\mathfrak{P}$ .

(d) If the Frobenius vector of  $\mathfrak{p}$  is 0, a Frobenius element  $g \in G_B$  of a prime of  $B_G$  above  $\mathfrak{p}$  lies in  $D_2G_B$ , and the primes above  $\mathfrak{p}$  give conjugate elements, whose classes in  $\text{gr}_2 G_B$  agree because  $[G_B, D_2G_B] \subseteq D_3G_B$ . By (b),  $\pi_M(g) = z^{\psi(\overline{\text{Frob}}_{\mathfrak{p}}^{(2)})}$ , and  $\pi_M(g)$  is the Frobenius of a prime of  $M$  above  $\mathfrak{p}$ , which is  $z$  exactly when the hypothesis of (c) holds.  $\square$

**Lemma 5.6.** *For each of the 27 forms of Lemma 5.4, with the data  $(r_1, r_2, \mathbf{r})$  of `d4all27.json`, there is an element  $\beta$  satisfying the hypotheses of Lemma 5.5. For the fifteen census forms, the forms numbered 0, 5, 9, 17, 22, 14, 3, 7, 4, 15, 6, 20, 12, 24, 13 (Definition 5.9), and the seven forms of Table 7, the elements used in this paper are given by their coordinates in `d4fields15.json` and in `vd4.data27.gp`; the forms 7, 17, 20 and 24 belong to both lists, so these are 18 distinct elements, checked 22 times. For each of them, the ideal factorization involves only primes above 2, 3 and 5, and for every  $\sigma \neq 1$  in  $\text{Gal}(F_0/B)$  the quotient  $\sigma(\beta)/\beta$  is a square and the sign  $t_\sigma$  is the one required by (D2).*

*Proof (computer-assisted).* The supplementary program `d4beta.gp` finds the elements: it computes the  $S$ -units of  $F_0$  modulo squares, the elements whose conjugates are squares up to the element itself, and the linear map  $\beta \mapsto (t_\sigma)_\sigma$ , and solves for the pattern of  $\mathbf{r}$ . The programs `vd4.gp` (for the census forms) and `vplane4.gp` (for the seven forms of Table 7) verify each of the 22 (form, element) pairs in an independently built model of  $F_0$ : that  $\beta$  is a unit outside the primes above  $S$  (by PARI's `idealfactor`), that the quotients  $\sigma(\beta)/\beta$  are squares with the stated signs  $t_\sigma$ , and that the relative discriminant of  $F_0(\sqrt{\beta})/F_0$  has norm divisible only by 2, 3 and 5.  $\square$

**5.3. The space  $W''$ .** This subsection defines the space  $W''$  of linear forms on  $\text{gr}_2 G_B$  spanned by four forms of dihedral type, its subspaces  $W \subset W'$  used for the intermediate results of Section 12, and the field  $E_{W''}$  (Definition 5.7), and describes the fifteen nonzero elements of  $W''$  (Lemma 5.8). The census (Subsection 5.4) decides which primes lie in  $\ker W''$ , and Subsection 5.5 studies  $E_{W''}$ .

TABLE 7. The seven forms  $\psi_o$  of dihedral type in  $W''$ , numbered as in `d4a1127.json`, with data  $(r_{1,o}, r_{2,o}, \mathbf{r}_o)$ , the vectors written as strings of their coordinates as in Section 2, and the element  $c_o \in B$  with  $B_{c_o} = B(\sqrt{c_o})$  of Lemma 5.16. The forms satisfy  $\psi_{24} = \psi_{10} + \psi_{23}$ ,  $\psi_{20} = \psi_{10} + \psi_{19}$  and  $\psi_7 = \psi_{17} + \psi_{19}$ .

| $o$ | $r_{1,o}$ | $r_{2,o}$ | $\mathbf{r}_o$ | $c_o$                            |
|-----|-----------|-----------|----------------|----------------------------------|
| 10  | 00010011  | 01001100  | (1, 1)         | $213033204 - 13722675\sqrt{241}$ |
| 23  | 01011111  | 10001011  | (0, 1)         | $155 - 10\sqrt{241}$             |
| 24  | 01011111  | 10011000  | (0, 1)         | $(-378557 + 24385\sqrt{241})/2$  |
| 19  | 01001100  | 10000010  | (1, 1)         | $-326 + 21\sqrt{241}$            |
| 20  | 01001100  | 10010001  | (1, 1)         | $(47 - 3\sqrt{241})/2$           |
| 17  | 01000110  | 10001000  | (1, 1)         | $-31 + 2\sqrt{241}$              |
| 7   | 00001010  | 11000100  | (1, 1)         | $-3433342 + 221161\sqrt{241}$    |

**Definition 5.7.** Let  $\psi_o$ ,  $o \in \{10, 23, 24, 19, 20, 17, 7\}$ , be the forms of Table 7, with data  $(r_{1,o}, r_{2,o}, \mathbf{r}_o)$  and associated maps  $\phi_o(v) = (r_{1,o} \cdot v, r_{2,o} \cdot v)$ . Let  $F_{0,o} = B(\sqrt{\alpha_{r_{1,o}}}, \sqrt{\alpha_{r_{2,o}}})$ , let  $\beta_o \in F_{0,o}$  be the element of Lemma 5.6, and let  $M_o = F_{0,o}(\sqrt{\beta_o})$  be the dihedral field of Lemma 5.5. Put

$$W = \langle \psi_{10}, \psi_{23} \rangle \subset W' = \langle \psi_{10}, \psi_{23}, \psi_{19} \rangle \subset W'' = \langle \psi_{10}, \psi_{23}, \psi_{19}, \psi_{17} \rangle.$$

Let  $W''^\perp \subset \text{gr}_2 G_B$  be the common kernel of the forms in  $W''$ , let  $N_{W''} \subseteq D_2 G_B$  be its preimage, and let  $E_{W''}$  be the fixed field of  $N_{W''}$  in  $B_G$ . A prime  $\mathfrak{p} \notin S$  of  $B$  with Frobenius vector 0 lies in  $\ker W''$  if  $\overline{\text{Frob}_{\mathfrak{p}}}^{(2)} \in W''^\perp$  (Lemma 5.5(d)), that is, if  $\omega(\overline{\text{Frob}_{\mathfrak{p}}}^{(2)}) = 0$  for every  $\omega \in W''$ ; likewise for  $\ker W$  and  $\ker W'$ .

**Lemma 5.8.** *The space  $W''$  has dimension 4. Its 15 nonzero elements are the seven forms of Table 7, which are of dihedral type, and the eight forms  $\psi_a + \psi_b$  for the pairs*

$$(a, b) = (19, 23), (19, 24), (7, 10), (17, 10), (17, 24), (7, 24), (7, 23), (17, 23),$$

*whose polar forms have rank 4; for each of these pairs the four vectors  $r_{1,a}, r_{2,a}, r_{1,b}, r_{2,b}$  span a space of dimension 4, and  $c_a/c_b$  is not a square in  $B$ . Every subspace of the dual of  $\text{gr}_2 G_B$  that properly contains  $W''$  contains a form whose polar form has rank at least 6.*

*Proof (computer-assisted).* The supplementary program `plane4.py` computes the 15 elements and their polar ranks from `d4a1127.json`, and checks the last statement by running over all  $2^{15}$  linear forms; `vplane4.gp` verifies the seven dihedral fields (Lemma 5.6). The rank of the four vectors and the fields  $B(\sqrt{c_a}, \sqrt{c_b})$ , of degree 8 over  $\mathbb{Q}$ , are checked by `deg8/export8.gp`.  $\square$

**5.4. The census.** This subsection determines, for the primes of  $B$  of degree one with Frobenius vector 0 and norm at most  $4 \cdot 10^{13}$ , whether they lie in  $\ker W''$  and whether fifteen fixed dihedral fields detect them (Proposition 5.12). The detected primes in  $\ker W''$  receive the floor 2 in Definition 5.20, and the census determines the residue degrees in  $E_{W''}$  of the primes of small norm (Lemma 5.21).

**Definition 5.9.** The *census forms* are  $\psi_i^c = \psi_{o_i}$ ,  $1 \leq i \leq 15$ , where

$$(o_1, \dots, o_{15}) = (0, 5, 9, 17, 22, 14, 3, 7, 4, 15, 6, 20, 12, 24, 13)$$

is the order of the file `d4fields15.json`, which records their data and elements  $\beta_1^c, \dots, \beta_{15}^c$  (Lemma 5.6); let  $F_{0,i}^c$  be the field  $F_0$  of Lemma 5.5 for  $\psi_i^c$ . (The superscript distinguishes these from  $\beta_o$  and  $F_{0,o}$  of Definition 5.7, indexed by the form number  $o$ .) For a prime  $\mathfrak{p}$  of  $B$  of degree one with Frobenius vector 0, its *pattern* is

$$\text{pat}(\mathfrak{p}) = (\psi_i^c(\overline{\text{Frob}_{\mathfrak{p}}}^{(2)}))_{i \leq 15} \in \mathbb{F}_2^{15},$$

and  $\mathfrak{p}$  is *detected* if  $\text{pat}(\mathfrak{p}) \neq 0$ .

**Lemma 5.10.** *Let  $p \geq 7$  be a prime with  $(241/p) = 1$ , let  $r^2 \equiv 241 \pmod{p}$ , and let  $\mathfrak{p} = (p, \sqrt{241} - r)$ . Then  $\mathfrak{p}$  has Frobenius vector 0 exactly when  $p \equiv 1$  or  $49 \pmod{120}$  and the images of  $\alpha_1, \alpha_2, \alpha_4, \alpha_6$  under  $\sqrt{241} \mapsto r$  are squares modulo  $p$ . In that case the conjugate prime  $(p, \sqrt{241} + r)$  also has Frobenius vector 0.*

*Proof.* The residue field of  $\mathfrak{p}$  is  $\mathbb{F}_p$ , and by Definition 3.3 and Euler's criterion  $\mathfrak{p}$  has Frobenius vector 0 exactly when  $\alpha_0, \dots, \alpha_7$  are squares modulo  $\mathfrak{p}$ ; they are units at  $\mathfrak{p}$  since  $p \geq 7$  and  $p \neq 241$ . By (2.4),  $\alpha_0 = -1$ ,  $\alpha_2\alpha_3 = 2$ ,  $\alpha_4\alpha_5 = -3$ ,  $\alpha_6\alpha_7 = -5$  and  $N_{B/\mathbb{Q}}(\alpha_1) = -1$ . If  $\mathfrak{p}$  has vector 0, then  $-1, 2, -3$  and  $-5$  are squares modulo  $p$ , so  $p \equiv 1 \pmod{8}$ ,  $p \equiv 1 \pmod{3}$  and  $p \equiv \pm 1 \pmod{5}$ , that is,  $p \equiv 1$  or  $49 \pmod{120}$ . Conversely, for such  $p$  the numbers  $-1, 2, 3, 5$  are squares modulo  $p$ , and the relations show that  $\alpha_0, \alpha_3, \alpha_5, \alpha_7$  are squares modulo  $\mathfrak{p}$  when  $\alpha_2, \alpha_4, \alpha_6$  are. By (2.4), the nontrivial automorphism of  $B$  maps  $\alpha_1, \alpha_2, \alpha_4, \alpha_6$  to  $-\alpha_1^{-1}$ ,  $-\alpha_3 = -2\alpha_2^{-1}$ ,  $\alpha_5 = -3\alpha_4^{-1}$  and  $\alpha_7 = -5\alpha_6^{-1}$ , which are squares modulo  $\mathfrak{p}$  exactly when  $\alpha_1, \alpha_2, \alpha_4, \alpha_6$  are; so the conjugate prime also has vector 0.  $\square$

**Lemma 5.11.** *Let  $\mathfrak{p}$  be a prime of  $B$  of degree one with Frobenius vector 0, and  $p = N\mathfrak{p}$ , with  $\text{pat}(\mathfrak{p})$  as in Definition 5.9.*

- (a)  $\text{pat}(\mathfrak{p})_i = 1$  exactly when  $\beta_i^c$  is a nonsquare modulo a prime of  $F_{0,i}^c$  above  $\mathfrak{p}$ ; these primes have residue field  $\mathbb{F}_p$ .
- (b)  $\text{pat}(\mathfrak{p}) = 0$  exactly when  $\overline{\text{Frob}}_{\mathfrak{p}}^{(2)} = 0$ , that is, when the Frobenius elements of the primes of  $B_G$  above  $\mathfrak{p}$  lie in  $D_3G_B$ .
- (c) If  $\psi = \sum_{i \in I} \psi_i^c$  for a set  $I$  of indices, then  $\psi(\overline{\text{Frob}}_{\mathfrak{p}}^{(2)}) = \sum_{i \in I} \text{pat}(\mathfrak{p})_i$ .
- (d) If  $\mathfrak{p}$  is detected, then  $f_K(\mathfrak{p})$  is even for every  $K \in \mathcal{K}$ .
- (e)  $\psi_{17} = \psi_4^c$ ,  $\psi_{19} = \psi_4^c + \psi_8^c$ ,  $\psi_{10} = \psi_4^c + \psi_8^c + \psi_{12}^c$  and  $\psi_{23} = \psi_4^c + \psi_8^c + \psi_{12}^c + \psi_{14}^c$ ; the index sets are encoded, with bit  $i - 1$  for  $\psi_i^c$ , by the masks  $0x8$ ,  $0x88$ ,  $0x888$  and  $0x2888$  of the file `umasks4.json`. Hence  $\mathfrak{p}$  lies in  $\ker W''$  exactly when  $\text{pat}(\mathfrak{p})$  has even weight on each of these four index sets.

*Proof.* (a) The prime  $\mathfrak{p}$  splits completely in  $E \supseteq F_{0,i}^c$ , so the primes of  $F_{0,i}^c$  above it have residue field  $\mathbb{F}_p$ , and the statement is Lemma 5.5(d) for  $\psi_i^c$  and  $\beta_i^c$ . (b) The supplementary program `d4fields.py` checks that the fifteen census forms have rank 15, so they form a basis of the dual of  $\text{gr}_2 G_B$ , which has dimension 15; hence  $\text{pat}(\mathfrak{p}) = 0$  exactly when  $\overline{\text{Frob}}_{\mathfrak{p}}^{(2)} = 0$ . (c) is linearity. (d) Some  $\text{pat}(\mathfrak{p})_i$  is 1, and Lemma 5.5(c) applies to  $\psi_i^c$  by (a). (e) We have  $o_4 = 17$ ,  $o_8 = 7$ ,  $o_{12} = 20$  and  $o_{14} = 24$ , and the relations of Table 7 give  $\psi_{19} = \psi_{17} + \psi_7$ ,  $\psi_{10} = \psi_{19} + \psi_{20}$  and  $\psi_{23} = \psi_{10} + \psi_{24}$ . The last statement follows from (c), since  $\psi_{10}, \psi_{23}, \psi_{19}, \psi_{17}$  span  $W''$ .  $\square$

**Proposition 5.12** (The census). *The primes of  $B$  of degree one with Frobenius vector 0 and norm at most  $4 \cdot 10^{13}$ , sorted by whether they lie in  $\ker W''$  (Definition 5.7) and are detected (Definition 5.9), are as follows:*

| range of norms                                 | vector 0   | in $\ker W''$ | in $\ker W''$ , detected |
|------------------------------------------------|------------|---------------|--------------------------|
| $65809 \leq N\mathfrak{p} \leq 1.2 \cdot 10^7$ | 2924       | 136           | 136                      |
| $(1.2 \cdot 10^7, 10^{13}]$                    | 1351669408 | 84431399      | 84395189                 |
| $(10^{13}, 4 \cdot 10^{13}]$                   | 3807510358 | 237942878     | 237834284                |

*The smallest norm of a prime of degree one with vector 0 is 65809. The undetected primes are those in  $\ker W''$  that are not detected; all other primes of the table are detected or lie outside  $\ker W''$ . The norms of the detected primes in  $\ker W''$  are recorded exactly for norms at most  $1.2 \cdot 10^7$ , and above that in the geometric bins  $[X(1 + 2^{-16})^j, X(1 + 2^{-16})^{j+1})$ ,  $X = 1.2 \cdot 10^7$  or  $10^{13}$ , as counts per bin (files `census/w4_1e13.binsBW4` and `w4_4e13.binsBW4`).*

*Proof (computer-assisted).* The census runs over the primes  $\mathfrak{p} = (p, \sqrt{241} - r)$  of degree one,  $r^2 \equiv 241 \pmod{p}$ , and tests vector 0 by Lemma 5.10. Square roots modulo  $p$  of the images of the Kummer

generators  $\alpha_0, \dots, \alpha_7$  under  $\sqrt{241} \mapsto r$  give an embedding of each  $F_{0,i}^c$  into  $\mathbb{F}_p$ ; each square root is checked by squaring, and  $\beta_i^c$  is evaluated from its coordinates, so that  $\text{pat}(\mathbf{p})$  is computed with Legendre symbols modulo  $p$  (Lemma 5.11(a)). By Lemma 5.6,  $\beta_i^c$  is a unit at every prime above  $p \geq 7$ , so no Legendre symbol is 0; every run reports this. Membership in  $\ker W''$  is decided by Lemma 5.11(e). For norms at most  $1.2 \cdot 10^7$ , the supplementary program `dihedral_ceiling3.py` classifies the primes in Python with the functions of `rootcheck.py`. Above  $1.2 \cdot 10^7$ , the C program `census_kv4.c` produced the bins; it computes, eight primes at a time in Montgomery arithmetic with the AVX-512 IFMA instructions, the vector-0 test and the Legendre symbols of the  $\beta_i^c$ : first for the four census fields whose bits determine  $\psi_{10}$ ,  $\psi_{23}$ ,  $\psi_{19}$  and  $\psi_{17}$ , and then, for the primes on which  $\psi_{10}$  and  $\psi_{23}$  vanish, for the other census fields until one detects. In the bins a norm may be assigned to a neighboring bin by floating-point rounding; the bound of Lemma 7.3 allows one bin of slack on each side. The program and its data were checked as follows; the earlier programs named here are those of the intermediate certificates.

- (1) On the vector-0 primes of norm  $6 \cdot 10^4$  to  $1.2 \cdot 10^7$ , all C programs reproduce the Python classification prime by prime and field by field, and `census_kv4.c`'s bins for  $\ker W$ ,  $\ker W'$  and  $\ker W''$  (Definition 5.7) equal an independent classification by `rootcheck.py`.
- (2) Its bins for  $\ker W$  on  $(1.2 \cdot 10^7, 10^{13}]$  and  $(10^{13}, 4 \cdot 10^{13}]$  are byte-identical to those of the earlier programs `census_d3k.c` and `census_kw.c`, which use scalar arithmetic and a different structure. On sample ranges near  $10^{13}$  and  $5 \cdot 10^{13}$ , `census_kv4.c` and `census_kv.c` agree in both their checking and their fast modes. In the fast mode about one vector-0 prime in sixteen, and in the checking mode every one, is also recomputed by the scalar code, and the outcomes must agree; all sixteen square roots of the Kummer elements are checked by squaring, which re-proves vector 0.
- (3) Independent reviews recounted bins chosen at random with their own programs and found exact agreement, and a second implementation in PARI/GP matched patterns, bins and undetected primes on eight ranges up to  $10^{12}$ .

The replay program reruns (1) and the comparisons of (2) on sample ranges, and checks the stored bins by their SHA-256 hashes.  $\square$

**5.5. The field  $E_{W''}$  and its  $L$ -functions.** This subsection shows that the field  $E_{W''}$  of Definition 5.7 is Galois over  $B$ , of degree 8192 over  $\mathbb{Q}$ , and contained in every  $K \in \mathcal{K}$ ; it factors  $\zeta_{E_{W''}}$  into  $\zeta_E$  and 576  $L$ -functions (Lemma 5.13), identifies these as Hecke  $L$ -functions of quadratic characters with known conductors and gamma factors (Lemmas 5.16 and 5.17), whose values Section 6 encloses, and computes residue degrees in  $E_{W''}/B$  (Lemma 5.18).

**Lemma 5.13.** (a)  *$E_{W''}$  is Galois over  $B$  and contained in every  $K \in \mathcal{K}$ . It contains  $E$  and the seven dihedral fields  $M_o$  of Definition 5.7. Its group  $G_{W''} = \text{Gal}(E_{W''}/B)$  is a central extension of  $\text{Gal}(E/B) = \mathbb{F}_2^8$  by  $Z_{W''} = D_2 G_B / N_{W''} \cong \mathbb{F}_2^4$ , and  $[E_{W''} : \mathbb{Q}] = 8192$ .*

- (b) *For  $\omega \in W'' \setminus \{0\}$ , regarded as a character of  $Z_{W''} = \text{gr}_2 G_B / W''^\perp$ , let  $r(\omega)$  be the rank of its polar form  $\text{pol}_\omega$ . The irreducible complex representations of  $G_{W''}$  with central character  $\omega$  have dimension  $2^{r(\omega)/2}$ , and there are  $256/2^{r(\omega)}$  of them. Those with trivial central character are the 256 characters  $\chi_w$ .*
- (c) *For  $\omega = \psi_o$  of dihedral type, they are the 64 representations  $\rho_o \otimes \chi_w$ , where  $\rho_o$  is the two-dimensional irreducible representation of  $\text{Gal}(M_o/B) \cong \text{Dih}_4$ , inflated to  $G_{W''}$ , and  $w$  runs over a complement of the span of  $r_{1,o}, r_{2,o}$ .*
- (d) *For  $\omega = \psi_a + \psi_b$  as in Lemma 5.8, they are the 16 representations  $\rho_a \otimes \rho_b \otimes \chi_w$ , with  $w$  over a complement of the span of  $r_{1,a}, r_{2,a}, r_{1,b}, r_{2,b}$ .*
- (e) *With  $L(s, \pi)$  the Artin  $L$ -function over  $B$ ,*

$$\zeta_{E_{W''}}(s) = \zeta_E(s) \prod_o \prod_w L(s, \rho_o \otimes \chi_w)^2 \prod_{(a,b)} \prod_w L(s, \rho_a \otimes \rho_b \otimes \chi_w)^4,$$

the products over the seven forms and the eight pairs, and over the complements of (c) and (d). Hence, for real  $s > 1$ ,

$$(5.14) \quad Y_{W''}(s) := \frac{\log \zeta_{E_{W''}}(s)}{8192} = \frac{Y_E(s)}{16} + \frac{1}{4096} \sum_{o,w} \log L(s, \rho_o \otimes \chi_w) + \frac{1}{2048} \sum_{(a,b),w} \log L(s, \rho_a \otimes \rho_b \otimes \chi_w),$$

where  $Y_E(s) = \log \zeta_E(s)/512$  as in Proposition 4.31.

*Proof.* (a) Since  $[G_B, D_2G_B] \subseteq D_3G_B \subseteq N_{W''}$ , every subgroup between  $D_3G_B$  and  $D_2G_B$  is normal in  $G_B$ , and  $D_2G_B/N_{W''}$  is central in  $G_B/N_{W''}$ ; so  $E_{W''}$  is Galois over  $B$  and  $G_{W''}$  is a central extension of  $G_B/D_2G_B = \text{Gal}(E/B)$  by  $Z_{W''}$ . The latter is  $\text{gr}_2 G_B/W''^\perp$ , which is dual to  $W''$ , of dimension four. Hence  $[E_{W''} : B] = 2^{12}$  and  $[E_{W''} : \mathbb{Q}] = 8192$ . Since  $N_{W''} \supseteq D_3G_B \supseteq D_4G_B$ ,  $E_{W''}$  lies in every  $K \in \mathcal{K}$ . By Lemma 5.5(b), the kernel of  $\phi_{M_o}$  contains the elements of  $D_2G_B$  whose class is killed by  $\psi_o$ , hence contains  $N_{W''}$ , so  $M_o \subseteq E_{W''}$ .

(b) The commutator of elements of  $G_{W''}$  with elementary images  $v, w$  is the class of  $[v, w]$  in  $Z_{W''}$ , and the square of an element with image  $v$  is the class of  $v^{[2]}$ . Let  $\omega \neq 0$ , and let  $H = G_{W''}/\ker \omega$ . The representations with central character  $\omega$  factor through  $H$ , a central extension of  $\mathbb{F}_2^8$  by  $\langle z \rangle \cong C_2$  in which elements with images  $v, w$  have commutator  $z^{\text{pol}_\omega(v,w)}$ . The center  $C_H$  of  $H$  is the preimage of the radical of  $\text{pol}_\omega$ , of index  $2^{r(\omega)}$  in  $H$ . Let  $\pi$  be irreducible with  $\pi(z) = -1$ . If  $g \notin C_H$ , there is  $h$  with  $h^{-1}gh = gz$ , so  $\text{tr } \pi(g) = -\text{tr } \pi(g) = 0$ ; on  $C_H$ ,  $\pi$  acts by scalars, so  $|\text{tr } \pi| = \dim \pi$  there. The orthogonality relation  $\sum_{g \in H} |\text{tr } \pi(g)|^2 = |H|$  gives  $(\dim \pi)^2 = [H : C_H] = 2^{r(\omega)}$ . The irreducible representations of  $H$  with  $z \mapsto -1$  have  $\sum (\dim \pi)^2 = |H| - |H/\langle z \rangle| = 2^8$ , so there are  $2^8/2^{r(\omega)}$  of them. Those with trivial central character are the representations of  $\text{Gal}(E/B) = \mathbb{F}_2^8$ .

(c) The representation  $\rho_o \otimes \chi_w$  has central character  $\psi_o$ , by Lemma 5.5(b), and dimension  $2 = 2^{r(\psi_o)/2}$ , so it is irreducible. Its character vanishes outside the preimage of the radical  $\ker \phi_o$  of  $\text{pol}_{\psi_o}$  (Lemma 5.3), and is  $\pm 2\chi_w$  on it. Hence  $\rho_o \otimes \chi_w \cong \rho_o \otimes \chi_{w'}$  exactly when  $\chi_{w-w'}$  is trivial on  $\ker \phi_o$ , that is, when  $w - w'$  lies in the span of  $r_{1,o}, r_{2,o}$ . This gives  $256/4 = 64$  classes, all of them by (b).

(d) Likewise  $\rho_a \otimes \rho_b \otimes \chi_w$  has central character  $\psi_a + \psi_b$  and dimension  $4 = 2^{r(\psi_a + \psi_b)/2}$ , so it is irreducible. The radical of the polar form, of codimension four, contains  $\ker \phi_a \cap \ker \phi_b$ , which has codimension four by Lemma 5.8, so they are equal, and the twists are distinct modulo the span of the four vectors.

(e) The Artin formalism gives  $\zeta_{E_{W''}} = \prod_\pi L(s, \pi)^{\dim \pi}$  over the irreducible representations of  $G_{W''}$ , and  $\prod_w L(s, \chi_w) = \zeta_E(s)$  (Proposition 3.8). By Lemma 5.8 every nonzero  $\omega \in W''$  is of one of the two kinds in (c) and (d), which gives the product; the count  $256 + 7 \cdot 64 \cdot 4 + 8 \cdot 16 \cdot 16 = 4096 = |G_{W''}|$  is a check. Taking logarithms and dividing by  $8192 = 16 \cdot 512$  gives (5.14).  $\square$

*Remark 5.15.* The proof of Lemma 5.13 uses only that every nonzero element of  $W''$  is a form of dihedral type or a sum  $\psi_a + \psi_b$  as in Lemma 5.8. It therefore applies to every subspace  $U \subseteq W''$ , for instance to  $W$  and  $W'$ , with  $E_U$  the fixed field of the preimage in  $D_2G_B$  of the common kernel of the forms in  $U$ : the field  $E_U$  is Galois over  $B$ , contained in every  $K \in \mathcal{K}$ , of degree  $512 \cdot 2^{\dim U}$  over  $\mathbb{Q}$ , and  $\zeta_{E_U}$  is  $\zeta_E$  times the squares of the 64 functions  $L(s, \rho_o \otimes \chi_w)$  of each form  $\psi_o \in U$  and the fourth powers of the 16 functions  $L(s, \rho_a \otimes \rho_b \otimes \chi_w)$  of each sum  $\psi_a + \psi_b \in U$ .

**Lemma 5.16.** *Let  $\rho_o$  and  $\chi_w$  be as in Lemma 5.13.*

- (a) *Let  $\psi_o$  be a form of Table 7. Let  $\tau_o \in \text{Gal}(F_{0,o}/B)$  be one of the two nonzero elements other than  $\mathbf{r}_o$ , and let  $B_{c_o} = B(\sqrt{c_o})$  be its fixed field in  $F_{0,o}$ ; Table 7 records the element  $c_o$  used. Let  $u_o \in F_{0,o}^\times$  satisfy  $\tau_o(\beta_o)/\beta_o = u_o^2$  and  $u_o\tau_o(u_o) = 1$  (Lemma 5.5, (D1) and (D2)), with  $u_o \neq -1$  (replace  $u_o$  by  $-u_o$  if necessary). Then  $\gamma_o = (1 + u_o)^2\beta_o$  lies in  $B_{c_o}$ , and for every*

$w$ ,

$$L(s, \rho_o \otimes \chi_w) = \frac{\zeta_{M_{o,w}}(s)}{\zeta_{B_{c_o}}(s)}, \quad M_{o,w} = B_{c_o}(\sqrt{\gamma_o \alpha_w}).$$

(b) For a pair  $(a, b)$  of Lemma 5.8, put  $B_{ab} = B(\sqrt{c_a}, \sqrt{c_b})$ . Then for every  $w$

$$L(s, \rho_a \otimes \rho_b \otimes \chi_w) = \frac{\zeta_{B_{ab,w}}(s)}{\zeta_{B_{ab}}(s)}, \quad B_{ab,w} = B_{ab}(\sqrt{\gamma_a \gamma_b \alpha_w}).$$

(c) Each of these quotients is the Hecke  $L$ -function  $L(s)$  of a nontrivial quadratic character of  $A = B_{c_o}$ , respectively  $A = B_{ab}$ , and it is entire. Let  $A'$  be the quadratic extension  $M_{o,w}$ , respectively  $B_{ab,w}$ , of  $A$ , and  $Q = |\Delta_{A'}|/|\Delta_A|$ . Then the function  $\Lambda(s) = Q^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1(A')-r_1(A)} \Gamma_{\mathbb{C}}(s)^{r_2(A')-r_2(A)} L(s)$  satisfies  $\Lambda(1-s) = \Lambda(s)$ , where  $(r_1(\cdot), r_2(\cdot))$  is the signature.

*Proof.* (a) Fix  $o$  and write  $F_0, \beta, \tau, u, \gamma$  and  $c$  for  $F_{0,o}, \beta_o, \tau_o, u_o, \gamma_o$  and  $c_o$ . Let  $\tilde{\tau} \in \text{Gal}(M_o/B)$  lift  $\tau$  with  $\tilde{\tau}(\sqrt{\beta}) = u\sqrt{\beta}$ . Then  $\tilde{\tau}^2(\sqrt{\beta}) = \tau(u)u\sqrt{\beta} = \sqrt{\beta}$ , so  $\tilde{\tau}$  has order two, and  $\tilde{\tau}((1+u)\sqrt{\beta}) = (1+\tau(u))u\sqrt{\beta} = (1+u)\sqrt{\beta}$ . So the nonzero element  $(1+u)\sqrt{\beta}$  is fixed by  $\tilde{\tau}$ ; its square  $\gamma$  lies in  $F_0$  and is fixed by  $\tau$ , so it lies in  $B_c$ ; and  $\sqrt{\gamma} \notin B_c$ , since  $\sqrt{\beta} \notin F_0$ . The fixed field of  $\langle \tilde{\tau} \rangle$  in  $M_o$  is therefore  $B_c(\sqrt{\gamma})$ . Let  $H_o \subset G_{W''}$  be the fixed group of  $B_c$ , of index two, and let  $\xi_o$  be the quadratic character of  $H_o$  that cuts out  $B_c(\sqrt{\gamma})$ . The image of  $H_o$  in  $\text{Gal}(M_o/B) \cong \text{Dih}_4$  is  $\langle \tilde{\tau}, z \rangle$ , and  $\xi_o$  factors through it, trivial on  $\tilde{\tau}$  and nontrivial on  $z$ . Hence  $\text{Ind}_{H_o}^{G_{W''}} \xi_o$  is inflated from the representation of  $\text{Dih}_4$  induced from this character of  $\langle \tilde{\tau}, z \rangle$ , which has dimension two and is nontrivial on the center, so it is the two-dimensional irreducible representation:  $\text{Ind}_{H_o} \xi_o = \rho_o$ . Twisting,  $\rho_o \otimes \chi_w = \text{Ind}_{H_o}(\xi_o \cdot \chi_w|_{H_o})$ , and  $\xi_o \cdot \chi_w|_{H_o}$  is the quadratic character of  $H_o$  that cuts out  $M_{o,w}$ . It is nontrivial, since  $\rho_o \otimes \chi_w$  is irreducible. By the invariance of Artin  $L$ -functions under induction,  $L(s, \rho_o \otimes \chi_w) = L(s, \xi_o \chi_w|_{H_o})$ , which is  $\zeta_{M_{o,w}}(s)/\zeta_{B_c}(s)$ .

(b) Write  $\rho_a = \text{Ind}_{H_a} \xi_a$  and  $\rho_b = \text{Ind}_{H_b} \xi_b$  as in (a). Since  $c_a/c_b$  is not a square,  $H_a \neq H_b$ , so  $H_a H_b = G_{W''}$ , and Mackey's formula [34, Section 7.3] gives  $\text{Res}_{H_a} \text{Ind}_{H_b} \xi_b = \text{Ind}_{H_a \cap H_b}^{H_a} \xi_b$ . Hence

$$\rho_a \otimes \rho_b \otimes \chi_w = \text{Ind}_{H_a}(\xi_a \otimes \text{Res}_{H_a}(\rho_b \otimes \chi_w)) = \text{Ind}_{H_a \cap H_b}(\xi_a \xi_b \chi_w),$$

and  $H_a \cap H_b$  is the fixed group of  $B_{ab}$ ; the character  $\xi_a \xi_b \chi_w$  cuts out  $B_{ab,w}$ , and it is nontrivial since the representation is irreducible.

(c) A nontrivial Hecke character has an entire  $L$ -function [11, 38]. The completed Dedekind zeta functions satisfy  $\Lambda_A(1-s) = \Lambda_A(s)$  (Section 3), and the quotient of those of  $A'$  and  $A$  is the stated  $\Lambda$ .  $\square$

**Lemma 5.17.** *The conductors and gamma factors of the 576 functions of Lemma 5.16 are as follows. For  $o = 10, 23, 24, 19, 17, 7$ , all 64 twists have  $r_1(M_{o,w}) = r_1(B_{c_o})$ , so their gamma factor is  $\Gamma_{\mathbb{C}}(s)^2$ ; for  $o = 20$ ,  $B_{c_o}$  is totally real and  $r_1(M_{o,w}) = 6$  for 32 twists and 2 for the other 32, so the gamma factor is  $\Gamma_{\mathbb{R}}(s)^3 \Gamma_{\mathbb{R}}(s+1)$  or  $\Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s+1)^3$ . For the eight pairs,  $B_{ab}$  and all  $B_{ab,w}$  are totally complex, so the gamma factor is  $\Gamma_{\mathbb{C}}(s)^4$ . The conductors lie in the following ranges:*

| functions                | degree over $\mathbb{Q}$ | conductors                                                                 |
|--------------------------|--------------------------|----------------------------------------------------------------------------|
| $o = 10$                 | 4                        | $4.18 \cdot 10^8$ to $2.68 \cdot 10^{10}$                                  |
| $o = 23, 24$             | 4                        | $1.67 \cdot 10^9$ to $2.68 \cdot 10^{10}$                                  |
| $o = 19, 7$              | 4                        | $1.67 \cdot 10^8$ to $2.68 \cdot 10^{11}$                                  |
| $o = 20$                 | 4                        | $3.35 \cdot 10^8$ to $1.34 \cdot 10^{11}$                                  |
| $o = 17$                 | 4                        | $6.69 \cdot 10^8$ to $2.68 \cdot 10^{11}$                                  |
| pairs (19, 23), (19, 24) | 8                        | $6.995 \cdot 10^{17}$ and $1.791 \cdot 10^{20}$                            |
| the other six pairs      | 8                        | $2.798 \cdot 10^{18}$ or $4.477 \cdot 10^{19}$ , and $7.163 \cdot 10^{20}$ |

*Proof (computer-assisted).* The twists of  $\psi_{10}, \psi_{23}, \psi_{24}$  are treated by the supplementary program `export.gp`, those of the other four forms by the program `deg8/exportg.gp`, and the pairs by `deg8/export8.gp`. These programs construct  $B_{c_o}, \gamma_o, M_{o,w}, B_{ab}$  and  $B_{ab,w}$  in PARI/GP from the data of Lemmas 5.5 and 5.6, and compute the signatures, the discriminants and the Euler factors at small primes from the maximal orders. For the twists of the seven forms the maximal orders come from PARI's `nfinit`. For the pairs, whose fields have degree 16, the program computes orders maximal at 2, 3, 5, 241 and asserts that their discriminants are, up to sign, products of powers of these primes, so that the orders are maximal; it also asserts the signatures and that each local quotient of Euler factors is a polynomial of degree at most 8 in  $p^{-s}$ . Wrong conductors or gamma factors would also be detected by the checks of Subsection 6.3.  $\square$

**Lemma 5.18.** *Let  $\mathfrak{p} \notin S$  be a prime of  $B$  with Frobenius vector  $v$ , and let  $f_{W''}(\mathfrak{p})$  be its residue degree in the extension  $E_{W''}/B$  of Lemma 5.13, with the maps  $\phi_o$  of Definition 5.7.*

- (a) *If  $v \neq 0$ , then  $f_{W''}(\mathfrak{p}) = 4$  if  $\phi_o(v) = \mathbf{r}_o$  for one of the seven forms  $\psi_o$  of Table 7, and  $f_{W''}(\mathfrak{p}) = 2$  otherwise.*
- (b) *If  $v = 0$ , then  $f_{W''}(\mathfrak{p}) = 2$  if  $\mathfrak{p}$  does not lie in  $\ker W''$ , and  $f_{W''}(\mathfrak{p}) = 1$  if it does.*

*Proof.* Let  $g \in G_{W''}$  be a Frobenius of a prime above  $\mathfrak{p}$ ; its order is  $f_{W''}(\mathfrak{p})$ . (a) If  $v \neq 0$ , then  $g \notin Z_{W''}$  and  $g^2 \in Z_{W''}$ , and  $\omega(g^2) = q_\omega(v)$  for  $\omega \in W''$ . So  $g^2 = 1$  exactly when  $q_\omega(v) = 0$  for all  $\omega \in W''$ , that is, for the seven dihedral forms, which span  $W''$ ; and  $q_{\psi_o}(v) = 1$  exactly when  $\phi_o(v) = \mathbf{r}_o$ . (b) If  $v = 0$ , then  $g \in Z_{W''}$ , and  $g \neq 1$  exactly when  $\omega(\overline{\text{Frob}}_{\mathfrak{p}}^{(2)}) \neq 0$  for some  $\omega \in W''$ .  $\square$

**5.6. Floors.** This subsection defines the floors used in the proof of Theorem 4.2 (Definition 5.20), shows that they form a system of floors (Lemma 5.21), and expresses their floor sum through  $Y_{W''}$  and explicit corrections (Lemmas 5.22 and 5.23); Section 7 evaluates the result. For primes of degree one with vector 0, Lemma 5.18(b) is read from the census (Lemma 5.11(e)); the primes of degree two with vector 0 and small norm are treated by the next lemma.

**Lemma 5.19.** *There are exactly thirteen primes of  $B$  of degree two, that is,  $p\mathcal{O}_B$  with  $p$  inert in  $B$ , with Frobenius vector 0 and norm  $p^2 \leq 1.2 \cdot 10^7$ , namely  $p = 409, 769, 1129, 1249, 1489, 1609, 1801, 2281, 2521, 2689, 3001, 3049$  and  $3361$ . None of them lies in  $\ker W''$ , so  $f_{W''}(p\mathcal{O}_B) = 2$  for each of them.*

*Proof (computer-assisted).* For such a prime  $\mathfrak{p} = p\mathcal{O}_B$ , the Frobenius in  $\text{Gal}(M_o/B)$  is central by Lemma 5.5(b), so it is 1 or  $z$ , and accordingly the Euler factor at  $p$  of  $L(s, \rho_o \otimes \chi_0)$  is  $(1 - p^{-2s})^{-2}$  or  $(1 + p^{-2s})^{-2}$ ; by Lemma 5.5(b) it is  $z$  exactly when  $\psi_o(\overline{\text{Frob}}_{\mathfrak{p}}^{(2)}) = 1$ . The supplementary program `inertv0.4.py` lists the inert primes of vector 0 with  $p^2 \leq 1.2 \cdot 10^7$ , computes these Euler factors with PARI from the prime decompositions of  $p$  in  $M_{o,0}$  and  $B_{c_o}$  (Lemma 5.16(a)), and finds that none of the thirteen primes lies in  $\ker W''$ . Lemma 5.18(b) then gives  $f_{W''}(p\mathcal{O}_B) = 2$ .  $\square$

**Definition 5.20.** Let  $\mathcal{P}_2$  be the set of the primes of  $B$  of degree one with vector 0 and norm at most  $4 \cdot 10^{13}$  that lie in  $\ker W''$  and are detected; they are counted in the last column of Proposition 5.12. For a free prime  $\mathfrak{p}$  of  $B$  put  $f_{\mathfrak{p}}^0 = 4$  if  $\mathfrak{p} \in \mathcal{P}_4$  (Definition 4.32),  $f_{\mathfrak{p}}^0 = 2$  if  $\mathfrak{p} \in \mathcal{P}_2$ , and  $f_{\mathfrak{p}}^0 = f_{W''}(\mathfrak{p})$  otherwise.

**Lemma 5.21.** *The numbers  $f_{\mathfrak{p}}^0$  form a system of floors (Definition 4.18), and  $f_{\mathfrak{p}}^0 \geq f_{W''}(\mathfrak{p})$  for every free  $\mathfrak{p}$ .*

*Proof.* (Fl1) The residue degree  $f_{W''}(\mathfrak{p})$  divides  $f_K(\mathfrak{p})$ , since  $E_{W''} \subseteq K$  (Lemmas 5.13(a) and 4.10). For  $\mathfrak{p} \in \mathcal{P}_4$ , 4 divides  $f_K(\mathfrak{p})$  by Lemma 4.33; for  $\mathfrak{p} \in \mathcal{P}_2$ , 2 divides  $f_K(\mathfrak{p})$  by Lemma 5.11(d). Since  $f_{W''}(\mathfrak{p}) \leq 4$  always and  $f_{W''}(\mathfrak{p}) = 1$  on  $\mathcal{P}_2$ , the floors are at least  $f_{W''}(\mathfrak{p})$ . (Fl2) For  $N_{\mathfrak{p}} > 1.2 \cdot 10^7 > 41^4$  it is clear. For  $N_{\mathfrak{p}} \leq 1.2 \cdot 10^7$  the supplementary program `dihedral_ceiling3.py`

computes  $f_p^0$  by Lemma 5.18, using Proposition 5.12 for the primes of degree one with vector 0 and Lemma 5.19 for those of degree two, and checks  $Np^{f_p^0} \geq 41^4$ ; in particular every free prime of norm less than 1681 has floor 4.  $\square$

**Lemma 5.22.** *For real  $\sigma > 1$ , the floor sum of the floors of Definition 5.20 is*

$$Y_{\text{fl}}(\sigma) = Y_{W''}(\sigma) - \Delta_{\text{sel}}(\sigma) - Z_{\text{sel}}(\sigma) - \Delta_4(\sigma) - \sum_{\mathfrak{p} \in \mathcal{P}_2} T_\sigma(N\mathfrak{p}),$$

where  $T_\sigma(N) = g_\sigma(N)/2 - g_\sigma(N^2)/4$ ,

$$\Delta_4(\sigma) = \sum \left( \frac{g_\sigma(N\mathfrak{p}^2)}{4} - \frac{g_\sigma(N\mathfrak{p}^4)}{8} \right),$$

the sum over the  $\mathfrak{p} \in \mathcal{P}_4$  with  $f_{W''}(\mathfrak{p}) = 2$ , and  $\Delta_{\text{sel}}(\sigma)$  is the sum over the selected primes  $\mathfrak{p}$  of the difference between the term of  $\mathfrak{p}$  in (4.11) for  $M = E_{W''}$  and for  $M = K$ , with the types of Theorem 2.46.

*Proof.* By (4.11) for  $M = E_{W''}$ ,  $Y_{W''}(\sigma)$  is the sum over all primes of  $B$  of the terms  $g_\sigma(N\mathfrak{p}^f)/(2ef)$  with the type  $(e, f)$  of  $\mathfrak{p}$  in  $E_{W''}/B$ . For the selected primes, the term for  $E_{W''}$  is the term for  $K$  plus a summand of  $\Delta_{\text{sel}}(\sigma)$ , and the terms for  $K$  add up to  $Z_{\text{sel}}(\sigma)$  by Lemma 4.17. A free prime has  $e = 1$  in  $E_{W''}$ , and its floor differs from  $f_{W''}(\mathfrak{p})$  only on  $\mathcal{P}_4$ , from 2 to 4, and on  $\mathcal{P}_2$ , from 1 to 2; these changes lower its term by the summands of  $\Delta_4(\sigma)$  and by  $T_\sigma(N\mathfrak{p})$ . The sets  $\mathcal{P}_4$  and  $\mathcal{P}_2$  are disjoint, since the primes of  $\mathcal{P}_4$  have nonzero vectors.  $\square$

**Lemma 5.23.** *For real  $\sigma > 1$ ,*

$$\Delta_{\text{sel}}(\sigma) = Y_{W''}^{(2)}(\sigma) - \frac{g_\sigma(16)}{32} + \sum_{k=1}^3 \left( \frac{g_\sigma(N\mathfrak{t}_k^{f_k})}{2f_k} - \frac{g_\sigma(N\mathfrak{t}_k^4)}{8} \right),$$

where  $f_k = f_{W''}(\mathfrak{t}_k) \in \{2, 4\}$  is given by Lemma 5.18(a), and  $Y_{W''}^{(2)}(\sigma)$  is the right side of (5.14) at  $s = \sigma$  with  $\zeta_E$  and each  $L$ -function replaced by the product of its Euler factors at the primes of  $B$  above 2. The selected primes above 3 and 5 contribute 0 to  $\Delta_{\text{sel}}$ .

*Proof.* By (4.11) for  $M = E_{W''}$ , restricted to the primes above 2, the terms of  $\mathfrak{p}_1, \mathfrak{p}_2$  for  $M = E_{W''}$  add up to the logarithm of the product of the Euler factors of  $\zeta_{E_{W''}}$  at the primes above 2, divided by 8192; by the factorization of Lemma 5.13(e), which holds Euler factor by Euler factor, this is  $Y_{W''}^{(2)}(\sigma)$ . Their terms for  $K$ , of type  $(8, 4)$  and norm 2, are  $g_\sigma(16)/64$  each. Above 3 and 5 the types in  $E$  (Corollary 3.7) and in  $K$  are both  $(2, 2)$ , so the type in  $E_{W''}$  is  $(2, 2)$  too, since  $E \subseteq E_{W''} \subseteq K$  and ramification indices and residue degrees divide in towers; these primes contribute nothing. The capped primes have nonzero Frobenius vectors (Table 5), so their residue degree  $f_k$  in  $E_{W''}$  is 2 or 4 by Lemma 5.18(a), with  $e = 1$ ; their type in  $K$  is  $(1, 4)$ .  $\square$

The supplementary program `dihedral_ceiling3.py` evaluates  $\Delta_{\text{sel}}$  by Lemma 5.23, reading the Euler factors at 2 of all the  $L$ -functions in (5.14); it also checks that the Euler factors at 3 and 5 give the types  $(2, 2)$ . For orientation, at  $\sigma = 1001/1000$  it gives  $Y_E = 0.0853580483$ ,  $Y_{W''} = 0.050492599$  (radius  $4 \cdot 10^{-12}$ ),  $\Delta_{\text{sel}} = 0.0079701070$  and  $\Delta_4 = 0.0005116777$ .

## 6. VALUES OF THE $L$ -FUNCTIONS OF $E_{W''}$

By (5.14),  $Y_{W''}(\sigma)$  is determined by  $Y_E(\sigma)$  and by the values at  $\sigma$  of 576 further  $L$ -functions: 448 of degree 4 over  $\mathbb{Q}$ , the twists  $L(s, \rho_a \otimes \chi_w)$  of the seven dihedral representations, and 128 of degree 8, the functions  $L(s, \rho_a \otimes \rho_b \otimes \chi_w)$ . They are needed at the 21 abscissae of Table 9, all in  $(1, 101/100)$ ; the values were computed at 36 abscissae, from which the linear programme of Section 7 chose these 21. Proposition 4.31 gives  $Y_E(\sigma)$ . This section encloses the 576 values (Proposition 6.5); Lemma 7.3 uses them.

All 576 functions are evaluated with the approximate functional equation and the kernels of Subsection 6.1, which cover the four gamma factors of Lemma 5.17. The 192 twists of the forms  $\psi_{10}, \psi_{23}, \psi_{24}$  were also evaluated by a second, independent implementation for the gamma factor  $\Gamma_{\mathbb{C}}(s)^2$ , the program `dafe.py` with the kernels of the data archive in `papers/0.0418235/certificates` of [23]; the two agree (Subsection 6.3, item (3)), and the proof uses only the first.

**6.1. An approximate functional equation for products of gamma functions.** This subsection proves an approximate functional equation (Lemma 6.1) and the properties of its kernels (Lemma 6.2) for the four gamma factors of Lemma 5.17; Subsection 6.2 uses them. In this section  $d \in \{1, 2\}$  is a parameter of the gamma factor, not the degree  $[F : \mathbb{Q}]$  of Section 4.

Let  $d \in \{1, 2\}$ , let  $m \geq 1$  and  $\mu_1, \dots, \mu_m \in \{0, \frac{1}{2}\}$  with at least one  $\mu_j = 0$ , and let  $C_G, \kappa_G > 0$ . The gamma factors of Lemma 5.17 have the form  $G(s) = C_G \kappa_G^{-s} \prod_{j=1}^m \Gamma(s/d + \mu_j)$ :

$$\Gamma_{\mathbb{C}}(s)^4 = 16(2\pi)^{-4s} \Gamma(s)^4, \quad \Gamma_{\mathbb{C}}(s)^2 = 4(2\pi)^{-2s} \Gamma(s)^2,$$

$$\Gamma_{\mathbb{R}}(s)^3 \Gamma_{\mathbb{R}}(s+1) = \pi^{-1/2} \pi^{-2s} \Gamma(\frac{s}{2})^3 \Gamma(\frac{s}{2} + \frac{1}{2}), \quad \Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s+1)^3 = \pi^{-3/2} \pi^{-2s} \Gamma(\frac{s}{2}) \Gamma(\frac{s}{2} + \frac{1}{2})^3,$$

with  $(d, \kappa_G) = (1, (2\pi)^4), (1, (2\pi)^2), (2, \pi^2)$  and  $(2, \pi^2)$ . Define the kernels

$$h(x) = \frac{1}{2\pi i} \int_{(\eta)} \prod_j \Gamma(u + \mu_j) x^{-u} du \quad (x > 0, \eta > 0),$$

$$\mathcal{I}_b(x) = \int_1^\infty r^{b-1} h(xr) dr \quad (b \in \mathbb{R}).$$

Thus  $h$  is the inverse Mellin transform of  $\prod_j \Gamma(u + \mu_j)$ , the multiplicative convolution of the functions  $x^{\mu_j} e^{-x}$ ; it is positive and decays exponentially, so  $\mathcal{I}_b(x)$  converges for every real  $b$ .

**Lemma 6.1.** *Let  $L(s) = \sum_{n \geq 1} a_n n^{-s}$  with real coefficients of polynomial growth, let  $Q > 0$ , and suppose that  $\Lambda(s) = Q^{s/2} G(s) L(s)$  extends to an entire function of finite order with  $\Lambda(1-s) = \Lambda(s)$ . Put  $t = \kappa_G / \sqrt{Q}$  and  $x_n = (tn)^d$ . Then for real  $s > 1$*

$$L(s) = \frac{t^s}{\prod_j \Gamma(s/d + \mu_j)} \sum_{n \geq 1} a_n (\mathcal{I}_{s/d}(x_n) + \mathcal{I}_{(1-s)/d}(x_n)),$$

and the series converges absolutely.

*Proof.* For  $y > 0$  put  $\Phi(y) = \sum_n a_n h(x_n y)$ . Since  $\int_0^\infty h(x) x^{u-1} dx = \prod_j \Gamma(u + \mu_j)$  for  $\operatorname{Re} u > 0$  and  $Q^{s/2} \kappa_G^{-s} n^{-s} = x_n^{-s/d}$ , termwise integration gives, for  $\operatorname{Re}(du) > 1$ ,

$$\int_0^\infty \Phi(y) y^{u-1} dy = \prod_j \Gamma(u + \mu_j) \sum_n a_n x_n^{-u} = \Lambda(du) / C_G.$$

The right side is entire and invariant under  $u \mapsto 1/d - u$ . As in the proof of Lemma 4.21,  $L$  has polynomial growth in vertical strips by the Phragmén–Lindelöf principle, so by Stirling's formula  $\Lambda(du)$  decays exponentially in  $|\operatorname{Im} u|$  on vertical strips. Mellin inversion on a line  $\operatorname{Re} u = c > 1/d$  and a shift to  $\operatorname{Re} u = 1/d - c$ , where no poles occur, give  $\Phi(y) = y^{-1/d} \Phi(1/y)$ . Splitting the Mellin integral at  $y = 1$  and substituting  $y \mapsto 1/y$  below 1,

$$\begin{aligned} \frac{\Lambda(s)}{C_G} &= \int_1^\infty \Phi(y) (y^{s/d-1} + y^{(1-s)/d-1}) dy \\ &= \sum_n a_n (\mathcal{I}_{s/d}(x_n) + \mathcal{I}_{(1-s)/d}(x_n)), \end{aligned}$$

by termwise integration, which the exponential decay of  $h$  justifies. Finally

$$L(s) = \frac{\Lambda(s)}{C_G t^{-s} \prod_j \Gamma(s/d + \mu_j)}.$$

□

**Lemma 6.2.** (a)  $h$  and every  $\mathcal{I}_b$  are completely monotone on  $(0, \infty)$ ; in particular  $|\mathcal{I}_b^{(k)}|$  is nonincreasing for every  $k \geq 0$ .

(b)  $x\mathcal{I}_b'(x) + b\mathcal{I}_b(x) = -h(x)$ .

(c)  $h(x)$ , and  $x^b\mathcal{I}_b(x)$  when no pole of  $\prod_j \Gamma(b + \mu_j + u)$  lies at  $u = 0$ , are given by convergent series of residues at the poles of the gamma factors, at  $u = -n - \mu$  for  $h$  and at  $u = -n - \mu - b$  for  $x^b\mathcal{I}_b$  ( $n \geq 0$ ,  $\mu \in \{\mu_j\}$ ), and  $x^b\mathcal{I}_b(x)$  has the additional term  $\prod_j \Gamma(b + \mu_j)$  from the pole of  $1/u$ . When  $b < 0$  the pole with  $n = 0$ ,  $\mu = 0$  lies at  $u = -b > 0$ , and the line of integration is taken to its right.

(d) For  $\eta > 0$  with  $b + \mu_j + \eta > 0$  for all  $j$ ,  $|\mathcal{I}_b(x)| \leq C_{b,\eta} x^{-b-\eta}$ , where  $C_{b,\eta} = \prod_j \Gamma(b + \mu_j + \eta) \cdot \frac{1}{2\pi} \int_{\mathbb{R}} \prod_j \left(1 + \frac{y^2}{(b + \mu_j + \eta)^2}\right)^{-1/2} \frac{dy}{|\eta + iy|}$ .

*Proof.* (a) If  $\mu_{j_0} = 0$ , then  $h(x) = \int_0^\infty e^{-x/v} \varrho(v) dv/v$ , where  $\varrho \geq 0$  is the convolution of the other factors  $x^{\mu_j} e^{-x}$ ; this is a positive combination of the completely monotone functions  $e^{-x/v}$ . Then  $\mathcal{I}_b(x) = \int_1^\infty r^{b-1} h(xr) dr$  is also one, and the derivatives of a completely monotone function alternate in sign and have nonincreasing absolute values. (b) Substituting  $v = xr$ ,  $\mathcal{I}_b(x) = x^{-b} \int_x^\infty v^{b-1} h(v) dv$ ; now differentiate. (c) The Mellin transform of  $x^b\mathcal{I}_b(x) = \int_x^\infty v^{b-1} h(v) dv$  is  $\prod_j \Gamma(b + \mu_j + u)/u$ ; shift the inversion integral to the left. The residues decay faster than any geometric sequence. (d) Write  $x^b\mathcal{I}_b(x) = \frac{1}{2\pi i} \int_{(\eta)} \prod_j \Gamma(b + \mu_j + u) x^{-u} du/u$  and use  $|\Gamma(a + iy)| \leq \Gamma(a)(1 + y^2/a^2)^{-1/2}$  for  $a > 0$ , which follows from the product formula for  $|\Gamma(a + iy)|^2$ . □

**6.2. The computation.** This subsection describes how the kernels and the coefficients are computed and how their errors are bounded (Lemmas 6.3 and 6.4); the resulting enclosures, Proposition 6.5, are the input of Lemma 7.3. For each  $L$ -function let  $a_n$  be its coefficients and  $N$  the truncation point of the series of Lemma 6.1 (the column “terms” of Table 8).

For each gamma factor, the supplementary program `deg8/gkernel.py` encloses  $\mathcal{I}_{\sigma/d}$  and  $\mathcal{I}_{(1-\sigma)/d}$  in Arb on a grid of cells: the points  $\xi_0 > \xi_1 > \dots$  are  $\xi_0 = 6144$  for  $\Gamma_{\mathbb{C}}(s)^4$ , 512 for  $\Gamma_{\mathbb{C}}(s)^2$  and  $2^{14}$  for the mixed factors, and  $\xi_{i+1} = 31\xi_i/32$  rounded down to 53 significant bits, down to  $2^{-40}$ . At each  $\xi_i$  the Taylor coefficients of order 0 to 20 of  $\mathcal{I}_b$  are computed from the residue series of Lemma 6.2(c), with the working precision raised to absorb the cancellation in these alternating series, whose terms reach about  $\exp(mx^{1/m})$ , and with the truncated tail bounded by Cauchy’s estimate on circles of radius 1/2 or 1/4 around the poles; the recursion of Lemma 6.2(b) gives the higher coefficients from those of  $h$ . The next lemma bounds the error on each cell and beyond the last cell used.

**Lemma 6.3.** Let  $b \in \mathbb{R}$ .

(a) For  $i \geq 0$  and  $x \in [\xi_{i+1}, \xi_i]$ ,

$$\left| \mathcal{I}_b(x) - \sum_{k=0}^{20} \frac{\mathcal{I}_b^{(k)}(\xi_i)}{k!} (x - \xi_i)^k \right| \leq \frac{|\mathcal{I}_b^{(21)}(\xi_{i+1})|}{21!} (\xi_i - \xi_{i+1})^{21}.$$

(b) Let  $\eta$  and  $C_{b,\eta}$  be as in Lemma 6.2(d), let  $0 < s_0 < d(b + \eta)$ , let  $t > 0$  and  $N \geq 1$ , and let  $x_n = (tn)^d$ . Then for real numbers  $a_n$

$$\sum_{n > N} |a_n| |\mathcal{I}_b(x_n)| \leq C_{b,\eta} t^{-d(b+\eta)} N^{s_0 - d(b+\eta)} \sum_{n \geq 1} |a_n| n^{-s_0}.$$

*Proof.* (a) By Taylor's theorem the difference is  $\mathcal{I}_b^{(21)}(\vartheta)(x - \xi_i)^{21}/21!$  for some  $\vartheta \in [x, \xi_i]$ . By Lemma 6.2(a),  $|\mathcal{I}_b^{(21)}(\vartheta)| \leq |\mathcal{I}_b^{(21)}(\xi_{i+1})|$ , since  $\vartheta \geq \xi_{i+1}$ ; and  $|x - \xi_i| \leq \xi_i - \xi_{i+1}$ . (b) This is Rankin's trick. By Lemma 6.2(d),  $|\mathcal{I}_b(x_n)| \leq C_{b,\eta}(tn)^{-d(b+\eta)}$ , and for  $n > N$ ,  $n^{-d(b+\eta)} = n^{-s_0}n^{s_0-d(b+\eta)} \leq n^{-s_0}N^{s_0-d(b+\eta)}$ .  $\square$

The coefficient programs `deg8/dcoef4.c` (degree 4) and `deg8/octcoef.c` (degree 8) compute, for each  $L$ -function and each cell  $i$  (the  $n$  with  $x_n \in (\xi_{i+1}, \xi_i]$ ), the moments  $S_{ik} = \sum_n a_n u_n^k$ ,  $u_n = x_n/\xi_i - 1$ , for  $k \leq 20$ , and  $A_i = \sum_n |a_n|$ , in double precision with compensated (Kahan) summation. These moments differ from those of Subsection 4.6: the variable is  $u_n$ , and there is no weight  $n^\nu$ . The program `deg8/leval.py` turns kernels and moments into enclosures

$$L(\sigma) \in \frac{t^\sigma}{\prod_j \Gamma(\sigma/d + \mu_j)} \left( \sum_i \sum_k p_{ik} S_{ik} \pm (\sum_i A_i R_i + \text{tail}) \right),$$

where  $p_{ik}$  are the Taylor coefficients of the kernels at  $\xi_i$  in the variable  $u$ ,  $R_i$  the cell remainders of Lemma 6.3(a) and “tail” the bound of Lemma 6.3(b), for the two kernels  $\mathcal{I}_{\sigma/d}$  and  $\mathcal{I}_{(1-\sigma)/d}$ . It treats each moment as a ball whose radius bounds the floating-point errors: the error of  $t$  in double precision, bounded in Arb; the errors of  $x_n$ ,  $u_n$  and the powers, a few units in the last place each ( $|u_n| \leq 1 - \xi_{i+1}/\xi_i$  exactly, since the cells are cut at exact thresholds); and the error of Kahan summation, at most  $(2 \cdot 2^{-53} + O(n2^{-106}))$  times the sum of the absolute values of the terms [12, Section 4.3], plus the merging of the thread accumulators. For the degree-4 functions the Rankin tail uses  $|a_n| \leq \tau_4(n)$ , where  $\tau_4(n)$  is the number of ordered factorizations of  $n$  into four positive integers, and  $\sum \tau_4(n)n^{-s_0} = \zeta(s_0)^4$ . For degree 8 it uses the Euler product of  $\sum |a_n|n^{-s_0}$ : PARI's Euler factors for  $p \leq p_0$ , where  $p_0 = 2^{18}$  for the pairs (19, 23), (19, 24) and  $2^{19}$  for the other six; the sums computed by `octcoef.c` for the primes in  $(p_0, N]$ ; the bound  $\binom{k+7}{7}$  for the coefficients of prime powers beyond; and the bound  $\pi(x) \leq 1.25506 x / \log x$  of Rosser and Schoenfeld [31] for the primes beyond  $N$ .

The coefficients at large primes follow from the next lemma. Recall from Lemma 5.16 the elements  $\gamma_o \in B_{c_o}$  and the fields  $M_{o,w}$ ,  $B_{ab}$  and  $B_{ab,w}$ .

**Lemma 6.4.** (a) Let  $\psi_o$  be a form of Table 7, let  $w \in \mathbb{F}_2^8$ , and let  $p \notin \{2, 3, 5, 241\}$  be prime. The coefficient  $a_p$  of  $L(s, \rho_o \otimes \chi_w)$  is 0 if  $p$  is inert in  $B$ . If  $p$  splits in  $B$ , then

$$a_p = \sum_{\mathfrak{P}} \left( \frac{\gamma_o \alpha_w}{\mathfrak{P}} \right),$$

the sum of quadratic residue symbols over the primes  $\mathfrak{P}$  of  $B_{c_o}$  of norm  $p$ , provided  $\gamma_o$  is a unit at these primes.

(b) Let  $(a, b)$  be a pair of Lemma 5.8, let  $w \in \mathbb{F}_2^8$ , and let  $\mathfrak{q} \notin S$  be a prime of  $B$  of degree one and norm  $q \neq 241$ , with Frobenius  $g \in G_{W''}$ . For  $o \in \{a, b\}$ : if the image of  $g$  in  $\text{Gal}(M_o/B)$  is central, then  $\mathfrak{q}$  splits completely in  $F_{0,o}$ ; let  $\epsilon_o(\mathfrak{q}) \in \{\pm 1\}$  be the quadratic residue symbol of  $\gamma_o$  modulo a prime of  $B_{c_o}$  above  $\mathfrak{q}$ , provided  $\gamma_o$  is a unit there. Then  $\text{tr}(\rho_a \otimes \rho_b \otimes \chi_w)(g) = 0$  unless the image of  $g$  is central in both  $\text{Gal}(M_a/B)$  and  $\text{Gal}(M_b/B)$ , and then it equals  $4\epsilon_a(\mathfrak{q})\epsilon_b(\mathfrak{q})\chi_w(\mathfrak{q})$ . The coefficient  $a_q$  of  $L(s, \rho_a \otimes \rho_b \otimes \chi_w)$  is the sum of these traces over the two primes of  $B$  above  $q$ .

*Proof.* The fields  $M_{o,w}$  and  $B_{ab,w}$  are subfields of  $E_{W''}$  (proof of Lemma 5.16), which is unramified over  $B$  outside  $S$  since  $E_{W''} \subseteq K$ ; so  $p$ ,  $q$  and  $\mathfrak{q}$  are unramified in them.

(a) By Lemma 5.16(a),  $L(s, \rho_o \otimes \chi_w)$  is the  $L$ -function of the quadratic character  $\chi$  of  $B_{c_o}$  that cuts out  $M_{o,w} = B_{c_o}(\sqrt{\gamma_o \alpha_w})$ , so  $a_p$  is the sum of  $\chi(\mathfrak{P})$  over the primes  $\mathfrak{P}$  of  $B_{c_o}$  of norm  $p$ . If  $p$  is inert in  $B$ , there are none. Otherwise  $\mathfrak{P}$  is odd and unramified in  $M_{o,w}$ , and  $\gamma_o \alpha_w$  is a unit at  $\mathfrak{P}$ , since  $\alpha_w$  is a unit outside  $S$ ; so  $\chi(\mathfrak{P}) = 1$  exactly when  $\gamma_o \alpha_w$  is a square modulo  $\mathfrak{P}$ .

(b) The trace of a tensor product is the product of the traces, and  $\chi_w(g) = \chi_w(\mathfrak{q})$ . The character of the two-dimensional irreducible representation of  $\text{Dih}_4$  is 2 at 1,  $-2$  at the central element  $z$ , and 0 elsewhere. The image of  $g$  in  $\text{Gal}(M_o/B)$  is central exactly when it lies in  $\langle z \rangle = \text{Gal}(M_o/F_{0,o})$ , that is, when  $\mathfrak{q}$  splits completely in  $F_{0,o}$ ; then the primes of  $B_{c_o}$  above  $\mathfrak{q}$  have degree one, and the image is 1 exactly when it fixes  $\sqrt{\gamma_o} = (1 + u_o)\sqrt{\beta_o}$ , since  $z$  negates it, that is, when  $\gamma_o$  is a square modulo a prime of  $B_{c_o}$  above  $\mathfrak{q}$ . So  $\text{tr } \rho_o(g) = 2\epsilon_o(\mathfrak{q})$  in that case, and 0 otherwise. Finally, the coefficient at  $q$  of an Artin  $L$ -function over  $B$  is the sum of the traces of the Frobenius elements of the primes of  $B$  of norm  $q$ .  $\square$

*Coefficients of degree 4.* For  $p \leq 3000$  the Euler factors are PARI's  $(\zeta_{M_o,w,p}/\zeta_{B_{c_o},p}$ , program `deg8/exportg.gp`). For  $p > 3000$  only  $a_p$  enters, since the truncation point  $N$  is at most  $6.7 \cdot 10^6 < 3000^2$ , and only primes  $p$  that split in  $B$ ; then  $a_p$  is given by Lemma 6.4(a). The program `dcoef4.c` stops if a residue symbol vanishes; this does not occur.

*Coefficients of degree 8.* For  $p \leq p_0$  the Euler factors are PARI's  $(\zeta_{B_{ab,w},p}/\zeta_{B_{ab},p}$ , program `deg8/export8.gp`). The truncation point is  $N = 5.28 \cdot 10^{10}$  for the first two pairs and  $1.055 \cdot 10^{11}$  for the others, which is less than  $p_0^2$ . So every  $n \leq N$  is either  $p_0$ -smooth or  $n_1q$  with a prime  $q > p_0$  and  $n_1 < p_0$ , and for  $q > p_0$  only  $a_q$  enters, and only primes  $q$  that split in  $B$ . The program `octcoef.c` sieves the primes  $q \in (p_0, N]$  ( $2.23 \cdot 10^9$  of them for the first two pairs,  $4.34 \cdot 10^9$  for the others), evaluates the rule of Lemma 6.4(b), and enumerates the  $n = n_1q$  and the  $p_0$ -smooth  $n$  with  $a_n \neq 0$ . A prime  $\mathfrak{q}$  at which the images of the Frobenius are central but  $\gamma_o$  is not a unit at a prime of  $B_{c_o}$  above  $\mathfrak{q}$  would be listed as exceptional; none occurs. Before each run the program compares the rule with PARI's Euler factors at every unramified prime in  $(1000, p_0]$ , for all sixteen twists of the pair: these are 22832 primes for the first two pairs and 43222 for the others, with between 1395 and 2722 primes of  $B$  per pair at which both quotients are central.

**6.3. Checks.** The following checks are independent of the coefficient rules and of the kernels, or of part of them; none is used in the proof.

- (1) *Euler products.* At  $s = 19/10$  the Euler products of the degree-8 functions converge absolutely. For every pair, the program `deg8/octtest.py` compares the value given by the approximate functional equation (radius about  $10^{-14}$ ) with the Euler product (radius about  $3 \cdot 10^{-10}$ ): all 128 functions agree, with midpoints within  $8 \cdot 10^{-16}$ . A wrong conductor, gamma factor, root number or coefficient rule would show here.
- (2) *Kernels.* For each of the four gamma factors, `gkernel.py` reproduces PARI's `lfun` values of products of quadratic Dirichlet  $L$ -functions with that gamma factor, within the certified radii.
- (3) *Two implementations.* `dcoef4.c` with `leval.py` reproduces the values computed by the independent program `dafe.py`, with the kernels of the data archive in `papers/0.0418235/certificates` of [23]: for the twists of  $\psi_{19}$  at 801/800, and for all 6912 values of the 192 twists of  $\psi_{10}, \psi_{23}, \psi_{24}$  at the 36 abscissae, where all balls overlap and the midpoints agree to  $3.4 \cdot 10^{-16}$  relative to the values.
- (4) *Coefficients.* The moments of `dcoef4.c` and `octcoef.c` agree with independent Python implementations up to  $10^6$  and  $2 \cdot 10^6$ ; the coefficients of the 192 twists of  $\psi_{10}, \psi_{23}, \psi_{24}$  agree with PARI's Dirichlet series  $\zeta_{M_o,w}/\zeta_{B_{c_o}}$  up to 20000, and for sample twists PARI's `lfun` with the same data satisfies the functional equation to  $2^{-41}$  or better.
- (5) *Reviews.* Independent reviews reproduced the Euler-factor identity of Lemma 5.13(e) at all primes up to 1000 and at 2, 3, 5; the degree-8 Euler factors at 57 primes of vector 0; all degree-8 conductors by a different construction; and PARI's `lfun` values of the twists of  $\psi_{20}, \psi_{17}$  and  $\psi_7$  inside the stored enclosures. No reviewer recomputed the degree-8 values, whose conductors are beyond the reach of general-purpose software.

**6.4. Results.** This subsection states the enclosures; with (5.14) they are used in Lemma 7.3.

**Proposition 6.5.** *For each abscissa  $\sigma_j$  of Table 9 and each of the 576  $L$ -functions  $L$  in (5.14), the directories `hp` and `hp3` contain an interval that contains  $L(\sigma_j)$ , of radius at most the entry of Table 8, relative to the value. With Proposition 4.31 and (5.14) they give an enclosure of  $Y_{W^n}(\sigma_j)$ ; for instance  $Y_{W^n}(1001/1000) = 0.050492599$  with radius  $4 \cdot 10^{-12}$ .*

*Proof (computer-assisted).* By Lemmas 5.16(c) and 5.17, each of the 576 functions satisfies the hypotheses of Lemma 6.1, with  $Q$  its conductor and  $G$  its gamma factor. For all 576 functions, the program `deg8/leval.py` evaluates the series of Lemma 6.1 as described in Subsection 6.2: with the kernels of `deg8/gkernel.py` (Lemma 6.2), the coefficients from PARI's Euler factors and Lemma 6.4, the cell remainders and tails of Lemma 6.3, and the floating-point errors bounded as described there. The Dirichlet coefficients are computed by `dcoef4.c` (degree 4) and `octcoef.c` (degree 8) from data exported with PARI/GP (Subsection 6.2).  $\square$

TABLE 8. The  $L$ -functions in (5.14): number, gamma factor, terms of the approximate functional equation, and the largest radius of the enclosures of their values at the abscissae (relative, except for  $Y_E$ , where it is absolute). All data are in the directories `hp` and `hp3`.

| functions                         | number | gamma factor                                                 | terms                           | radius                           |
|-----------------------------------|--------|--------------------------------------------------------------|---------------------------------|----------------------------------|
| quadratic, $E$                    | 255    | $\Gamma_{\mathbb{R}}(s + \nu)^2$ or $\Gamma_{\mathbb{C}}(s)$ | $8\lfloor\sqrt{Q_e}\rfloor + 1$ | $1.3 \cdot 10^{-19}$ (in $Y_E$ ) |
| $\psi_{10}, \psi_{23}, \psi_{24}$ | 192    | $\Gamma_{\mathbb{C}}(s)^2$                                   | up to $2.1 \cdot 10^6$          | $2.6 \cdot 10^{-13}$             |
| $\psi_{19}, \psi_{20}$            | 128    | $\Gamma_{\mathbb{C}}(s)^2$ , mixed                           | up to $6.7 \cdot 10^6$          | $6.4 \cdot 10^{-13}$             |
| $\psi_{17}, \psi_7$               | 128    | $\Gamma_{\mathbb{C}}(s)^2$                                   | up to $6.7 \cdot 10^6$          | $2.2 \cdot 10^{-13}$             |
| pairs (19, 23), (19, 24)          | 32     | $\Gamma_{\mathbb{C}}(s)^4$                                   | up to $5.28 \cdot 10^{10}$      | $5.1 \cdot 10^{-10}$             |
| other six pairs                   | 96     | $\Gamma_{\mathbb{C}}(s)^4$                                   | up to $1.055 \cdot 10^{11}$     | $5.1 \cdot 10^{-10}$             |

## 7. PROOF OF THE BOUND FOR THE RELATIVE ZETA VALUE

This section completes the proof of Theorem 4.2, the bound  $C_{\text{eff}}$  for the relative zeta value that the proof of Theorem 1.1 uses. We apply Proposition 4.19 with the floors of Definition 5.20, which form a system of floors by Lemma 5.21, and with the kernel of Definition 7.1. Lemma 7.2 checks the conditions on the kernel, and Lemma 7.3 bounds the terms of the right-hand side of Proposition 4.19 other than  $Z_{\text{sel}}(1)$ , from the census (Proposition 5.12) and the values of Propositions 4.31 and 6.5.

**Definition 7.1.** Let  $\sigma_1 < \dots < \sigma_{21}$  and  $c_1, \dots, c_{21}$  be the abscissae and coefficients of Table 9; the  $c_j$  are rational numbers, given exactly in the witness file `witness_0.043171.json`. Let  $b_{\text{TV}} = 8687735449/76582443134581$ , so that  $b_{\text{TV}} \approx 1.1344291 \cdot 10^{-4}$ , and let  $\mathbf{K} = \sum_j c_j g_{\sigma_j}$  be the kernel of Proposition 4.19 with  $n = 21$ .

**Lemma 7.2.** *The kernel  $\mathbf{K}$  and the number  $b_{\text{TV}}$  of Definition 7.1 satisfy conditions (i)–(iii) of Proposition 4.19 for every real  $q \geq q_{\min} = 41^4$ .*

*Proof (computer-assisted).* Write  $x = \log q$ , and consider

$$\Phi_1 = e^x(\mathbf{K} - g_1 + b_{\text{TV}} w)(e^x), \quad \Phi_2 = e^x \mathbf{K}(e^x), \quad \Phi_3 = e^x \frac{d}{dx} \mathbf{K}(e^x).$$

Conditions (i)–(iii) say  $\Phi_1 \geq 0$ ,  $\Phi_2 \geq 0$  and  $\Phi_3 \leq 0$ . The supplementary program `signed.py` (function `certify`) evaluates them in Arb interval arithmetic in the forms

$$e^x g_s(e^x) = e^{-(s-1)x} \sum_{k \geq 1} \frac{y^{k-1}}{k}, \quad e^x \frac{d}{dx} g_s(e^x) = -s e^{-(s-1)x} \sum_{k \geq 0} y^k, \quad y = e^{-sx},$$

TABLE 9. The abscissae  $\sigma_j$  and the coefficients  $c_j$  of the kernel  $K$ , rounded to ten significant digits; the exact rational  $c_j$  are in the witness file. The coefficients were found by a linear programme over 36 abscissae, which left the others at 0; the programme is only a search, and Lemma 7.2 certifies its output.

| $j$ | $\sigma_j$    | $c_j$          | $j$ | $\sigma_j$   | $c_j$        |
|-----|---------------|----------------|-----|--------------|--------------|
| 1   | $1 + 1/43691$ | 0.02910294798  | 12  | $1 + 1/1499$ | -151.8093424 |
| 2   | $1 + 1/38178$ | -0.08993884045 | 13  | $1 + 1/1000$ | 252.1350250  |
| 3   | $1 + 1/29151$ | 0.2136909555   | 14  | $1 + 1/667$  | -603.3009258 |
| 4   | $1 + 1/22258$ | -0.3750021755  | 15  | $1 + 1/510$  | 918.2080358  |
| 5   | $1 + 1/14851$ | 0.8571627861   | 16  | $1 + 1/389$  | -810.8699335 |
| 6   | $1 + 1/9909$  | -3.840291426   | 17  | $1 + 1/297$  | 442.3163431  |
| 7   | $1 + 1/7566$  | 10.76698443    | 18  | $1 + 1/198$  | -276.0370606 |
| 8   | $1 + 1/5777$  | -19.69796042   | 19  | $1 + 1/173$  | 175.9689941  |
| 9   | $1 + 1/4411$  | 23.59901759    | 20  | $1 + 1/115$  | -22.66409771 |
| 10  | $1 + 1/2943$  | -32.93912380   | 21  | $1 + 1/101$  | 8.602447576  |
| 11  | $1 + 1/1964$  | 89.92828213    |     |              |              |

which avoid cancellation, and  $e^x w(e^x) = 2x \sum_{m \geq 1} e^{-(m-1)x} / (1 + e^{-mx})$ . The series in  $y$  are cut after ten terms; since  $x \geq \log q_{\min} > 14$ , the remainder and its first three derivatives are less than  $10^{-55}$ , which is added as a radius. In  $w$  the terms with  $m > 6$  are dropped, which only lowers  $\Phi_1$ .

The range  $\log q_{\min} \leq x \leq 2 \cdot 10^6$ . This range is cut into cells of width  $1/20$  for  $x < 60$  and  $x/100$  beyond. On a cell with midpoint  $x_0$  and half-width  $r$ , the program computes the Taylor coefficients of orders 0, 1 and 2 of  $\Phi_k$  at  $x_0$ , and an enclosure of the third derivative over the whole cell, by power series arithmetic over a ball; this bounds  $\Phi_k$  on the cell. A cell on which a bound fails is bisected. All 1976 cells pass, with  $\Phi_1 \geq 1.86 \cdot 10^{-7}$ ,  $\Phi_2 \geq 3.73 \cdot 10^{-22}$  and  $-\Phi_3 \geq 3.73 \cdot 10^{-22}$ ; the last two minima occur near  $x = 2 \cdot 10^6$ , where  $\Phi_2$  is of order  $c_1 e^{-(\sigma_1-1)x}$ .

The range  $x \geq X = 2 \cdot 10^6$ . There  $0 \leq y \leq e^{-X}$ , so  $1 \leq \sum_k y^{k-1}/k \leq 1 + e^{-X}$  and  $1 \leq \sum_k y^k \leq 1 + 2e^{-X}$ . Since  $c_1 > 0$  and  $\sigma_1$  is the smallest abscissa,

$$e^{(\sigma_1-1)x} \Phi_2 \geq c_1 - \sum_{j \geq 2} |c_j| (1 + e^{-X}) e^{-(\sigma_j - \sigma_1)X},$$

$$-e^{(\sigma_1-1)x} \Phi_3 \geq c_1 \sigma_1 - \sum_{j \geq 2} |c_j| \sigma_j (1 + 2e^{-X}) e^{-(\sigma_j - \sigma_1)X},$$

and the program checks that both right sides are positive. Moreover  $e^x g_1(e^x) \leq 1 + e^{-X}$  and  $e^x w(e^x) \geq 2x(1 - e^{-X})$ , and  $2b_{TV}X > 1 + 3e^{-X}$ , so  $g_1 - b_{TV}w < 0 \leq K$  there, which is (i).  $\square$

**Lemma 7.3.** For the floors of Definition 5.20, with floor sum  $Y_{\text{fl}}$ , and the kernel of Definition 7.1,

$$\sum_{j=1}^{21} c_j Y_{\text{fl}}(\sigma_j) + b_{TV} (2\kappa_{\infty} - T_{\text{sel}}) < 0.000607837.$$

*Proof (computer-assisted).* For  $N > 1$  put  $T_{\mathbf{c}}(N) = \sum_j c_j T_{\sigma_j}(N)$ , with  $T_{\sigma}$  as in Lemma 5.22. By that lemma,

$$\sum_j c_j Y_{\text{fl}}(\sigma_j) = \sum_j c_j Y_{\text{cor}}(\sigma_j) - \sum_{\mathbf{p} \in \mathcal{P}_2, N_{\mathbf{p}} > 1.2 \cdot 10^7} T_{\mathbf{c}}(N_{\mathbf{p}}),$$

where  $Y_{\text{cor}}(\sigma) = Y_{W''}(\sigma) - \Delta_{\text{sel}}(\sigma) - Z_{\text{sel}}(\sigma) - \Delta_4(\sigma) - \sum T_{\sigma}(N_{\mathbf{p}})$ , the last sum over the 136 primes of  $\mathcal{P}_2$  of norm at most  $1.2 \cdot 10^7$ . The program `signed3.py` (with `signed.py`) computes  $Y_{\text{cor}}(\sigma_j)$  by `dihedral_ceiling3.py` from the enclosures of Propositions 6.5 and 4.31, with  $\Delta_{\text{sel}}$  given by Lemma 5.23, prime by prime for the corrections, in Arb; since the  $c_j$  have both signs, each  $Y_{\text{cor}}(\sigma_j)$

is used as a two-sided enclosure. This gives  $\sum_j c_j Y_{\text{cor}}(\sigma_j) \leq 0.000561519780954$  (the enclosure is  $[0.000561490206974, 0.000561519780954]$ ; only the upper end is used).

The primes of  $\mathcal{P}_2$  above  $1.2 \cdot 10^7$  are known through their bin counts (Proposition 5.12). The program groups the nonempty bins into runs of at most eight consecutive bins. On a run, every counted norm lies in an interval  $[\text{lo}, \text{hi}]$ , which includes one bin of slack on each side, with midpoint  $N_0$  and half-length  $r$ , and by the mean value theorem

$$T_{\mathbf{c}}(N) \in T_{\mathbf{c}}(N_0) + T'_{\mathbf{c}}([\text{lo}, \text{hi}]) [-r, r],$$

which is multiplied by the exact count of the run. Evaluating the large signed coefficients only in the derivative term keeps the enclosure narrow. This gives  $\sum T_{\mathbf{c}}(\mathbf{Np}) \geq 0.0000757399496680$  (the enclosure is  $[0.0000757399496680, 0.000075736213684]$ ; only the lower end is used). Finally  $2\kappa_{\infty} - T_{\text{sel}} = 1.07342687156367 \dots$  is computed in Arb from the definitions, so that  $b_{\text{TV}}(2\kappa_{\infty} - T_{\text{sel}}) \leq 0.000121772671416$ , and

$$\begin{aligned} & 0.000561519780954 - 0.0000757399496680 + 0.000121772671416 \\ &= 0.000607552502702 < 0.000607837. \end{aligned}$$

The displayed endpoints are rounded outward from the Arb enclosures; the supplementary program `ce_values_digits.py` prints them with all digits, and the upper end of the total computed in Arb is  $0.00060755250270059 \dots$ . The bound of the lemma is stated with a margin of about  $2.8 \cdot 10^{-7}$ ; it is not tight, and Theorem 4.2 needs only the bound  $0.000607837$ .  $\square$

*Proof of Theorem 4.2.* By Lemmas 5.21 and 7.2, Proposition 4.19 applies to the floors of Definition 5.20 and the kernel of Definition 7.1. By Lemmas 4.17 and 7.3,

$$\begin{aligned} Z_{\text{sel}}(1) + \sum_j c_j Y_{\text{fl}}(\sigma_j) + b_{\text{TV}}(2\kappa_{\infty} - T_{\text{sel}}) &< 0.0416684840321405 + 0.000607837 \\ &< 0.0422763211 < 0.0422764. \end{aligned}$$

The interval evaluation of the same expression from the unrounded enclosures, by `signed.py`, gives the upper bound  $0.04227603653484 \dots$ . Proposition 4.19 with  $C' = C_{\text{eff}}$  proves the theorem.  $\square$

*Remark 7.4.* For comparison, the comparison field  $E_{W''}$  with a single abscissa does less. At  $\sigma = 1001/1000$ , the bound of Proposition 4.15 with the termwise bound  $Y_{W''} - \Delta_{\text{sel}} - \Delta_4$ , the census credit  $\sum_{\mathbf{p} \in \mathcal{P}_2} T_{\sigma}(\mathbf{Np})$  of Lemma 5.22, and the adaptive credits of Definition 12.2, as computed by `dihedral_ceiling3.py`, is  $0.0425629$ ; the signed kernel lowers this by  $2.9 \cdot 10^{-4}$ . The linear programme that chose the kernel is a floating-point search over 36 abscissae; the proof uses only its rounded output, checked by Lemma 7.2.

## 8. UNITS OF RELATIVE NORM ONE AND PLANAR POINT SETS

This section and Sections 9 and 10 turn arithmetic data of a quadratic extension into planar point sets. Let  $K/F$  be a quadratic extension of number fields, let  $\iota$  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  $\text{rd}$  and the discriminants  $\Delta_M$  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  $\Delta_K$  and  $\Delta_F$  are the absolute discriminants. Theorem 2.46 provides such extensions, with  $\lambda = 2^{9/4} \sqrt{3615}$  and  $\theta \geq \theta_*$ ; there  $\iota$  is the complex conjugation  $\iota_1$ . 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  $N(x\mathcal{O}_K) = |N_{K/\mathbb{Q}}x|$

[17, Propositions 4.1 and 4.2]. We take the unit theorem and the covolumes of ideal lattices from [17], and the Herbrand quotient, Hilbert's Theorem 90 and the analytic class-number formula from [18].

The argument has five steps. Proposition 8.5 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 8.11 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  $\beta_i \mathcal{O}_K^1$ , where  $\mathcal{O}_K^1$  is the group of units of relative norm one (Definition 8.4). Lemmas 8.14 and 8.19 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 8.16) that differ by the image of an element of  $\bigcup_i \beta_i \mathcal{O}_K^1$ . Lemmas 8.22 and 8.24 bound the number of lattice points in a window uniformly, by Poisson summation. Finally, Proposition 8.32, the geometric transfer, takes the window to be a sublevel set of the total energy of a pair of profiles (Definition 8.28 and Lemma 8.31) and combines these steps. Section 9 adds weights at finitely many split finite places (Proposition 9.26); that is the form used in Section 11. As in the introduction,  $u(U)$  denotes the number of unordered pairs of points at distance one in a finite set  $U \subset \mathbb{R}^2$ .

**8.1. Coordinates.** This subsection identifies  $K \otimes_{\mathbb{Q}} \mathbb{R}$  with  $\mathbb{C}^d$  so that elements of relative norm one have modulus one at the compact coordinates, which give the planar map, and reciprocal moduli at the pair coordinates, which are used for unit averaging (Lemma 8.2).

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.

**Definition 8.1.** (a) 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  $v$ , and write  $v(y) \in \mathbb{R}$  for the image of  $y \in F$  under the real embedding  $v$ . 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  $\tau_j$  to  $F$  induces it, and put  $\phi_j^- = \phi_j^+ \circ \iota$ .

(b) For  $x \in K$  put

$$x_{\infty} = ((\phi_v(x))_v, (\phi_j^+(x), \phi_j^-(x))_j) \in \mathbb{C}^d,$$

and for  $\mathfrak{a} \subset K$  put  $\mathfrak{a}_{\infty} = \{x_{\infty} : x \in \mathfrak{a}\}$ .

(c) For  $x \in K^{\times}$  put

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

(d) The  $b$  coordinates  $\phi_v$  of  $x_{\infty}$  are the *compact coordinates*, and the  $c$  pairs  $(\phi_j^+, \phi_j^-)$  are the *pair coordinates*. A compact coordinate, or a pair of coordinates, is called a *block*.

The embeddings  $\phi_j^{\pm}$  induce the two places of  $K$  above the  $j$ -th complex place of  $F$ : they are distinct, and they are not complex conjugate, because  $\tau_j$  is not real. We identify  $K \otimes_{\mathbb{Q}} \mathbb{R}$  with  $\mathbb{C}^d$  through the map  $x \mapsto x_{\infty}$ , and  $\mathbb{C}^d$  with  $\mathbb{R}^{2d}$  through real and imaginary parts. Volumes are Lebesgue measure in these coordinates, and  $\langle x, \xi \rangle = \operatorname{Re} \sum_w x_w \overline{\xi_w}$  is the real inner product on  $\mathbb{C}^d$ , where  $w$  runs over the  $d$  coordinates. For a Borel set  $\Omega$ ,  $|\Omega|$  denotes its volume; for a finite set,  $|\cdot|$  denotes its cardinality.

**Lemma 8.2.** For  $x \in K$ , every real place  $v$  of  $F$  and  $1 \leq j \leq c$ ,

$$(8.3) \quad |\phi_v(x)|^2 = v(N_{K/F}x), \quad \phi_j^+(x) \phi_j^-(x) = \tau_j(N_{K/F}x).$$

In particular, if  $N_{K/F}\beta = 1$ , then  $|\phi_v(\beta)| = 1$  for every real place  $v$ , and  $|\phi_j^{\pm}(\beta)| = e^{\pm l_j(\beta)}$  for every  $j$ .

*Proof.* At a real place  $v$  of  $F$ , the automorphism  $\iota$  induces complex conjugation on the completion  $\mathbb{C}$  of  $K$ , so  $\phi_v(\iota x) = \overline{\phi_v(x)}$ , and  $|\phi_v(x)|^2 = \phi_v(x) \phi_v(\iota x) = v(N_{K/F}x)$ . Similarly  $\phi_j^+(x) \phi_j^-(x) =$

$\phi_j^+(x \iota x) = \tau_j(N_{K/F}x)$ . If  $N_{K/F}\beta = 1$ , the first identity gives  $|\phi_v(\beta)| = 1$ , and the second gives  $|\phi_j^+(\beta)| |\phi_j^-(\beta)| = 1$ , that is,  $\log |\phi_j^\pm(\beta)| = \pm l_j(\beta)$ .  $\square$

Thus at the compact coordinates the elements of relative norm one lie on the unit circle, and at the pair coordinates they have reciprocal moduli. 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.

**8.2. The Class-Number Formula for Units of Relative Norm One.** This subsection expresses the quantity  $w_K/(h_{\text{rel}}h_{\text{cap}}\text{Reg}^1)$  (Definition 8.4 and Proposition 8.5), which governs the number of elements of relative norm one produced in the next subsections, through  $L_F(1)$  (Proposition 8.5). The hypothesis on  $L_F(1)$  in Propositions 8.32 and 9.26 enters only through this formula.

**Definition 8.4.** Let  $\mathcal{O}_K^\times$  and  $\mathcal{O}_F^\times$  be the unit groups, and put

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

the group of *units of relative norm one* and the *unit norm index*. 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  $h_{\text{rel}} = h_K/h_F$ , and let  $h_{\text{cap}}$  be the order of the *capitulation kernel*  $\ker(\text{Cl}(F) \rightarrow \text{Cl}(K))$ , the map being induced by extension of ideals. Let  $L_F(s) = \zeta_K(s)/\zeta_F(s)$ , the relative zeta function of the introduction; at  $s = 1$ ,  $L_F(1)$  denotes the quotient of the residues of  $\zeta_K$  and  $\zeta_F$ . The regulators  $\text{Reg}_K$  and  $\text{Reg}_F$  are the ordinary ones, which use twice the logarithm of the absolute value at a complex place [17, Chapter 5].

**Proposition 8.5.** *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  $\text{Reg}^1$  be the covolume of this lattice, with  $\text{Reg}^1 = 1$  if  $c = 0$ . Then*

$$h_{\text{cap}} = u_N/2^{b-1}, \quad \text{Reg}_K / \text{Reg}_F = 2^{c-1}u_N \text{Reg}^1,$$

and consequently

$$(8.6) \quad \frac{w_K}{h_{\text{rel}}h_{\text{cap}}\text{Reg}^1} = \frac{2^{d-1}\pi^{b+c}}{\lambda^{d/2}L_F(1)}.$$

*Proof. Signs.* Fix a real place  $v_0$  of  $F$ . By (8.3),  $v_0(N_{K/F}x) = |\phi_{v_0}(x)|^2 > 0$  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  $\pm 1$  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  $\text{Log}_F$  is  $\{\pm 1\}$  [17, Proposition 5.8], and  $\text{Reg}_K$  and  $\text{Reg}_F$  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  $\beta$  has absolute value one, that is, when  $\beta$  is a root of unity [17, 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 [17, 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 of a  $\langle \iota \rangle$ -module  $M$  is

$$h_{\text{Her}}(M) = |\widehat{H}^0(\langle \iota \rangle, M)|/|H^1(\langle \iota \rangle, M)|$$

[18, Chapter II, §3]. For the units it satisfies  $2h_{\text{Her}}(\mathcal{O}_K^\times) = \prod_v [K_w : F_v]$ , where  $v$  runs over the archimedean places of  $F$ ,  $w$  lies above  $v$ , and  $K_w$  and  $F_v$  are the completions [18, Chapter VII, Proposition 3.1]. Each real place contributes 2 and each complex place 1, so  $h_{\text{Her}}(\mathcal{O}_K^\times) = 2^{b-1}$ . Since  $\widehat{H}^0(\langle \iota \rangle, \mathcal{O}_K^\times) = \mathcal{O}_F^\times / N_{K/F}(\mathcal{O}_K^\times)$  has order  $u_N$ , we get  $|H^1(\langle \iota \rangle, \mathcal{O}_K^\times)| = u_N / 2^{b-1}$ . 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 [18, Chapter II, Corollary 1.23], an element of  $\mathcal{O}_K^1$  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  $\iota$ . By (G2), every  $\iota$ -invariant fractional ideal of  $K$  is extended from  $F$ : at a split prime  $\mathfrak{P} \iota \mathfrak{P}$  invariance forces equal exponents, an inert prime of  $F$  stays prime, and no prime ramifies. Hence  $h_{\text{cap}} = u_N / 2^{b-1}$ .

*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  $\text{Reg}_K$  and  $\text{Reg}_F$ . By (8.3),  $\text{Log}_F(N_{K/F}x)$  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  $\mathcal{O}_K^1$ , which after the substitution is  $2l(\mathcal{O}_K^1)$ , of covolume  $2^c \text{Reg}^1$ . Since  $-1 \notin N_{K/F}(\mathcal{O}_K^\times)$ , the projection  $T(\mathcal{U}_K)$  has index  $[\mathcal{O}_F^\times : \{\pm 1\}N_{K/F}(\mathcal{O}_K^\times)] = u_N/2$  in  $\mathcal{U}_F$ . Hence  $\text{Reg}_K = 2^c \text{Reg}^1 \cdot \text{Reg}_F u_N/2$ .

*The class-number formula.* The analytic class-number formula [18, 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

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

Substituting  $\text{Reg}_K / \text{Reg}_F = 2^{c-1} u_N \text{Reg}^1 = 2^{b+c-2} h_{\text{cap}} \text{Reg}^1$  gives (8.6).  $\square$

**8.3. Norm-One Elements from Split Primes.** This subsection produces, from the split primes above a finite set  $\mathcal{R}$  of rational primes, at least  $e^{dJ}/(h_{\text{cap}} h_{\text{rel}})$  elements of relative norm one in one fractional ideal, with pairwise disjoint cosets modulo  $\mathcal{O}_K^1$  (Lemma 8.11); this is the source of the term  $J$  of Definition 8.9 in the margin.

**Definition 8.7.** 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 2.45).

**Lemma 8.8.** *If  $K/F$  has uniform local types  $(e_r, f_r)_{r \in \mathcal{R}}$ , then for every  $r \in \mathcal{R}$  the field  $F$  has exactly  $d/(e_r f_r)$  primes above  $r$ , each of norm  $r^{f_r}$ .*

*Proof.* 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  $[F : \mathbb{Q}] = d$ , and here each product is  $e_r f_r$  and each norm is  $r^{f_r}$ .  $\square$

**Definition 8.9.** Let  $\mathcal{R}$  and  $(e_r, f_r)_{r \in \mathcal{R}}$  be as in Definition 8.7. Given integers  $k_r \geq 0$  ( $r \in \mathcal{R}$ ), called the *exponents*, put

$$(8.10) \quad H = \sum_{r \in \mathcal{R}} \frac{k_r \log r}{e_r}, \quad J = \sum_{r \in \mathcal{R}} \frac{\log(k_r + 1)}{e_r f_r}.$$

If  $K/F$  has uniform local types  $(e_r, f_r)_{r \in \mathcal{R}}$ , then by Lemma 8.8,  $e^{dH} = \prod_{\mathfrak{p}} (\mathcal{N}\mathfrak{p})^{k_r}$  and  $e^{dJ} = \prod_{\mathfrak{p}} (k_r + 1)$ , the products over the primes  $\mathfrak{p}$  of  $F$  above  $\mathcal{R}$ , with  $r$  the prime below  $\mathfrak{p}$ :  $H$  measures the density of the ideal lattice used, and  $J$  the number of equal-norm choices.

**Lemma 8.11.** *Assume that  $K/F$  has uniform local types  $(e_r, f_r)_{r \in \mathcal{R}}$ , and fix exponents  $k_r \geq 0$ , with  $H$  and  $J$  as in Definition 8.9. There are a fractional ideal  $\mathfrak{b}$  of  $K$  with  $\mathcal{N}\mathfrak{b} = e^{-dH}$ , an integer  $t \geq e^{dJ}/(h_{\text{cap}}h_{\text{rel}})$ , and elements  $\beta_1, \dots, \beta_t \in \mathfrak{b}$  of relative norm one whose cosets  $\beta_i \mathcal{O}_K^1$  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  $h_K h_{\text{cap}}/h_F = h_{\text{cap}}h_{\text{rel}}$ , so one class of this quotient contains the classes of  $\mathfrak{A}_{\mathbf{j}}$  for a set of  $t \geq e^{dJ}/(h_{\text{cap}}h_{\text{rel}})$  vectors  $\mathbf{j}$ . Fix one of them,  $\mathbf{j}_0$ , and put  $\mathfrak{b} = \mathfrak{J}_{\mathbf{j}_0}^{-1}$ . 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  $\iota$  fixes  $\mathfrak{a} \mathcal{O}_K$ ,

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

As  $\mathfrak{J}_{\mathbf{j}}$  is integral,  $\beta_{\mathbf{j}} \in \mathfrak{b}$ . The ideals  $\mathfrak{J}_{\mathbf{j}} \mathfrak{b}$  are distinct for distinct  $\mathbf{j}$ , and every element of  $\beta_{\mathbf{j}} \mathcal{O}_K^1$  generates  $\mathfrak{J}_{\mathbf{j}} \mathfrak{b}$ , so the cosets are disjoint. Finally, since each  $\mathfrak{p}$  splits in  $K$ , Lemma 8.8 gives  $(\mathcal{N}\mathfrak{b})^{-1} = \prod_{\mathfrak{p}} (\mathcal{N}\mathfrak{p})^{k_{\mathfrak{p}}} = \prod_r r^{f_r k_r d / (e_r f_r)} = e^{dH}$ .  $\square$

**8.4. Unit Averaging and Translation.** This subsection averages over the units of relative norm one and over the translates of an ideal lattice (Lemmas 8.14 and 8.19), which yields a translate with many ordered edges per point (Definition 8.18), and turns such a translate into a planar set (Lemma 8.21).

In this subsection and the next,  $\mathfrak{b}$  is a fractional ideal of  $K$  and  $\beta_1, \dots, \beta_t \in \mathfrak{b}$  are elements of relative norm one whose cosets  $\beta_i \mathcal{O}_K^1$  are pairwise disjoint; Lemma 8.11 provides such data. For  $h \in \mathbb{R}^c$  let  $W_h: \mathbb{C}^d \rightarrow \mathbb{C}^d$  multiply the coordinate  $\phi_j^+$  by  $e^{-h_j}$  and  $\phi_j^-$  by  $e^{h_j}$ , and fix the compact coordinates. It is a real diagonal map of determinant one. Put  $\Lambda_h = W_h \mathfrak{b}_{\infty}$ . For a lattice  $\Lambda \subset \mathbb{C}^d$ ,  $\text{covol}(\Lambda)$  denotes the volume of a fundamental domain. By [17, Proposition 4.26], extended to fractional ideals by scaling and [17, Proposition 4.2],

$$(8.12) \quad \text{covol}(\mathfrak{a}_{\infty}) = 2^{-d} |\Delta_K|^{1/2} \mathcal{N}\mathfrak{a}$$

for every fractional ideal  $\mathfrak{a}$  of  $K$ . Hence  $\text{covol}(\Lambda_h) = 2^{-d} \lambda^d \mathcal{N}\mathfrak{b}$ , independently of  $h$ ; for the ideal of Lemma 8.11,

$$(8.13) \quad \text{covol}(\Lambda_h) = 2^{-d} \lambda^d e^{-dH}.$$

If  $N_{K/F} \beta = 1$ , then by Lemma 8.2  $W_h \beta_{\infty}$  has compact coordinates of modulus one and pair coordinates of moduli  $e^{\pm(l_j(\beta) - h_j)}$ . Let  $\Pi^1$  be a fundamental parallelepiped of the lattice  $l(\mathcal{O}_K^1)$ ; its volume is  $\text{Reg}^1$ . When  $c = 0$ , integrals over  $\mathbb{R}^0$  and over  $\Pi^1$  are evaluations at the single point.

**Lemma 8.14.** *For every Borel function  $\Phi: \mathbb{R}^c \rightarrow [0, \infty]$ ,*

$$(8.15) \quad \frac{1}{\text{Reg}^1} \int_{\Pi^1} \sum_{i=1}^t \sum_{\beta \in \beta_i \mathcal{O}_K^1} \Phi(l(\beta) - h) dh = \frac{tw_K}{\text{Reg}^1} \int_{\mathbb{R}^c} \Phi(u) du.$$

*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 8.5 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 8.16.** 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 the *unit-norm displacement*  $\mathbf{e}(u) \in \mathbb{C}^d$  have compact coordinates 1 and pair coordinates  $(e^{u_j}, e^{-u_j})$ , and for a Borel set  $\Omega \subset \mathbb{C}^d$  put

$$\Phi_\Omega(u) = |\Omega \cap (\Omega - \mathbf{e}(u))|.$$

**Lemma 8.17.** *Let  $\Omega$  be a window.*

- (a) *If  $h \in \mathbb{R}^c$  and  $\beta \in K$  satisfies  $N_{K/F}\beta = 1$ , then  $|\Omega \cap (\Omega - W_h \beta_\infty)| = \Phi_\Omega(l(\beta) - h)$ .*
- (b) *The function  $\Phi_\Omega$  is continuous, bounded by  $|\Omega|$ , and vanishes at every  $u$  for which some  $e^{|u_j|}$  exceeds the diameter of  $\Omega$ .*

*Proof.* (a) 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  $\Omega$  and maps  $\mathbf{e}(u)$  to  $x$ , so  $|\Omega \cap (\Omega - x)| = \Phi_\Omega(u)$ . By the remark before Lemma 8.14,  $x = W_h \beta_\infty$  is such a point, with  $u = l(\beta) - h$ .

(b) We have  $\Phi_\Omega(u) = \int \mathbf{1}_\Omega(x) \mathbf{1}_\Omega(x + \mathbf{e}(u)) dx \leq |\Omega|$ . For  $y, y' \in \mathbb{C}^d$ ,  $||\Omega \cap (\Omega - y)| - |\Omega \cap (\Omega - y')||$  is at most the  $L^1$ -norm of  $\mathbf{1}_\Omega(\cdot + y) - \mathbf{1}_\Omega(\cdot + y')$ , which tends to 0 as  $y' \rightarrow y$  because translation is continuous in  $L^1(\mathbb{C}^d)$ ; and  $u \mapsto \mathbf{e}(u)$  is continuous. So  $\Phi_\Omega$  is continuous. If  $x$  and  $x + \mathbf{e}(u)$  both lie in  $\Omega$ , then  $e^{|u_j|}$ , the modulus of a coordinate of their difference  $\mathbf{e}(u)$ , is at most the diameter of  $\Omega$ .  $\square$

**Definition 8.18.** Let  $\Omega$  be a window. Fix a  $\mathbb{Z}$ -basis of  $\mathfrak{b}_\infty$ , and for  $y \in [0, 1)^{2d}$  let  $y_{\mathfrak{b}} \in \mathbb{C}^d$  be the point with coordinate vector  $y$  in this basis. For  $h \in \mathbb{R}^c$  let  $\mathcal{X}(h, y) = (\Lambda_h + W_h y_{\mathfrak{b}}) \cap \Omega$  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  $(x, \beta)$  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  $\beta \in \mathfrak{b}$ , the second endpoint  $x + W_h \beta_\infty$  of an ordered edge  $(x, \beta)$  also lies in  $\mathcal{X}(h, y)$ .

**Lemma 8.19.** *Let  $\Omega$  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*

$$(8.20) \quad \frac{\mathcal{E}(h, y)}{n(h, y)} \geq \frac{tw_K}{\text{Reg}^1} \frac{\int_{\mathbb{R}^c} \Phi_\Omega(u) du}{|\Omega|}.$$

*Proof.* For fixed  $x$ , distinct  $\beta$  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  $y \mapsto W_h y_{\mathfrak{b}}$  has Jacobian  $\text{covol}(\Lambda_h)$  and maps  $[0, 1)^{2d}$  onto a fundamental domain of  $\Lambda_h$ , so tiling and Lemma 8.17(a) 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  $dh/\text{Reg}^1$  and apply (8.15). 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  $\rho$  is the right side of (8.20). 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 8.21.** *Let  $\Omega$  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  $0 \neq \gamma \in \mathfrak{b}$ , whose  $v_0$ -coordinate  $\phi_{v_0}(\gamma)$  is nonzero, so  $|U| = n(h, y)$ . An ordered edge  $(x, \beta)$  gives two points of  $U$  at distance  $|\phi_{v_0}(\beta)| = 1$ , and distinct ordered edges give distinct ordered pairs of points. Hence  $u(U) \geq \mathcal{E}(h, y)/2$ .  $\square$

**8.5. Uniform Lattice Counting.** This subsection bounds the number of lattice points in a window uniformly in the translate (Lemmas 8.22 and 8.24); this gives the bound for  $n(h, y)$  in the proof of Proposition 8.32.

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

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

*In particular, if  $\mathbf{N}\mathfrak{b} = e^{-dH}$ , as for the ideal of Lemma 8.11, every nonzero dual vector of  $\Lambda_h$  satisfies*

$$(8.23) \quad \prod_w |\xi_w| \geq \mu^d, \quad \mu = 2e^{H/2-\ell}, \quad \|\xi\|_* \geq d\mu.$$

*Proof.* First let  $h = 0$ . For  $x, y \in K$  we have  $\langle x_\infty, \overline{y_\infty} \rangle = \operatorname{Re} \sum_w \phi_w(xy) = \frac{1}{2} \operatorname{Tr}_{K/\mathbb{Q}}(xy)$ , where the bar is coordinatewise complex conjugation and  $\phi_w$  is the embedding of the coordinate  $w$ , because these embeddings and their complex conjugates are all the embeddings of  $K$ . Let  $\mathfrak{a}^\vee = \{y \in K : \operatorname{Tr}_{K/\mathbb{Q}}(y\mathfrak{a}) \subset \mathbb{Z}\}$ . 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 (8.12) and  $\mathbf{N}(2\mathfrak{a}^\vee) = 2^{2d} \mathbf{N}(\mathfrak{a}^\vee)$ , this gives  $\mathbf{N}(\mathfrak{a}^\vee) = \lambda^{-2d} (\mathbf{N}\mathfrak{a})^{-1}$ . If  $0 \neq y \in \mathfrak{a}^\vee$ , then  $y\mathcal{O}_K \subset \mathfrak{a}^\vee$  and  $|N_{K/\mathbb{Q}} y| = \mathbf{N}(y\mathcal{O}_K) \geq \mathbf{N}(\mathfrak{a}^\vee)$  [17, Propositions 4.1 and 4.2]. For  $\xi = (2y)_\infty$ ,

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

For general  $h$ , the dual lattice of  $W_h \mathfrak{a}_\infty$  is the image of the dual lattice of  $\mathfrak{a}_\infty$  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 (8.23) take  $\mathfrak{a} = \mathfrak{b}$ .  $\square$

**Lemma 8.24.** *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*

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

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

$$(8.25) \quad \varsigma \mu \geq \log M + 2 \log 5 + 2$$

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

$$(8.26) \quad \sum_{x \in \Lambda + y} \Psi(x) \leq \frac{2}{\operatorname{covol}(\Lambda)} \int \Psi.$$

*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  $\Lambda^*$  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 (8.25) and  $M \geq 1$ ,

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

For  $\varepsilon > 0$  put  $\Psi_\varepsilon(x) = \Psi(x)e^{-\varepsilon|x|^2}$ , a Schwartz function. Its Fourier transform is  $\widehat{\Psi} * G_\varepsilon$ , where  $G_\varepsilon(\zeta) = (\pi/\varepsilon)^d e^{-\pi^2|\zeta|^2/\varepsilon}$  is a probability density on  $\mathbb{R}^{2d}$ . Hence  $|\widehat{\Psi}_\varepsilon(\xi)| \leq m_\varepsilon M^d e^{-\varsigma \|\xi\|_*} \int \Psi$ , with  $m_\varepsilon = \int e^{\varsigma \|\zeta\|_*} G_\varepsilon(\zeta) d\zeta$ . The function  $y \mapsto \sum_{x \in \Lambda} \Psi_\varepsilon(x+y)$  is smooth and  $\Lambda$ -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  $G_\varepsilon$  is the image of  $G_1$  under  $\zeta \mapsto \sqrt{\varepsilon} \zeta$ ; moreover  $\Psi_\varepsilon$  increases to  $\Psi$ . Monotone convergence gives (8.26).  $\square$

The next bound is used in Section 10 for the Gaussian real-place profile (Definition 8.28).

**Lemma 8.27.** *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  $\log 2 - 1/(4\pi^2) > 0$ .  $\square$

**8.6. Profiles at Real and Complex Places.** This subsection defines the archimedean profiles, their functionals  $J_{\mathbb{R}}$  and  $J_{\mathbb{C}}$  and the admissibility conditions (P1)–(P5), and combines the previous subsections into Proposition 8.32. Section 10 verifies admissibility for the profiles used in Section 11.

**Definition 8.28.** 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 8.32.

**Definition 8.29.** Let  $M \geq 1$  and  $\varsigma > 0$ . The pair  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  is *admissible with Fourier constants*  $(M, \varsigma)$  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)  $|\widehat{f_{\mathbb{R}}^p}(\xi)| \leq M e^{-\varsigma|\xi|} A_{\mathbb{R}}$  and  $|\widehat{g_{\mathbb{C}}^p}(\xi_1, \xi_2)| \leq M^2 e^{-\varsigma(|\xi_1|+|\xi_2|)} A_{\mathbb{C}}$  for all  $\xi, \xi_1, \xi_2 \in \mathbb{C}$ .

Section 10 proves admissibility for the profiles we use.

**Lemma 8.30.** *Let  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  be admissible with Fourier constants  $(M, \varsigma)$  (Definition 8.29), 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  $\Psi$  satisfies the hypotheses that Lemma 8.24 places on  $\Psi$ , other than the Fourier condition (8.25): it is smooth and bounded, with bounded derivatives,  $\int \Psi = A_{\mathbb{R}}^b A_{\mathbb{C}}^c$ , and*

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

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

**Lemma 8.31.** *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  $\Omega$  is closed, hence a Borel set. The function  $(x, u) \mapsto e^{-V(x)} e^{-V(x+\mathbf{e}(u))} / (I_{\mathbb{R}}^b I_{\mathbb{C}}^c)$  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  $V(x + \mathbf{e}(u))$  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,  $V(x + \mathbf{e}(u))$  has the same law as  $V(x)$ . By Chebyshev's inequality, each of the two energies differs from  $d\bar{m}$  by more than  $\eta d$  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  $\eta$ ,  $\text{Var}_{\mathbb{R}}$  and  $\text{Var}_{\mathbb{C}}$ . On  $\mathcal{Y}$  both endpoints lie in  $\Omega$  and  $e^{-V(x)} e^{-V(x+\mathbf{e}(u))} \leq e^{-2d(\bar{m}-\eta)}$ . Therefore, with  $|\mathcal{Y}|$  the Lebesgue measure of  $\mathcal{Y}$ ,

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

$\square$

**Proposition 8.32** (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  $\lambda$  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 (8.10), and let  $\mu = 2e^{H/2-\ell}$ . Let  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  be admissible with Fourier constants  $(M, \varsigma)$  (Definition 8.29) satisfying the Fourier condition (8.25). Put*

$$(8.33) \quad \mathcal{M}(\theta) = J - \delta H - (1/2 - \delta)\ell - C + (1 - \delta) \log 2 + (1 - \theta) \log \pi + (1 - 2\theta)J_{\mathbb{R}} + \theta J_{\mathbb{C}}.$$

*We call  $\mathcal{M}(\theta)$  the margin. If  $\inf_i \mathcal{M}(\theta_i) > 0$ , where  $\theta_i$  is the value of  $\theta$  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 8.31; 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  $\mathbf{b}$ ,  $t$  and  $\beta_1, \dots, \beta_t$  from Lemma 8.11, so that  $\Lambda_h$  is defined; the counts  $n(h, y)$  and  $\mathcal{E}(h, y)$  of

Definition 8.18 are those of the window  $\Omega$  chosen next. With the total energy  $V$  and the mean  $\bar{m}$  of Lemma 8.31, let

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

By (P1) and (P3) (see the proof of Lemma 8.31), this is a bounded Borel set, and it is invariant under coordinate rotations because the profiles are radial in each coordinate. By Lemma 8.31,

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

for all large  $d$ , uniformly in the signature. In particular  $|\Omega| > 0$  for large  $d$ , so  $\Omega$  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 8.30, 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 8.22, 8.24 and 8.30 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 (8.13),  $b/d = 1 - 2\theta$  and  $c/d = \theta$  (here  $b$  and  $c$  are the numbers of real and complex places of  $F$ ; the ideal  $\mathfrak{b}$  is unrelated).

*Counting edges.* Now take a pair  $(h, y)$  from Lemma 8.19, applied with  $n_{\max} = 2e^{dY_\eta}$ . By  $t \geq e^{dJ}/(h_{\text{cap}} h_{\text{rel}})$ , Proposition 8.5,  $\log L_F(1) \leq dC$  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  $\Phi_\Omega$ , (8.20) 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

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

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 8.21,  $|U| = n$  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.  $\square$

### 9. 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 11 these are the places above the selected primes of  $B$  (Definition 4.16). In Lemma 8.11, 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 9.7; shell profiles replace this indicator by weighted sums of indicators of products of shells (Corollary 9.29). The main result is Proposition 9.26, the transfer with shell profiles, which is the form of the construction applied in Section 11; its margin (9.27) replaces the terms  $J - \delta H$  of (8.33) by the values of a local functional (Definition 9.3). We keep the hypotheses (G1)–(G3) and the notation of Section 8, and put

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

**9.1. The Local Functional.** This subsection defines the local functional at a split finite place and computes it for shell profiles (Lemma 9.11); its values are the terms  $\log \mathcal{F}_{\delta,p}$  of the margin (9.27).

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

**Definition 9.1.** For  $n \in \mathbb{Z}$  and  $\omega \in \mathcal{O}^\times$  put

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

for a locally constant, compactly supported function  $g$  on  $\mathbb{L}^2$ .

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.

**Lemma 9.2.** Let  $\varphi_1$  and  $\varphi_2$  be locally constant and compactly supported on  $\mathbb{L}^2$ . Then only finitely many  $n$  contribute to  $\int_{\mathbb{L}^2} \varphi_1 \mathcal{T}\varphi_2$ , which is therefore a finite sum of finite integrals.

*Proof.* If  $\varphi_1(z)\varphi_2(z + s(n, \omega)) \neq 0$ , then both coordinates of  $s(n, \omega)$  lie in the compact set  $\text{supp } \varphi_2 - \text{supp } \varphi_1$ , which bounds  $n$  from above and from below.  $\square$

**Definition 9.3.** For locally constant, compactly supported functions  $\varphi_1, \varphi_2$  on  $\mathbb{L}^2$  put  $\langle \varphi_1, \varphi_2 \rangle_{\mathcal{T}} = \int_{\mathbb{L}^2} \varphi_1 \mathcal{T}\varphi_2$  (Lemma 9.2). For a nonnegative, locally constant, compactly supported function  $g$  on  $\mathbb{L}^2$  with  $g \neq 0$ , and  $0 < \delta < 1$ ,  $p = 2/(1 + \delta)$ , put

$$(9.4) \quad A(g) = \int_{\mathbb{L}^2} g^p, \quad I(g) = \langle g, g \rangle_{\mathcal{T}}, \quad \mathcal{F}_\delta(g) = \frac{I(g)}{A(g)^{1+\delta}}.$$

We call  $A(g)$  the *mass*,  $I(g)$  the *overlap* and  $\mathcal{F}_\delta$  the *local functional*, as for the archimedean masses and overlaps of Definition 8.28.

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 9.5.** For all integers  $i_1, j_1, i_2, j_2$ ,

$$(9.6) \quad \langle \mathbf{1}_{\mathcal{B}_{i_1} \times \mathcal{B}_{j_1}}, \mathbf{1}_{\mathcal{B}_{i_2} \times \mathcal{B}_{j_2}} \rangle_{\mathcal{T}} = Q^{\min(i_1, i_2) + \min(j_1, j_2)} [\max(i_1, i_2) + \max(j_1, j_2) + 1]_+.$$

*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 (9.6) is therefore  $Q^{\min(i_1, i_2) + \min(j_1, j_2)}$  times the measure of the set of  $(n, \omega)$  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  $\omega$ , and  $d\omega$  has total measure one.  $\square$

**Definition 9.7.** 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  $\mathbb{L}^2$  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 9.8.** 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

$$(9.9) \quad \mathcal{C} = \mathcal{O} \times \varpi^{-k}\mathcal{O}, \quad |\mathcal{C}| = Q^k.$$

*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  $\varpi^k$  times the second.  $\square$

We call  $\mathcal{C}$  the *period* of  $g$ .

**Definition 9.10.** Let  $Q$  and  $k$  be as in Definition 9.7, with shell measures  $m_i$ . The symmetric matrix  $\mathbf{D} = (\mathbf{D}_{ii'})_{i,i' \geq 0}$  is defined by

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

and the *shell Gram matrix*  $\mathbf{G}$ , indexed by pairs of pairs of nonnegative integers, by

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

**Lemma 9.11.** The shell profile  $g$  with parameters  $(Q, k, w)$  satisfies, with the shell measures  $m_i$  and the shell Gram matrix  $\mathbf{G}$  of Definition 9.10,

$$(9.12) \quad A(g) = Q^k \sum_{i,j} m_im_j w_{ij}^p, \quad I(g) = Q^k \sum_{(i,j),(i',j')} w_{ij} \mathbf{G}_{(i,j),(i',j')} w_{i'j'}.$$

All entries of  $\mathbf{G}$  are nonnegative, and  $I(g) \geq (k+1)Q^k w_{00}^2 > 0$ . 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  $I(g)$ , 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 (9.6) 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  $\varphi$  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  $\partial$  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  $\mathbf{D}_{ii'}$ . 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  $\langle \mathbf{1}_{\mathcal{S}_{i_1} \times \varpi^{-k}\mathcal{S}_{j_1}}, \mathbf{1}_{\mathcal{S}_{i_2} \times \varpi^{-k}\mathcal{S}_{j_2}} \rangle_{\mathcal{T}} = Q^k \mathbf{G}_{(i,j),(i',j')}$ , and hence the formula for  $I(g)$ . All entries of  $\mathbf{G}$  are nonnegative, since  $\mathbf{D}_{ii} = Q^{i-1}(iQ - i - 1) \geq 0$  for  $i \geq 1$ ; as  $\mathbf{G}_{(0,0),(0,0)} = k+1$ , this gives  $I(g) \geq (k+1)Q^k w_{00}^2$ . For the unweighted shell profile only  $\mathbf{G}_{(0,0),(0,0)} = k+1$  contributes.  $\square$

**Definition 9.13.** Let  $g$  be a shell profile. By Lemma 9.11,  $I(g) > 0$ , and by the definition of  $I(g)$  the function  $(z, n, \omega) \mapsto g(z)g(z+s(n,\omega))/I(g)$  is a probability density on  $\mathbb{L}^2 \times \mathbb{Z} \times \mathcal{O}^\times$ , with counting measure on  $\mathbb{Z}$ . As at the archimedean places (Definition 8.28), we call it the *endpoint law* of  $g$ ; its first endpoint is  $z$  and its second endpoint is  $z+s(n,\omega)$ .

**Corollary 9.14.** Let  $x = (x_i)_{i \geq 0}$  and  $x' = (x'_j)_{j \geq 0}$  be finitely supported vectors of nonnegative numbers with  $x_0 x'_0 > 0$ , and with  $\mathbf{D}$  as in Definition 9.10 put

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

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

$$(9.15) \quad A(g) = Q^k P_x P_{x'}, \quad I(g) = Q^k [(k+1)S_x S_{x'} + R_x S_{x'} + S_x R_{x'}].$$

*Proof.* Substitute  $w_{ij} = x_i x'_j$  in (9.12). □

*Remark 9.16.* 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

$$(9.17) \quad \log \frac{(k + 1)S_x^2 + 2S_x R_x}{k + 1} - 2(1 + \delta) \log(1 + (Q - 1)t^p).$$

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.

*Remark 9.18.* Section 11 uses general weights  $w_{ij}$ , symmetric  $10 \times 10$  matrices, at the places above 2, 3 and 5, through the formulas (9.12), and product weights, through (9.15), at the places above 29 and  $t_3$ . Nothing in the rest of this section, in particular in the proof of Proposition 9.26, uses the product form: it uses only that a shell profile is nonnegative, locally constant and compactly supported, invariant under units in each coordinate and under its period (Lemma 9.8), with  $I(g) > 0$  (Lemma 9.11), and that its parameters range over a finite set. As a check of (9.12) for general weights, the supplementary program `general_windows_check.py` compares it with a direct computation in a finite model of the local field, in 48 cases, 32 of them with random weights and 16 with a fixed family of monotone weights that are not symmetric, and finds exact agreement; the program `general_windows.py` that evaluates (9.12) for the certificate reproduces (9.15) exactly for product weights.

**9.2. Finite Periods and Lattice Counting.** This subsection adds finite coordinates at the places of a finite set  $\mathcal{P}$  of split places and proves the lattice-point bound of Lemma 9.22, the analogue of Lemma 8.24.

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  $\iota$  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  $F_{\mathfrak{p}}$ ; thus  $Q_{\mathfrak{p}} = N_{\mathfrak{p}}$ , the absolute norm of  $\mathfrak{p}$ , and  $Q_{\mathfrak{p}}$  plays the role of  $Q$  in Subsection 9.1 for  $\mathbb{L} = F_{\mathfrak{p}}$ .

**Definition 9.19.** 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  $(z, \zeta)$  of  $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$  we call  $z$  its *archimedean part* and  $\zeta$  its *finite part*. Let  $\mathcal{O}_{\mathcal{P}} = \mathcal{O}_{K, \mathcal{P}}$  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  $\mathcal{O}_{\mathcal{P}}$  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  $\gamma_{\infty}$  and  $\gamma_f$  are the archimedean part and the finite part of the image of  $\gamma$ . 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 9.20.** Let  $\mathcal{C}_f$  be rectangular and put  $\mathfrak{a}_{\mathcal{C}_f} = \prod_{\mathfrak{p}} \mathfrak{P}_{\mathfrak{p}}^{a_{\mathfrak{p}}} (\iota \mathfrak{P}_{\mathfrak{p}})^{b_{\mathfrak{p}}}$ .

- (a) The elements  $\gamma \in \mathcal{O}_{\mathcal{P}}$  with  $\gamma_f \in \mathcal{C}_f$  form  $\mathfrak{a}_{\mathcal{C}_f}$ , and  $N \mathfrak{a}_{\mathcal{C}_f} = |\mathcal{C}_f|^{-1}$ , so  $\text{covol}((\mathfrak{a}_{\mathcal{C}_f})_{\infty}) = \text{covol}_0 / |\mathcal{C}_f|$ .
- (b) Every coset of  $\mathcal{C}_f$  in  $\mathbb{A}_{\mathcal{P}}$  contains  $\gamma_f$  for some  $\gamma \in \mathcal{O}_{\mathcal{P}}$ .

- (c)  $\mathcal{O}_{\mathcal{P}}$  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  $P_{\mathcal{C}_f}$  is a fundamental parallelepiped of  $(\mathfrak{a}_{\mathcal{C}_f})_{\infty}$ , then  $P_{\mathcal{C}_f} \times \mathcal{C}_f$  is a fundamental domain for  $\mathcal{O}_{\mathcal{P}}$ , of measure  $\text{covol}_0$ .
- (d) For  $h \in \mathbb{R}^c$ , the set  $\mathcal{O}_{\mathcal{P},h} = \{(W_h \gamma_{\infty}, \gamma_f) : \gamma \in \mathcal{O}_{\mathcal{P}}\}$  is again a lattice, with fundamental domain  $W_h P_{\mathcal{C}_f} \times \mathcal{C}_f$  of measure  $\text{covol}_0$ . Put  $H_f = d^{-1} \log |\mathcal{C}_f|$ . Every nonzero vector  $\xi$  of the dual lattice of  $W_h(\mathfrak{a}_{\mathcal{C}_f})_{\infty}$  satisfies  $\prod_w |\xi_w| \geq \mu_f^d$ , where  $\mu_f = 2e^{H_f/2-\ell}$ .

*Proof.* (a) The valuation of  $\gamma_{\mathfrak{p}}$  is the exponent of  $\mathfrak{P}_{\mathfrak{p}}$  in  $\gamma$ , and that of  $(\iota\gamma)_{\mathfrak{p}}$  is the exponent of  $\iota\mathfrak{P}_{\mathfrak{p}}$ . Together with integrality at the other primes,  $\gamma_f \in \mathcal{C}_f$  says exactly that  $\gamma \in \mathfrak{a}_{\mathcal{C}_f}$ . As  $N\mathfrak{P}_{\mathfrak{p}} = N(\iota\mathfrak{P}_{\mathfrak{p}}) = Q_{\mathfrak{p}}$ , we get  $N\mathfrak{a}_{\mathcal{C}_f} = \prod_{\mathfrak{p}} Q_{\mathfrak{p}}^{a_{\mathfrak{p}}+b_{\mathfrak{p}}} = |\mathcal{C}_f|^{-1}$ , and the covolume follows from the covolume formula (8.12).

(b) Choose  $\tilde{a}_{\mathfrak{p}} \leq a_{\mathfrak{p}}$  and  $\tilde{b}_{\mathfrak{p}} \leq b_{\mathfrak{p}}$  such that the given coset lies in  $\tilde{\mathcal{C}}_f = \prod_{\mathfrak{p}} (\varpi_{\mathfrak{p}}^{\tilde{a}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}} \times \varpi_{\mathfrak{p}}^{\tilde{b}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}})$ , and let  $\mathfrak{a}_{\tilde{\mathcal{C}}_f} \supset \mathfrak{a}_{\mathcal{C}_f}$  be the corresponding ideal. The map  $\gamma \mapsto \gamma_f$  induces a homomorphism  $\mathfrak{a}_{\tilde{\mathcal{C}}_f}/\mathfrak{a}_{\mathcal{C}_f} \rightarrow \tilde{\mathcal{C}}_f/\mathcal{C}_f$ . 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  $|\mathfrak{a}_{\tilde{\mathcal{C}}_f}/\mathfrak{a}_{\mathcal{C}_f}| = N\mathfrak{a}_{\mathcal{C}_f}/N\mathfrak{a}_{\tilde{\mathcal{C}}_f}$  [17, 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  $\gamma_f$  for some  $\gamma \in \mathfrak{a}_{\tilde{\mathcal{C}}_f} \subset \mathcal{O}_{\mathcal{P}}$ . No principality is needed.

(c) Given  $(z, \zeta) \in \mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$ , by (b) there is  $\gamma \in \mathcal{O}_{\mathcal{P}}$  with  $\zeta - \gamma_f \in \mathcal{C}_f$ , and then a unique  $\gamma' \in \mathfrak{a}_{\mathcal{C}_f}$  with  $z - (\gamma + \gamma')_{\infty} \in P_{\mathcal{C}_f}$ . If  $(z, \zeta)$  had two such representations, the difference of the two elements of  $\mathcal{O}_{\mathcal{P}}$  would have finite part in  $\mathcal{C}_f$ , hence lie in  $\mathfrak{a}_{\mathcal{C}_f}$  by (a), and then it would vanish because  $P_{\mathcal{C}_f}$  is a fundamental domain. Thus  $P_{\mathcal{C}_f} \times \mathcal{C}_f$  is a fundamental domain, of measure  $(\text{covol}_0/|\mathcal{C}_f|) \cdot |\mathcal{C}_f| = \text{covol}_0$ . Finally  $\mathcal{O}_{\mathcal{P}}$  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  $\gamma \in \mathfrak{a}_{\mathcal{C}_f}$  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  $\mathcal{O}_{\mathcal{P}}$  to  $\mathcal{O}_{\mathcal{P},h}$  and  $P_{\mathcal{C}_f} \times \mathcal{C}_f$  to  $W_h P_{\mathcal{C}_f} \times \mathcal{C}_f$ ; so the first assertion follows from (c). By (a),  $N\mathfrak{a}_{\mathcal{C}_f} = e^{-dH_f}$ , and Lemma 8.22 gives the bound for the dual vectors.  $\square$

Accordingly, the Fourier condition used in this section is

$$(9.21) \quad \varsigma \cdot 2e^{H_f/2-\ell} \geq \log M + 2 \log 5 + 2.$$

**Lemma 9.22.** *Let  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  be admissible with Fourier constants  $(M, \varsigma)$  (Definition 8.29), 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 8.30). 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 (9.21) 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),*

$$(9.23) \quad \sum_{(z, \zeta) \in \mathcal{O}_{\mathcal{P},h} + z_0} \Psi_{\infty}(z) \Psi_f(\zeta) \leq \frac{2}{\text{covol}_0} \int \Psi_{\infty} \int \Psi_f.$$

*Proof.* Group the points by the coset of  $\mathcal{C}_f$  containing their finite part. If two points of  $\mathcal{O}_{\mathcal{P},h} + z_0$  have finite parts in the same coset, their difference comes from an element of  $\mathfrak{a}_{\mathcal{C}_f}$ , by Lemma 9.20(a). So the archimedean parts of the points in one coset form a translate of  $W_h(\mathfrak{a}_{\mathcal{C}_f})_{\infty}$ , or the empty set. By Lemma 8.24, with the dual bound of Lemma 9.20(d) and the Fourier bound for  $\Psi_{\infty}$  of Lemma 8.30, the sum of  $\Psi_{\infty}$  over such a translate is at most  $2|\mathcal{C}_f| \int \Psi_{\infty} / \text{covol}_0$ . The values of  $\Psi_f$  on its finitely many nonzero cosets sum to  $\int \Psi_f / |\mathcal{C}_f|$ .  $\square$

**Lemma 9.24.** *Let  $\alpha \in \mathbb{A}_{\mathcal{P}}$  have coordinates  $(\varpi_{\mathfrak{p}}^{n_{\mathfrak{p}}}, \varpi_{\mathfrak{p}}^{-n_{\mathfrak{p}}})$  with  $n_{\mathfrak{p}} \in \mathbb{Z}$ . If  $\Psi_f$  satisfies the hypotheses of Lemma 9.22 with a rectangular group  $\mathcal{C}_f$ , then  $\Psi_f \circ \alpha$  satisfies them with the rectangular group  $\alpha^{-1}\mathcal{C}_f$ , which gives the same  $H_f$ , and  $\int \Psi_f \circ \alpha = \int \Psi_f$ .*

*Proof.* Multiplication by  $\alpha$  preserves the Haar measure, since at each  $\mathfrak{p}$  it scales the two coordinates by factors of absolute values  $Q_{\mathfrak{p}}^{-n_{\mathfrak{p}}}$  and  $Q_{\mathfrak{p}}^{n_{\mathfrak{p}}}$ . For a rectangular group  $\mathcal{C}_f$  the group  $\alpha^{-1}\mathcal{C}_f$  is rectangular, with exponents  $a_{\mathfrak{p}} - n_{\mathfrak{p}}$  and  $b_{\mathfrak{p}} + n_{\mathfrak{p}}$ , and of the same measure. The function  $\Psi_f \circ \alpha$  is invariant under translation by  $\alpha^{-1}\mathcal{C}_f$  and vanishes outside the images under  $\alpha^{-1}$  of finitely many cosets of  $\mathcal{C}_f$ , which are cosets of  $\alpha^{-1}\mathcal{C}_f$ .  $\square$

**9.3. Class Selection.** This subsection is the analogue of Lemma 8.11 for weighted counts: it selects one ideal class and produces elements of relative norm one with prescribed valuations at the places of  $\mathcal{P}$  (Lemma 9.25).

For  $u \in \mathbb{R}^c$  and  $n = (n_{\mathfrak{p}}) \in \mathbb{Z}^{\mathcal{P}}$  let  $\mathbf{e}(u, n) \in \mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$  have archimedean part the unit-norm displacement  $\mathbf{e}(u)$  of Definition 8.16 and finite part  $(\varpi_{\mathfrak{p}}^{n_{\mathfrak{p}}}, \varpi_{\mathfrak{p}}^{-n_{\mathfrak{p}}})_{\mathfrak{p}}$ .

**Lemma 9.25.** *Let  $\mathcal{N} \subset \mathbb{Z}^{\mathcal{P}}$  be finite, and let  $\mathcal{W}: \mathcal{N} \rightarrow [0, \infty)$  have positive sum. There are a subset  $\mathcal{N}' \subset \mathcal{N}$  with*

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

*an element  $n_0 \in \mathcal{N}'$  with  $\mathcal{W}(n_0) > 0$ , and elements  $\beta_n \in \mathcal{O}_{\mathcal{P}}$ , 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  $\beta_{n_0} \mathcal{O}_K^1$  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  $h_{\text{cap}} h_{\text{rel}}$ . 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 8.11,  $N_{K/F}\beta_n = 1$  and  $\beta_n$  generates the displayed ideal, which is supported on the primes  $\mathfrak{P}_{\mathfrak{p}}, \iota \mathfrak{P}_{\mathfrak{p}}$ ; hence  $\beta_n \in \mathcal{O}_{\mathcal{P}}$ . 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.  $\square$

**9.4. Transfer with Shell Profiles.** This subsection proves Proposition 9.26, the form of the construction used in Section 11. Its proof follows that of Proposition 8.32, with the window and the lattice extended by the finite coordinates of Definition 9.19.

**Proposition 9.26** (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  $\lambda$ , 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 (Definition 9.7) 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  $\mathcal{F}_{\delta,\mathfrak{p}} = \mathcal{F}_{\delta}(g_{\mathfrak{p}})$  be the local functional (Definition 9.3), let  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  be admissible with Fourier constants  $(M, \varsigma)$  (Definition 8.29), and suppose that (9.21) 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  $\theta_j$  be the value of  $\theta$  for  $F_j$ , and put*

$$(9.27) \quad \begin{aligned} \mathcal{M}_{\text{fin},j} = & \frac{1}{d_j} \sum_{\mathfrak{p} \in \mathcal{P}_j} \log \mathcal{F}_{\delta,\mathfrak{p}} - (1/2 - \delta)\ell - C + (1 - \delta) \log 2 + (1 - \theta_j) \log \pi \\ & + (1 - 2\theta_j)J_{\mathbb{R}} + \theta_j J_{\mathbb{C}}; \end{aligned}$$

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  $u(U_j)/|U_j|^{1+\delta} \rightarrow \infty$ .

*Remark 9.28.* Compared with (8.33), the margin (9.27) has no separate term  $-\delta H$ : by (9.12), each  $\mathcal{F}_{\delta,\mathfrak{p}}$  contains the factor  $Q_{\mathfrak{p}}^{-\delta k_{\mathfrak{p}}}$ , and Corollary 9.29 shows that for uniform local types and unweighted shell profiles (9.27) reduces to (8.33).

*Proof of Proposition 9.26.* 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 the *total profile* be

$$f_{\text{tot}} = \prod_v f_{\mathbb{R}} \prod_{j=1}^c g_{\mathbb{C}} \prod_{\mathfrak{p} \in \mathcal{P}} g_{\mathfrak{p}},$$

with one factor for each real place  $v$  of  $F$ , each complex place  $j$  of  $F$  and each  $\mathfrak{p} \in \mathcal{P}$ , let  $V = -\log f_{\text{tot}}$  on the set where  $f_{\text{tot}} > 0$ , and put, for the total mass and the total overlap,

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

Besides the points  $\mathbf{e}(u, n)$  defined before Lemma 9.25, let  $\mathbf{e}(u, n, \omega)$ , for  $\omega = (\omega_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times}$ , have archimedean part  $\mathbf{e}(u)$  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  $f_{\text{tot}}(x) f_{\text{tot}}(x + \mathbf{e}(u, n, \omega)) / I_{\text{tot}}$  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 8.28) and of the endpoint laws (Definition 9.13) of the  $g_{\mathfrak{p}}$ . Its endpoints are  $x$  and  $x + \mathbf{e}(u, n, \omega)$ . Their energies  $V(x)$  and  $V(x + \mathbf{e}(u, n, \omega))$  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 8.31, and at  $\mathfrak{p} \in \mathcal{P}$  the map  $(z, n, \omega) \mapsto (-z - s(n, \omega), n, \omega)$  preserves the endpoint law of  $g_{\mathfrak{p}}$  and carries its first endpoint to minus the second,  $g_{\mathfrak{p}}$  is even, and the energy  $-\log g_{\mathfrak{p}}$  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 8.31. The  $Q_{\mathfrak{p}}$  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  $\chi$  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 8.31,  $\mathbb{P}(\chi = 1) \geq 1/2$  for large  $d$ .

*The set  $\Omega$ .* Let  $\Omega$  be the set of points of  $\mathbb{C}^d \times \mathbb{A}_{\mathcal{P}}$  where  $f_{\text{tot}} > 0$  and  $V \leq d(\bar{m} + \eta)$ ; it plays the role of the window of Definition 8.16. It is a bounded Borel set: the archimedean energies are coercive and bounded below, and the finite part lies in the compact support of  $\prod_{\mathfrak{p}} g_{\mathfrak{p}}$ , on which the finite energies are bounded. It is invariant under rotations of the archimedean coordinates, and, by Lemma 9.8, under  $(x_{\mathfrak{p}}, y_{\mathfrak{p}}) \mapsto (\omega x_{\mathfrak{p}}, \omega' y_{\mathfrak{p}})$  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  $\Phi(u, n) = |\Omega \cap (\Omega - \mathbf{e}(u, n))|$ , 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  $\Omega$  with its translate by any vector whose archimedean part has the moduli of  $\mathbf{e}(u)$  and whose finite part is that of some  $\mathbf{e}(u, n, \omega)$  equals  $\Phi(u, n)$ . Where  $\chi = 1$ , both endpoints lie in  $\Omega$  and

$f_{\text{tot}}(x)f_{\text{tot}}(x + \mathbf{e}(u, n, \omega)) \leq e^{-2d(\bar{m}-\eta)}$ . Integrating over  $x$ ,  $u$  and  $\omega$  and summing over  $n$ , we obtain

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

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

*Class selection and rescaling.* Apply Lemma 9.25 to the finitely many  $n$  with  $\mathcal{W}(n) > 0$ , obtaining  $n_0$ ,  $\mathcal{N}'$  and  $\beta_n$ , and let  $\varpi_0$  be as in that lemma. Put  $\Omega' = \varpi_0^{-1}\Omega$ , where  $\varpi_0$  acts on the finite part. Then  $|\Omega'| = |\Omega|$ , and  $\Omega'$  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  $\beta^{(h)} = (W_h \beta_\infty, \beta_f) \in \mathcal{O}_{\mathcal{P},h}$  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 9.25 and the invariances of  $\Omega$ , as in Lemma 8.17.

*Points and edges.* Let  $\mathfrak{a}_{\mathcal{C}'_f}$  be the ideal attached to  $\mathcal{C}'_f$  in Lemma 9.20. Fix a  $\mathbb{Z}$ -basis of  $(\mathfrak{a}_{\mathcal{C}'_f})_\infty$ , let  $P_{\mathcal{C}'_f}$  be the fundamental parallelepiped that it spans, and for  $y \in [0, 1)^{2d}$  let  $y_{\mathcal{C}'_f} \in P_{\mathcal{C}'_f}$  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  $z_0 = (W_h y_{\mathcal{C}'_f}, \zeta)$ ; these points form the fundamental domain  $W_h P_{\mathcal{C}'_f} \times \mathcal{C}'_f$  of  $\mathcal{O}_{\mathcal{P},h}$  of Lemma 9.20(d). Let  $\mathcal{X}(h, z_0) = (\mathcal{O}_{\mathcal{P},h} + z_0) \cap \Omega'$  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 Definition 8.18; we write  $N$  because  $n$  indexes  $\mathbb{Z}^P$  in this proof), and let  $\mathcal{E}(h, z_0)$  count the pairs  $(x, \beta)$  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  $\mathbf{1}_{\Omega'} \leq e^{pd(\bar{m}+\eta)} (f_{\text{tot}} \circ \varpi_0)^p$  and  $(f_{\text{tot}} \circ \varpi_0)^p$  is the product of an archimedean factor and a function invariant under  $\mathcal{C}'_f$ , Lemmas 9.22 and 9.24 give

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

for all  $(h, z_0)$ . By tiling, for fixed  $h$  the average of  $N(h, z_0)$  over  $(y, \zeta)$  is  $|\Omega'| / \text{covol}_0$ , and the average of  $\mathcal{E}(h, z_0)$  is  $\text{covol}_0^{-1} \sum_{n \in \mathcal{N}'} \sum_{\beta \in \beta_n \mathcal{O}_K^1} \Phi(l(\beta) - h, n)$ . Averaging over  $h \in \Pi^1$  as in Lemma 8.14, the average of  $\mathcal{E}$  becomes

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

Measurability and integrability hold as in Lemma 8.19, since  $\mathcal{E} \leq N^2 \leq N_{\max}^2$ . The argument of that lemma yields a pair  $(h, z_0)$  with  $N = N(h, z_0) > 0$  and

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

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

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

By (8.6) 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  $I_{\text{tot}}/A_{\text{tot}}^{1+\delta} = \exp(bJ_{\mathbb{R}} + cJ_{\mathbb{C}} + \sum_{\mathfrak{p}} \log \mathcal{F}_{\delta, \mathfrak{p}})$ . 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  $0 \neq \gamma \in \mathcal{O}_{\mathcal{P}}$ , whose  $v_0$ -coordinate is nonzero, so

$|U| = N$ . Each counted pair  $(x, \beta)$  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 8.32 (Lemma 8.21),  $u(U) \geq \mathcal{E}/2$ , the ratio  $u(U)/|U|^{1+\delta}$  tends to infinity, and the bound  $u(U) \leq |U|^2/2$  forces  $|U| \rightarrow \infty$ .  $\square$

**9.5. Uniform Local Types.** This subsection shows that Proposition 9.26 contains Proposition 8.32 when the places carry uniform local types. The proof of Theorem 1.1 does not use Corollary 9.29, since the types at 41 are not uniform (Definition 11.2); it applies Proposition 9.26 directly.

**Corollary 9.29** (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  $\lambda$ , 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 8.7). For each  $r \in \mathcal{R}$  fix an integer  $k_r \geq 0$  and weights  $w^{(r)}$  as in Definition 9.7, 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 (8.10). Let  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  be admissible (Definition 8.29) with Fourier constants  $(M, \varsigma)$  satisfying (8.25) with  $\mu = 2e^{H/2-\ell}$ , and put*

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

If  $\inf_j \mathcal{M}_{\mathcal{R}}(\theta_j) > 0$ , where  $\theta_j$  is the value of  $\theta$  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 (8.33).

*Proof.* Apply Proposition 9.26 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  $\mathcal{F}_{\delta,\mathfrak{p}} = \mathcal{F}_{\delta,r}$ . By Lemma 8.8 there are  $d/(e_r f_r)$  places above  $r$ , each with  $Q_{\mathfrak{p}} = r^{f_r}$ , so

$$(9.30) \quad \frac{1}{d} \sum_{\mathfrak{p} \in \mathcal{P}} \log \mathcal{F}_{\delta,\mathfrak{p}} = \sum_{r \in \mathcal{R}} \frac{\log \mathcal{F}_{\delta,r}}{e_r f_r}, \quad H_f = \sum_{r \in \mathcal{R}} \frac{k_r \log r}{e_r} = H.$$

In particular (9.21) coincides with (8.25), whatever the shell weights, and the margin (9.27) of  $K_j/F_j$  equals  $\mathcal{M}_{\mathcal{R}}(\theta_j)$ . For unweighted shell profiles, Lemma 9.11 gives  $\log \mathcal{F}_{\delta,r} = \log(k_r + 1) - \delta k_r f_r \log r$ , and the sum in (9.30) is  $J - \delta H$ .  $\square$

Thus Proposition 9.26 contains Proposition 8.32, and the shell weights replace the term  $J - \delta H$  of (8.33) by  $\sum_r \log \mathcal{F}_{\delta,r}/(e_r f_r)$  without changing the Fourier condition.

## 10. ARCHIMEDEAN PROFILES

In this section we prove that the profiles used in Section 11 are admissible in the sense of Definition 8.29 (Proposition 10.14), and we derive bounds for the functionals  $J_{\mathbb{R}}$  and  $J_{\mathbb{C}}$  (Definition 8.28) that reduce to finite computations with rational data:  $J_{\mathbb{R}}$  in closed form (Lemma 10.4), and a lower bound for  $J_{\mathbb{C}}$  (Corollary 10.26) from a lower bound for the overlap  $I_{\mathbb{C}}$  (Proposition 10.18) and an upper bound for the mass  $A_{\mathbb{C}}$  (Proposition 10.21). Section 11 carries out these computations at  $\delta = 0.043171$ . We use a Gaussian at the compact coordinates, and at the pair coordinates a Student profile multiplied by a positive polynomial.

Throughout,  $0 < \delta < 1$  and  $p = 2/(1 + \delta)$ . We write  $\psi = \Gamma'/\Gamma$  for the digamma function,  $\gamma$  for Euler's constant,  $(x)_n$  for the rising factorial,  $H_n = \sum_{k=1}^n 1/k$  with  $H_0 = 0$  for the harmonic numbers, and  $\text{Beta}(\alpha, \alpha')$  for the beta distribution on  $(0, 1)$  with density proportional to  $t^{\alpha-1}(1-t)^{\alpha'-1}$ . The letters  $s$  and  $a$  (the parameters of Definition 10.1),  $\psi$ ,  $H_n$ , and the auxiliary quantities  $K_n(i, k)$ ,  $D_x(j)$ ,  $E_{rr'}$ ,  $E_{-,n*}$ ,  $G_n$ ,  $R_n$ ,  $\rho$ ,  $\Delta_1$ ,  $\Delta_2$  introduced below are local to this section and to Section 11; they are unrelated to the complex variable  $s$ , the linear forms  $\psi_o$  of Section 5 and the other uses of these letters elsewhere.

**Definition 10.1.** 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  $\beta_{ij}$  with

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

and  $b_i^m$  are the *Bernstein polynomials* of degree  $m$ . We write  $\min \beta$  and  $\max \beta$  for the smallest and largest Bernstein coefficient.

**Lemma 10.2.** *If  $P$  has Bernstein coefficients  $\beta_{ij}$  of degree  $m$ , then  $\min \beta \leq P(t, t') \leq \max \beta$  for  $(t, t') \in [0, 1]^2$ .*

*Proof.* The Bernstein polynomials  $b_i^m$  are nonnegative on  $[0, 1]$  and sum to one there, by the binomial theorem applied to  $(t + (1-t))^m$ . So  $P(t, t')$  is a convex combination of the  $\beta_{ij}$ , with weights  $b_i^m(t) b_j^m(t')$ .  $\square$

From now on,  $g_{\mathbb{C}}$  denotes a Student–Bernstein profile with parameters  $(s, a, P)$ . Section 11 uses

$$s = 1.147487, \quad a = 0.0000181980309901,$$

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

$$(10.3) \quad (\beta_{ij}) = \begin{pmatrix} 1 & 2.5157692640 & 2.8533380109 & 7.1926104676 \\ 2.5157692640 & 4.1154447568 & 4.9424163713 & 8.8954745458 \\ 2.8533380109 & 4.9424163713 & 5.8082616140 & 10.4120890697 \\ 7.1926104676 & 8.8954745458 & 10.4120890697 & 15.3284466977 \end{pmatrix}.$$

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 (8.3) 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 10.18, against the term  $2\delta \log a$  in (10.27), 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 10.6–10.11), which makes rigorous bounds possible, and the polynomial  $P$  couples the two radii.

**10.1. The Gaussian at the Compact Coordinates.** This subsection shows that the Gaussian with the parameter  $a_{\mathbb{R}} = 2p\delta$  is optimal among Gaussians and gives  $J_{\mathbb{R}}$  in closed form (Lemma 10.4).

**Lemma 10.4.** *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*

$$(10.5) \quad J_{\mathbb{R}} = \log(p/2) + \delta \log(a_{\mathbb{R}}/\pi) - a_{\mathbb{R}}/(2p) = \log(p/2) + \delta(\log(a_{\mathbb{R}}/\pi) - 1),$$

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 (8.33), the margin is affine in  $\theta$  with slope  $-\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}$ . This slope depends on the profiles; for ours it is positive (Section 11).

**10.2. The Pair Convolution.** This subsection reduces the overlap  $I_{\mathbb{C}}$  of a Student–Bernstein profile to expectations, under beta laws, of the function  $Q_{AB}$  defined below (Lemma 10.11), and expands  $Q_{AB}$  in a series with controlled remainder (Lemma 10.8).

**Lemma 10.6.** *Let  $\alpha, \alpha' > 0$  with  $A = \alpha + \alpha' - 1 > 0$ , and let  $h \in \mathbb{C}$ . Then*

$$(10.7) \quad \int_{\mathbb{C}} (1 + |z|^2)^{-\alpha} (1 + |z + h|^2)^{-\alpha'} dz = \frac{\pi}{A} \mathbb{E}(1 + T(1 - T)|h|^2)^{-A}, \quad T \sim \text{Beta}(\alpha, \alpha').$$

*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 (10.7) 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 10.8.** *Let  $A, B > 0$ .*

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

$$(10.9) \quad \left| Q_{AB}(y) - \log(1/y) + \frac{\psi(A) + \psi(B) + 2\gamma}{2} \right| \leq \frac{(A + B)y}{2}.$$

(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  $[0, B y / 2]$ . The substitution  $x = y e^{2v}$  gives  $\int_0^\infty (1 + y e^{2v})^{-A} dv = \frac{1}{2} \int_y^\infty (1 + x)^{-A} dx / x$ , 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  $\kappa_A = \int_0^1 (t^{A-1} - 1)(1-t)^{-1} dt = -\psi(A) - \gamma$  [24, 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 [24, 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 [24, 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  $\psi$  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 10.10.** 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  $\eta_0 = 2s - 1$ ,

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

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

**Lemma 10.11.** *Let  $s \geq 1$  and  $a > 0$ . Then*

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

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 10.6 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 (10.9),  $Q_{AB}(y)$  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.  $\square$

**10.3. Admissibility.** This subsection proves the Fourier bound (P5) at the pair coordinates by a contour shift (Lemma 10.13), and with it the admissibility of the profiles (Proposition 10.14). For the Fourier bound we assume that  $P$  has positive Bernstein coefficients  $\beta_{ij}$  of some degree  $m \geq 1$ .

**Definition 10.12.** Let  $\Delta_1$  and  $\Delta_2$  be the forward difference operators in the two indices of  $(\beta_{ij})$ . For  $0 < \rho < 1$ , the width of the complex tube in the proof of Lemma 10.13, 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 10.13.** *Let  $s > 0$ ,  $sp > 1$  and  $a > 0$ , let  $P$  have positive Bernstein coefficients  $\beta_{ij}$  of degree  $m \geq 1$ , let  $0 < \rho < 1$ , and suppose that the tube constant satisfies  $q_0 < 1$ . Then for all  $\xi_1, \xi_2 \in \mathbb{C}$ ,*

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

*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  $\mathcal{Z}(x + iy) = 1 + (x_1 + iy_1)^2 + (x_2 + iy_2)^2$ . Then

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

So the complexified  $t = \mathcal{Z}^{-1}$  lies within  $\omega$  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  $|P(t, t') - P(t_0, t'_0)| \leq q_0 \min \beta \leq q_0 P(t_0, t'_0)$ , the last step by Lemma 10.2. Thus  $P(t, t')$  lies in the right half-plane, and with principal branches,

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

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  $\rho$ , 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  $\xi_1$  and  $\xi_2$  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 10.14.** *Let  $s \geq 1$ ,  $a > 0$ , and let  $P$  have positive Bernstein coefficients  $\beta_{ij}$  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 10.4, and let  $0 < \rho < 1$  with  $q_0 < 1$ . Then  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  is admissible (Definition 8.29) with Fourier constants*

$$(10.15) \quad M = \max\{2, \sqrt{K_{\mathbb{C}}}\}, \quad \varsigma = \min\{1, \varsigma_{\mathbb{C}}\}.$$

*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  $[0, 1]^2$  (Lemma 10.2), and they and all their derivatives are bounded.

(P2) The integrals at the compact coordinates are computed in Lemma 10.4. The mass  $A_{\mathbb{C}}$  is finite because  $sp > 1$  (Proposition 10.21 below), and  $0 < I_{\mathbb{C}} < \infty$  because  $g_{\mathbb{C}} \leq \max \beta t^s t'^s$  and Lemma 10.11 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  $c_{\tau}$ , 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 10.11, 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 (10.9). The same holds for  $w$ .

(P5) By Lemma 8.27 the Gaussian satisfies  $|\widehat{f_{\mathbb{R}}^p}(\xi)| \leq 2e^{-|\xi|} A_{\mathbb{R}} \leq M e^{-\varsigma|\xi|} A_{\mathbb{R}}$ , and by Lemma 10.13 the pair profile satisfies the bound with  $K_{\mathbb{C}} e^{-\varsigma_{\mathbb{C}}(|\xi_1|+|\xi_2|)} \leq M^2 e^{-\varsigma(|\xi_1|+|\xi_2|)}$ .  $\square$

**10.4. A Lower Bound for the Overlap  $I_{\mathbb{C}}$ .** This subsection bounds  $I_{\mathbb{C}}$  from below by finitely many rational terms, a logarithm and one digamma constant (Proposition 10.18).

**Definition 10.16.** 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

$$(10.17) \quad c_s = -2\psi(s) + \psi(2s) + (2s-1)^{-1} - \gamma, \quad y_0 = a/4.$$

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

$$(10.19) \quad A_{ik}B_{jl}y_0^2 < 1, \quad 2\log(4/a) \geq H_{[A_{ik}]-1} + H_{[B_{jl}]-1}, \quad \log(4/a) > 1/2.$$

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

$$(10.20) \quad \frac{I_{\mathbb{C}}}{\pi^2 a^{-2}} \geq \sum_{n=0}^{n_*} a^{2n} \{G_n[\log(1/a) + c_s] + \tilde{G}_n\} - E_{-,n_*},$$

where the remainder term is

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

*Proof.* Start from Lemma 10.11. Since  $y \leq y_0 = a/4 < 1$ , the hypotheses of Lemma 10.8(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 10.8(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 Beta( $\alpha, \alpha'$ ) into 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  $v_{ijkl}$ , 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 10.8(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  $v_{ijkl} > 0$  we discard the remainder, and for crosses with  $v_{ijkl} < 0$  we subtract its upper bound. This proves (10.20).  $\square$

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.

**10.5. An Upper Bound for the Mass  $A_{\mathbb{C}}$ .** This subsection bounds  $A_{\mathbb{C}}$  from above by subdividing  $[0, 1]^2$  and using Bernstein coefficients on each rectangle (Proposition 10.21).

**Proposition 10.21.** *Let  $g_{\mathbb{C}}$  be a Student–Bernstein profile with parameters  $(s, a, P)$  such that  $q_* = sp - 1 > 0$ . Then*

$$(10.22) \quad A_{\mathbb{C}} = \frac{\pi^2}{a^2 q_*^2} \bar{A}_{\mathbb{C}}, \quad \bar{A}_{\mathbb{C}} = \mathbb{E} P(T, T')^p,$$

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

$$(10.23) \quad \text{Mom}_i(l, r) = \int_l^r q_* v^{q_*-1} \left( \frac{v-l}{r-l} \right)^i dv = \frac{q_*}{(r-l)^i} \sum_{j=0}^i \binom{i}{j} (-l)^{i-j} \frac{r^{q_*+j} - l^{q_*+j}}{q_* + j},$$

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

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

Then for every  $N \geq 1$ ,

$$(10.24) \quad \left| \bar{A}_{\mathbb{C}} - \sum_{\mathcal{Q}} \Sigma_{\mathcal{Q}, N} \right| \leq \sum_{\mathcal{Q}} c_{\mathcal{Q}}^p \frac{\binom{p}{N+1} |\rho_{\mathcal{Q}}|^{N+1}}{1 - \rho_{\mathcal{Q}}} M_0(l, r) M_0(l', r').$$

*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 (10.22) since  $sp - 2 = q_* - 1$ . Lemma 10.2, applied on  $\mathcal{Q}$  in the coordinates  $(x, x')$ , gives  $m_{\mathcal{Q}} \leq P \leq M_{\mathcal{Q}}$ , that is,  $|W_{\mathcal{Q}}| \leq \rho_{\mathcal{Q}} < 1$  on  $\mathcal{Q}$ . For  $1 < p < 2$  the binomial coefficients satisfy  $|\binom{p}{k+1}|/|\binom{p}{k}| = |p-k|/(k+1) < 1$  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  $|\binom{p}{N+1}| |\rho_{\mathcal{Q}}|^{N+1}/(1 - \rho_{\mathcal{Q}})$ . 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  $q_* > 0$ .  $\square$

*Remark 10.25.* If  $P$  is symmetric, that is,  $P(t, t') = P(t', t)$ , and both axes are partitioned alike, then the reflection  $(T, T') \mapsto (T', T)$  preserves the density of Proposition 10.21 and maps each rectangle  $\mathcal{Q}$  of the partition to a rectangle  $\mathcal{Q}'$  of the partition, with the same Bernstein coefficients up to transposition, hence the same  $c_{\mathcal{Q}}$  and  $\rho_{\mathcal{Q}}$ . So  $\mathcal{Q}$  and  $\mathcal{Q}'$  contribute equally to the sum and to

the error bound in (10.24), and off-diagonal rectangles may be evaluated once and counted twice, diagonal ones once. Subsection 11.5 describes how the quantities in Proposition 10.21 are evaluated.

**10.6. A Lower Bound for the Functional  $J_{\mathbb{C}}$ .** This subsection combines the two previous ones into the lower bound for  $J_{\mathbb{C}}$  used in Definition 11.5 (Corollary 10.26), and encloses the digamma values that it needs (Lemma 10.28).

**Corollary 10.26.** *Under the hypotheses of Propositions 10.18 and 10.21, let  $Z_*$  be the right side of (10.20) for some  $n_*$ , and suppose  $Z_* > 0$ . If  $\bar{A}_{\mathbb{C}}^* \geq \bar{A}_{\mathbb{C}}$ , then*

$$(10.27) \quad J_{\mathbb{C}} \geq \log Z_* + 2(1 + \delta) \log q_* - 2\delta \log \pi + 2\delta \log a - (1 + \delta) \log \bar{A}_{\mathbb{C}}^*.$$

*Proof.* By Proposition 10.18,  $I_{\mathbb{C}} \geq \pi^2 a^{-2} Z_*$ , and by (10.22),  $A_{\mathbb{C}} \leq \pi^2 a^{-2} q_*^{-2} \bar{A}_{\mathbb{C}}^*$ . Substitute into  $J_{\mathbb{C}} = \log I_{\mathbb{C}} - (1 + \delta) \log A_{\mathbb{C}}$ .  $\square$

Interval evaluation of the right side of (10.27) 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 10.18 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 10.28.** *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 [24, 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.  $\square$

## 11. PROOF OF THEOREM 1.1

We prove Theorem 1.1 by applying Proposition 9.26 to the fields of Theorem 2.46, with the upper bound for the relative zeta value in Theorem 4.2 and the data of Definition 11.1. Propositions 11.6 and 11.7 are verified by computer, in exact rational arithmetic and in outward-rounded interval arithmetic, as described in Subsection 11.5; the other steps are proved in the text. The inequalities between decimals in Propositions 11.6 and 11.7 and in the remarks, and the entries of Tables 10 and 11, are computed by the supplementary program `margin_general.py`, which calls the program `geom241.py` (directory `papers/0.04273/certificates` of [23]) unchanged; the replay records the final margin, and calling `margin_general` with `verbose=True` prints every enclosure and table entry. 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.

**11.1. Parameters and Local Data.** This subsection fixes  $\delta$ ,  $C$ , the archimedean profiles and the shell profiles (Definition 11.1), counts the places that carry shell profiles (Lemma 11.3), and defines the computable lower bound  $\mathcal{M}_*$  for the margin (Definition 11.5).

**Definition 11.1.** The *data* of this section are the following.

- (a)  $\delta = 43171/10^6 = 0.043171$ ,  $p = 2/(1 + \delta) = 2000000/1043171$  and  $C = C_{\text{eff}} = 0.0422764$ ;  $\lambda = 2^{9/4}\sqrt{3615}$  and  $\ell = \log \lambda$ , as in Theorem 2.46.
- (b) At the compact coordinates,  $f_{\mathbb{R}}$  is the Gaussian of Lemma 10.4, with  $f_{\mathbb{R}}^p = e^{-a_{\mathbb{R}}|z|^2}$  and  $a_{\mathbb{R}} = 2p\delta = 172684/1043171 < 1$ .
- (c) At the pair coordinates,  $g_{\mathbb{C}}$  is the Student–Bernstein profile of Definition 10.1 with  $s = 1.147487$ ,  $a = 0.0000181980309901$  and the polynomial  $P$  of degree  $m = 3$  in each variable whose Bernstein coefficients are (10.3). We put  $q_* = sp - 1 = 1251803/1043171$ , as in Proposition 10.21.
- (d) In Definition 10.12 and Lemma 10.13 we take  $\rho = 10^{-3}$ , with the Bernstein coefficients of degree  $m = 3$  of (c). In Proposition 10.21 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 10.18 we take  $n_* = 1$ .
- (e) For  $K \in \mathcal{K}$ ,  $\mathcal{P}$  is the set of places of  $F$  above the selected primes of  $B$  (Definition 4.16). Let  $\mathcal{R} = \{2, 3, 5, 29, 41\}$ . We index the local data by  $r \in \mathcal{R}$ ; the index 41 always refers to the places above the capped prime  $\mathfrak{t}_3$  of  $B$ , the only selected prime above 41, and never to the places above  $\mathfrak{t}_4$ . For  $r \in \mathcal{R}$  let  $k_r$  be the exponent of Table 10. At a place of  $\mathcal{P}$  above  $r \in \{2, 3, 5\}$ ,  $g_r$  is the shell profile with parameters  $(Q_r, k_r, (w_{r,ij}))$ , with the symmetric weight matrices of Appendix A; at a place above 29 or above  $\mathfrak{t}_3$  it is the shell profile with parameters  $(Q_r, k_r, (x_{r,i}x_{r,j}))$ , with the vectors  $x_{29}, x_{41}$  of that appendix. Here  $Q_r = r^4$  for  $r = 2, 29, 41$  and  $Q_r = r^2$  for  $r = 3, 5$ , the order of the residue field of these places (Theorem 2.46). By Lemma 9.11,  $\mathcal{F}_{\delta,r} = \mathcal{F}_{\delta}(g_r)$  depends only on these parameters.

Every parameter written as a finite decimal is exact. We recall  $\theta_* = 65535/131072$  from Theorem 2.46.

**Definition 11.2.** For the places of  $\mathcal{P}$  we put  $(e_r, f_r) = (8, 4), (2, 2), (2, 2), (1, 4)$  and  $(2, 4)$  for  $r = 2, 3, 5, 29, 41$ . For  $r \leq 29$  this is the absolute type of the places of  $\mathcal{P}$  above  $r$ . We call  $(e_{41}, f_{41}) = (2, 4)$  the *effective type at 41*: it is a counting device, not a local type. The places of  $\mathcal{P}$  above 41 are the places above  $\mathfrak{t}_3$ ; they have absolute type  $(1, 4)$ , and the effective type is chosen so that their number is  $d/(e_{41}f_{41})$  and their residue fields have order  $41^{f_{41}}$  (Lemma 11.3).

For  $r \in \{2, 3, 5, 29\}$  these are uniform local types in the sense of Definition 8.7 (Theorem 2.46); because of the index 41, the proof of Theorem 1.1 applies Proposition 9.26 directly rather than Corollary 9.29.

**Lemma 11.3.** Let  $K \in \mathcal{K}$ , let  $d = [F : \mathbb{Q}]$ , let  $\mathcal{P}$ ,  $\mathcal{R}$ ,  $Q_r$ ,  $k_r$  and  $g_r$  be as in Definition 11.1(e), and let  $(e_r, f_r)$  be as in Definition 11.2. For a place  $\mathfrak{p}$  of  $\mathcal{P}$  above  $r$  write  $g_{\mathfrak{p}} = g_r$ ,  $k_{\mathfrak{p}} = k_r$  and  $Q_{\mathfrak{p}} = Q_r$ . Every place of  $\mathcal{P}$  splits in  $K$ . For  $r \in \mathcal{R}$ , the number of places of  $\mathcal{P}$  above  $r$  is  $d/(e_r f_r)$ , and each has residue field of order  $Q_r$ . Consequently

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

*Proof.* By Theorem 2.46, the places of  $F$  above a selected prime  $\mathfrak{p}$  of  $B$  split in  $K$ , and  $\mathfrak{p}$  has a type  $(e, f)$  in  $K/B$ ; so  $K$  has  $[K : B]/(ef) = d/(ef)$  primes above  $\mathfrak{p}$ , and  $F$  has half as many, each with residue field of order  $N\mathfrak{p}^f$ . The types are  $(8, 4)$  at the two primes above 2,  $(2, 2)$  at the two primes above 3 and at the two above 5, and  $(1, 4)$  at  $\mathfrak{t}_1, \mathfrak{t}_2$  above 29 and at  $\mathfrak{t}_3$  above 41. This gives  $2 \cdot d/64 = d/32$  places above 2,  $2 \cdot d/8 = d/4$  above 3, above 5 and above 29, and  $d/8$  above 41 (the

places above  $t_3$ , each with residue field of order  $41^4$ ), which is  $d/(e_r f_r)$  in each case. The places above the uncapped prime  $t_4$ , whose residue degree is a multiple of 4 that may be larger, carry no shell profiles. The second identity follows in the same way, since  $(d/(e_r f_r)) k_r \log r^{f_r}/d = k_r \log r/e_r$ .  $\square$

Since the weights are nonnegative with  $w_{r,00} = 1$  (Appendix A and Proposition 11.6(a)), Lemma 9.11 gives

$$(11.4) \quad \log \mathcal{F}_{\delta,r} = \log \left( Q_r^{-\delta k_r} \sum_{(i,j),(i',j')} w_{r,ij} \mathbf{G}_{(i,j),(i',j')} w_{r,i'j'} \right) - (1 + \delta) \log \sum_{i,j} m_i m_j w_{r,ij}^p,$$

with the shell measures  $m_i$  and the shell Gram matrix  $\mathbf{G}$  of Definition 9.10 for  $Q = Q_r$  and  $k = k_r$ ; for product weights this is (9.15). Table 10 lists the local data.

TABLE 10. Local data. The last two columns give  $\log \mathcal{F}_{\delta,r}/(e_r f_r)$  for the shell profile  $g_r$  and for the unweighted shell profile with parameters  $(Q_r, k_r)$ , rounded to ten decimals. The row 41 refers to the places above  $t_3$ , with the effective type  $(e_{41}, f_{41})$  of Definition 11.2.

| $r$ | $e_r$ | $f_r$ | $Q_r$   | $k_r$ | weights               | $g_r$        | unweighted   |
|-----|-------|-------|---------|-------|-----------------------|--------------|--------------|
| 2   | 8     | 4     | 16      | 7     | $10 \times 10$ matrix | 0.0390649879 | 0.0387991734 |
| 3   | 2     | 2     | 9       | 9     | $10 \times 10$ matrix | 0.3652797033 | 0.3622194132 |
| 5   | 2     | 2     | 25      | 6     | $10 \times 10$ matrix | 0.2795380841 | 0.2780344049 |
| 29  | 1     | 4     | 707281  | 1     | product, 3 shells     | 0.0279173524 | 0.0279172669 |
| 41  | 2     | 4     | 2825761 | 1     | product, 2 shells     | 0.0064840963 | 0.0064840877 |

**Definition 11.5.** Let  $Z_*$  be the right side of (10.20) for the data of Definition 11.1, 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 11.5 (Proposition 11.7(a)), so that  $\bar{A}_{\mathbb{C}} \leq \bar{A}_{\mathbb{C}}^* < 45.4055724808268589$ , the last number being  $\bar{A}_{\mathbb{C}}^*$  rounded up. Let  $J_{\mathbb{C}}^*$  be the right side of (10.27) for these  $Z_*$  and  $\bar{A}_{\mathbb{C}}^*$ , and put

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

**11.2. Finite Checks and Rigorous Bounds.** This subsection states the finite checks (Proposition 11.6) and the interval enclosures (Proposition 11.7) on which the proof rests; both are verified by computer as described in Subsection 11.5.

**Proposition 11.6.** *For the data of Definition 11.1:*

- (a) *all weights  $w_{r,ij}$  ( $r = 2, 3, 5$ ,  $0 \leq i, j \leq 9$ ) and  $x_{r,i}$  ( $r = 29, 41$ ) are positive (Lemma 9.11 needs only  $w_{r,ij} \geq 0$  with  $w_{r,00} > 0$ , which is what the programs assert; strict positivity is checked separately);*
- (b) *the coefficients (10.3) are positive, and the tube constant satisfies  $q_0 < 0.0296$ ;*
- (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  $\rho_{\mathcal{Q}} < 0.3484$ ;*
- (d) *every cross satisfies (10.19).*

*Proof.* These are finite checks, made by the supplementary programs `margin_general.py` and `geom241.py` as described in Subsection 11.5. 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 11.7.** *For the data of Definition 11.1, with  $Z_*$ ,  $J_{\mathbb{C}}^*$  and  $\mathcal{M}_*$  as in Definition 11.5, the following hold.*

- (a) With  $T$  and  $T'$  independent with density  $q_* t^{q_*-1}$  on  $(0, 1)$ ,  
 (11.8)  $45.4055724808268557 < \bar{A}_{\mathbb{C}} = \mathbb{E} P(T, T')^p < 45.4055724808268589$ ,  
 and the right side of (10.24) is less than  $1.6 \cdot 10^{-15}$ .  
 (b) The expression  $Z_*$  satisfies  
 (11.9)  $397.6858754715135886 < Z_* < 397.6858754715135887$ ,  
 and the remainder term satisfies  $E_{-,1} < 2.8 \cdot 10^{-16}$ .  
 (c)  $1.3444924010459460 < J_{\mathbb{C}}^* < 1.3444924010459462$ .  
 (d)  $-0.2125007533361271 < J_{\mathbb{R}} < -0.2125007533361270$ .  
 (e)  $0.7182842240056688517 < \sum_{r \in \mathcal{R}} \log \mathcal{F}_{\delta,r} / (e_r f_r) < 0.7182842240056688518$ .  
 (f) The numbers  $H$  of Lemma 11.3 and  $\ell = \frac{9}{4} \log 2 + \frac{1}{2} \log 3615$  satisfy  
 $15.6026546826373748 < H < 15.6026546826373749$ ,  
 $5.6560047235563094 < \ell < 5.6560047235563095$ .  
 (g)  $\log K_{\mathbb{C}} < 0.0558518577$ ,  $\varsigma_{\mathbb{C}} > 1.4728810283$  and  $\mu = 2e^{H/2-\ell} > 17.0895949922$ .  
 (h)  $0.6247640218687999 < -\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}^* < 0.6247640218688001$ .  
 (i) The lower bound for the margin satisfies

$$(11.10) \quad \mathcal{M}_*(\theta_*) > 0.0000105426526168.$$

*Proof.* The program `margin_general.py` evaluates these quantities in outward-rounded interval arithmetic from the exact data, as described in Subsection 11.5: (a) by Proposition 10.21; (b) from (10.20), with Lemma 10.28 for the digamma values; (c) from (10.27); (d) from (10.5); (e) from (11.4); (f) from the definitions of  $H$  and  $\ell$ ; (g) from Lemma 10.13 and the definition of  $\mu$ ; and (h) and (i) from Definition 11.5, where  $\bar{A}_{\mathbb{C}}^*$  is the upper end of the enclosure computed for (a).  $\square$

The proof of Theorem 1.1 uses Proposition 11.6 and, from Proposition 11.7, 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). Table 11 lists the terms of  $\mathcal{M}_*(\theta_*)$ .

TABLE 11. The terms of  $\mathcal{M}_*(\theta_*)$ , rounded to ten decimals.

| Term                                             | Value         |
|--------------------------------------------------|---------------|
| $\sum_r \log \mathcal{F}_{\delta,r} / (e_r f_r)$ | 0.7182842240  |
| $-(1/2 - \delta)\ell$                            | -2.5838269819 |
| $-C$                                             | -0.0422764000 |
| $(1 - \delta) \log 2$                            | 0.6632233236  |
| $(1 - \theta_*) \log \pi$                        | 0.5723736765  |
| $(1 - 2\theta_*)J_{\mathbb{R}}$                  | -0.0000032425 |
| $\theta_* J_{\mathbb{C}}^*$                      | 0.6722359429  |
| $\mathcal{M}_*(\theta_*)$                        | 0.0000105427  |

**11.3. Conclusion of the Proof.** This subsection verifies the hypotheses of Proposition 9.26 for the fields of Theorem 2.46 and the data of Definition 11.1, and concludes the proof of Theorem 1.1.

**Corollary 11.11.** *The pair  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  of Definition 11.1 is admissible (Definition 8.29) with Fourier constants  $M = 2$  and  $\varsigma = 1$ , and these satisfy (9.21) with  $H_f = H$ .*

*Proof.* Proposition 10.14 applies, since  $s \geq 1$ ,  $a > 0$ ,  $a_{\mathbb{R}} \leq 1$  and  $0 < \rho < 1$ , the Bernstein coefficients (10.3) of degree  $m = 3$  are positive, and  $q_0 < 1$  (Proposition 11.6(b)). It gives the Fourier constants  $M = \max\{2, \sqrt{K_{\mathbb{C}}}\}$  and  $\varsigma = \min\{1, \varsigma_{\mathbb{C}}\}$ . By Proposition 11.7(g),  $K_{\mathbb{C}} < 4$  and

$\varsigma_{\mathbb{C}} > 1$ , so  $M = 2$  and  $\varsigma = 1$ . The right side of (9.21) is then  $\log 2 + 2 \log 5 + 2 < 5.9121$ , while  $\varsigma \cdot 2e^{H_f/2-\ell} = \mu > 17.0895949922$  by Lemma 11.3 and Proposition 11.7(g).  $\square$

**Lemma 11.12.** *For the data of Definition 11.1,  $J_{\mathbb{C}} \geq J_{\mathbb{C}}^*$ . Consequently, for  $\theta_* \leq \theta < 1/2$ , the expression  $\mathcal{M}_{\mathcal{R}}(\theta)$  obtained from  $\mathcal{M}_*(\theta)$  by replacing  $J_{\mathbb{C}}^*$  with  $J_{\mathbb{C}}$  (by Lemma 11.3, at  $\theta = c/d$  for  $F$  it is the margin (9.27) of  $K/F$ , for  $K \in \mathcal{K}$ ; the same expression appears in Corollary 9.29) satisfies*

$$\mathcal{M}_{\mathcal{R}}(\theta) \geq \mathcal{M}_*(\theta) \geq \mathcal{M}_*(\theta_*) > 0.0000105426526168.$$

*Proof.* Corollary 10.26 applies: the hypotheses of Propositions 10.18 and 10.21 hold by Proposition 11.6(c),(d),  $Z_* > 0$  by (11.9), and  $\bar{A}_{\mathbb{C}} \leq \bar{A}_{\mathbb{C}}^*$  by Proposition 11.7(a) and Definition 11.5. 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  $\theta$  with slope  $-\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}^*$ , which is positive by Proposition 11.7(h); so  $\mathcal{M}_*(\theta) \geq \mathcal{M}_*(\theta_*)$  for  $\theta \geq \theta_*$ , and (11.10) 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 2.46, let  $\iota_1$  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  $\theta_n$  be the value of  $\theta$  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 Proposition 9.26 to this sequence, with  $\delta = 0.043171$ , with  $\mathcal{P}_n$  the set  $\mathcal{P}$  of Definition 11.1(e) for  $K^{(n)}$ , the shell profiles  $g_r$  at its places, and the pair  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  of Definition 11.1, and check its hypotheses. By Theorem 2.46, each  $K^{(n)}/F^{(n)}$  satisfies (G1)–(G3) with the common  $\lambda = 2^{9/4} \sqrt{3615}$ , and  $d_n = 2^n \rightarrow \infty$ . By the choice above,  $\log L_{F^{(n)}}(1) \leq d_n C$ . The places of  $\mathcal{P}_n$  split in  $K^{(n)}$  (Lemma 11.3). The weights are as in Definition 9.7, by Proposition 11.6(a), and the parameters of the shell profiles take five values, independent of  $n$ . The pair  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  is admissible, and its Fourier constants satisfy (9.21), by Corollary 11.11, since  $H_f = H$  for every  $n$  by Lemma 11.3. By Lemma 11.3, the margin (9.27) of  $K^{(n)}/F^{(n)}$  with these shell profiles is  $\mathcal{M}_{\mathcal{R}}(\theta_n)$ . Finally,  $\theta_* \leq \theta_n < 1/2$  by Theorem 2.46, so Lemma 11.12 gives  $\mathcal{M}_{\mathcal{R}}(\theta_n) \geq \mathcal{M}_*(\theta_*) > 0$  for all  $n$ .

Proposition 9.26 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  $1 + \delta = 1.043171$ ; these are the sets of Theorem 1.1, indexed by  $n$ . In particular  $u(U_n) \geq |U_n|^{1.043171}$  for all large  $n$ , which gives the last assertion of Theorem 1.1 at the cardinalities  $|U_n|$ .  $\square$

**11.4. Remarks.** This subsection records numerical observations that are not used in the proof.

*Remark 11.13.* The program also encloses the value at  $\theta = 0$  and the zero  $\theta_0$  of the affine function  $\mathcal{M}_*$ :

$$\mathcal{M}_*(0) < -0.312, \quad \theta_0 < 0.49997550.$$

These enclosures are not used in the proof. Since  $\theta = 1/2 - 1/(4N_i)$  by Theorem 2.46, where  $N_i$  is the number of conjugates of  $\iota_1$  in  $\text{Gal}(K/B)$ ,  $N_i \geq 10205$  would suffice, whereas that theorem gives  $N_i \geq 2^{15}$ . At  $\theta = 0$  the margin does not involve  $J_{\mathbb{C}}$  and is negative: with these profiles, mixed signature is essential.

*Remark 11.14.* The following numerical observations are not used in the proof. The proof of Proposition 9.26 needs only some  $\eta > 0$  with  $4\eta$  below the margin; for instance,  $\eta = 10^{-9}$  gives

$$(11.15) \quad \mathcal{M}_*(\theta_*) - 4\eta > 0.0000105386526168 > 0.$$

The value  $\mathcal{M}_*(\theta_*)$  would be absorbed by an increase of  $1.05 \cdot 10^{-5}$  in  $C$ . The general weights at 2, 3 and 5 add  $1.53 \cdot 10^{-5}$  to the margin: with the product weights of the intermediate certificate, optimized at  $\delta = 0.043170$ , the margin at  $\delta = 0.043171$  is about  $-4.8 \cdot 10^{-6}$ . At  $\delta = 0.043172$ , with the same data and the same  $C$ , the evaluation gives about  $-1.33 \cdot 10^{-5}$ .

**11.5. Computations.** This subsection describes how the finite checks and enclosures of Propositions 11.6 and 11.7 are computed.

The program `margin_general.py` calls the function `margin` of `geom241.py` unchanged, and replaces only, for the duration of the call, its routine for the local functional at the places whose weights are given as a matrix, by the routine of `general_windows.py`, which evaluates (9.12) exactly in rational arithmetic, with the real powers  $w_{r,ij}^p$  in interval arithmetic. The routine for product weights, and the routines for Propositions 10.21 and 10.18, Lemma 10.13 and Corollary 10.26, are those of `geom241.py`, which takes three modules of the data archive in `papers/0.0418235/certificates` of [23] unchanged; the members of the archive are checked against their SHA-256 hashes when it is unpacked. In Proposition 10.21 the program uses the symmetry of (10.3): each square off the diagonal is evaluated once and counted twice. It checks the hypotheses listed in Proposition 11.6 (for (c), on the squares on or above the diagonal; the others follow by symmetry), the conditions  $a_{\mathbb{R}} \leq 1$ ,  $\varsigma_{\mathbb{C}} > 1$ ,  $\log K_{\mathbb{C}} < 2 \log 2$  and  $\mu > 10$  (which implies (9.21) for  $M = 2$  and  $\varsigma = 1$ , since  $\log 50 + 2 < 10$ ), and the positivity of the slope in Proposition 11.7(h). It then prints the enclosures stated in this section. The exponents and weights were produced by separate optimization programs; they enter the proof only as the exact data of Appendix A.

Rational quantities are computed exactly; the remaining quantities involve the logarithm, the exponential (also through the real powers  $x^y = \exp(y \log x)$ ), the square root in  $\varsigma_{\mathbb{C}}$ , the constant  $\pi$  and the digamma function, which enters only through Lemma 10.28. These are evaluated in the interval arithmetic of `mpmath` [40], with every operation rounded outward, at a working precision of 80 decimal digits. Hence every computed interval contains the exact value, and the decimals stated above are rigorous bounds.

The replay program `dihedral/reproduce_w3.py` recomputes Propositions 11.6 and 11.7 from the witness file, and also runs `general_windows_check.py` (Remark 9.18).

## 12. OTHER REFINEMENTS, INTERMEDIATE RESULTS AND LIMITS

This section is not needed for Theorem 1.1. It records the refinements behind the intermediate exponents of Table 2, with proofs, and what is known about the limits of the method. Statements about limits are labeled by the kind of evidence behind them. We use the notation of Section 4:  $\mathcal{K}$ ,  $F$ ,  $d$ ,  $\theta$ , the residue degree  $f_K(\mathfrak{p})$  of a prime  $\mathfrak{p}$  of  $B$  in  $K/B$ , the free and selected primes (Definition 4.16),  $g_s$  and  $w$  (Subsection 4.2), and  $\kappa_{\infty}$ ,  $Z_{\text{sel}}$  and  $T_{\text{sel}}$ .

**12.1. The adaptive dichotomy.** The comparison with a fixed field charges each free prime  $\mathfrak{p}$  of  $B$  with its floor  $f_{\mathfrak{p}}^0$ , a lower bound for its residue degree  $f_K(\mathfrak{p})$ . Where  $f_K(\mathfrak{p})$  is not known, an adversary choosing the fields cannot both keep it small and avoid a gain: if  $f_K(\mathfrak{p})$  is small, the places of  $F$  above  $\mathfrak{p}$  that split in  $K$  can carry shell profiles; if it is large, the term of  $\mathfrak{p}$  in  $\zeta_K$  is smaller; and places of  $F$  above  $\mathfrak{p}$  that are inert in  $K$  lower  $L_F$ . This subsection makes the three gains precise (Definition 12.2) and proves that their minimum can be added to the margin (Propositions 12.4 and 12.8). With the bound  $C = 0.04871285$  alone, Proposition 12.8 gave the exponent 1.042925.

**Lemma 12.1.** *Let  $K \in \mathcal{K}$  and  $s > 1$  real. Then*

$$\frac{1}{d} \log L_F(s) = \frac{1}{[K : \mathbb{Q}]} \log \zeta_K(s) - \frac{1}{d} \sum_{\mathfrak{q}} \operatorname{artanh}(N\mathfrak{q}^{-s}),$$

*the sum over the primes  $\mathfrak{q}$  of  $F$  that are inert in  $K$ . For a free prime  $\mathfrak{p}$  of  $B$  with  $f = f_K(\mathfrak{p})$  and  $N = N\mathfrak{p}$ , let  $\rho_K(\mathfrak{p})$  be the proportion of the primes  $\mathfrak{P}$  of  $K$  above  $\mathfrak{p}$  with  $\iota_1 \mathfrak{P} = \mathfrak{P}$ . The primes of  $F$  above  $\mathfrak{p}$  that are inert in  $K$  are the  $\mathfrak{P} \cap F$  with  $\iota_1 \mathfrak{P} = \mathfrak{P}$ ; there are  $\rho_K(\mathfrak{p})d/f$  of them, each of norm  $N^{f/2}$ , and  $\rho_K(\mathfrak{p}) > 0$  only if  $f$  is even. The primes of  $F$  above  $\mathfrak{p}$  that split in  $K$  number  $(1 - \rho_K(\mathfrak{p}))d/(2f)$ , each of norm  $N^f$ .*

*Proof.* At a prime  $\mathfrak{q}$  of  $F$ , with  $x = N\mathfrak{q}^{-s}$ , the Euler factor of  $L_F$  is  $(1-x)^{-1}$  if  $\mathfrak{q}$  splits in  $K$  and  $(1+x)^{-1}$  if  $\mathfrak{q}$  is inert; no finite prime of  $F$  ramifies in  $K$  (G2). The factor of  $\zeta_K$  is  $(1-x)^{-2}$ , respectively  $(1-x^2)^{-1}$ , and  $-\frac{1}{2}\log(1-x^2) + \log(1+x) = \operatorname{artanh} x$ . Since  $[K : \mathbb{Q}] = 2d$  this gives the identity. The prime  $\mathfrak{p}$  is unramified in  $K$ , and  $K/B$  is Galois of degree  $d$ , so there are  $d/f$  primes  $\mathfrak{P}$  above  $\mathfrak{p}$ , with cyclic decomposition groups of order  $f$ . The primes of  $K$  above  $\mathfrak{q} = \mathfrak{P} \cap F$  are  $\mathfrak{P}$  and  $\iota_1 \mathfrak{P}$ . If  $\iota_1 \mathfrak{P} = \mathfrak{P}$ , then  $\mathfrak{q}$  is inert,  $N\mathfrak{q} = N^{f/2}$ , and  $\iota_1$  lies in the cyclic decomposition group of  $\mathfrak{P}$ , so  $f$  is even. If  $\iota_1 \mathfrak{P} \neq \mathfrak{P}$ , then  $\mathfrak{q}$  splits and  $N\mathfrak{q} = N^f$ .  $\square$

**Definition 12.2.** Fix  $\sigma = 1 + \varepsilon \in (1, 2]$ ,  $0 < \delta < 1$ , and floors  $f_{\mathfrak{p}}^0$  for the free primes, that is, integers with  $f_{\mathfrak{p}}^0 \mid f_K(\mathfrak{p})$  for every  $K \in \mathcal{K}$ . For a free prime  $\mathfrak{p}$  with  $N = N\mathfrak{p}$ , and for  $f \in f_{\mathfrak{p}}^0 \cdot 2^{\mathbb{N}}$ , put

$$R_{\mathfrak{p}}(f) = \frac{g_{\sigma}(N^{f_{\mathfrak{p}}^0})}{2f_{\mathfrak{p}}^0} - \frac{g_{\sigma}(N^f)}{2f} \geq 0, \quad I_{\mathfrak{p}}(f) = \begin{cases} \operatorname{artanh}(N^{-f/2})/f & f \text{ even,} \\ 0 & f \text{ odd,} \end{cases}$$

$$S_{\mathfrak{p}}(f) = \frac{1}{2f} \max\left(0, \max_{k \geq 1} (\log(k+1) - \delta k f \log N)\right),$$

with  $R_{\mathfrak{p}}(\infty) = g_{\sigma}(N^{f_{\mathfrak{p}}^0})/(2f_{\mathfrak{p}}^0)$  and  $I_{\mathfrak{p}}(\infty) = S_{\mathfrak{p}}(\infty) = 0$ , and let

$$G_{\mathfrak{p}} = \inf\{R_{\mathfrak{p}}(f) + \rho I_{\mathfrak{p}}(f) + (1 - \rho)S_{\mathfrak{p}}(f)\} \geq 0,$$

over  $f \in f_{\mathfrak{p}}^0 \cdot 2^{\mathbb{N}} \cup \{\infty\}$  and  $\rho \in [0, 1]$ , with  $\rho = 0$  if  $f$  is odd. For  $K \in \mathcal{K}$  we call  $R_{\mathfrak{p}}(f_K(\mathfrak{p})) + \rho_K(\mathfrak{p})I_{\mathfrak{p}}(f_K(\mathfrak{p}))$  the *adaptive credit* of  $\mathfrak{p}$  (it lowers the bound for  $d^{-1} \log L_F(1)$ , Proposition 12.4), and  $(1 - \rho_K(\mathfrak{p}))S_{\mathfrak{p}}(f_K(\mathfrak{p}))$  its *window credit* (it raises the finite term of the margin, Proposition 12.8).

**Lemma 12.3.** In Definition 12.2,  $R_{\mathfrak{p}}(f) \geq 0$ . For every  $K \in \mathcal{K}$  and every free prime  $\mathfrak{p}$ , the sum of the adaptive credit and the window credit of  $\mathfrak{p}$  is at least  $G_{\mathfrak{p}}$ .

*Proof.* The inequality  $R_{\mathfrak{p}}(f) \geq 0$  follows from the monotonicity in Lemma 4.10. Since  $f_K(\mathfrak{p})$  is a power of two divisible by  $f_{\mathfrak{p}}^0$ , and  $\rho_K(\mathfrak{p}) = 0$  if  $f_K(\mathfrak{p})$  is odd (Lemma 12.1), the sum of the adaptive credit and the window credit of  $\mathfrak{p}$  is one of the expressions in the infimum defining  $G_{\mathfrak{p}}$ , and hence at least  $G_{\mathfrak{p}}$ .  $\square$

**Proposition 12.4** (Adaptive ceiling). Fix  $\sigma$ ,  $\delta$  and floors as in Definition 12.2, with the functions  $R_{\mathfrak{p}}$  and  $I_{\mathfrak{p}}$  defined there. Let  $Y_*$  be a real number such that, for every  $K \in \mathcal{K}$  and every finite set  $\mathcal{A}$  of free primes,

$$(12.5) \quad \frac{\log \zeta_K(\sigma)}{[K : \mathbb{Q}]} \leq Y_* - \sum_{\mathfrak{p} \in \mathcal{A}} R_{\mathfrak{p}}(f_K(\mathfrak{p})),$$

let  $Y'_*$  be as in Proposition 4.15, and let  $C' > Y_* + \varepsilon(\kappa_{\infty} + Y'_*)$ . For every finite set  $\mathcal{A}$  of free primes there is an  $m_0$  such that every  $K \in \mathcal{K}$  with  $[K : B] \geq m_0$  satisfies

$$\frac{1}{d} \log L_F(1) < C' - \sum_{\mathfrak{p} \in \mathcal{A}} (R_{\mathfrak{p}}(f_K(\mathfrak{p})) + \rho_K(\mathfrak{p})I_{\mathfrak{p}}(f_K(\mathfrak{p}))),$$

that is,  $C'$  minus the adaptive credits of the primes of  $\mathcal{A}$ .

*Remark 12.6.* The hypothesis (12.5) holds for the termwise bounds of this paper: by (4.11),  $Y_*$  is a sum of terms  $g_{\sigma}(N\mathfrak{p}^{f_{\mathfrak{p}}^0})/(2f_{\mathfrak{p}}^0)$  over the free primes, plus terms for the selected primes, and keeping the exact term  $g_{\sigma}(N^f)/(2f)$  at the primes of  $\mathcal{A}$  lowers it by  $\sum_{\mathfrak{p} \in \mathcal{A}} R_{\mathfrak{p}}$ .

*Proof of Proposition 12.4.* Suppose not, and let  $K^{(j)}$  be fields of strictly increasing degree that violate the inequality. As  $\mathcal{A}$  is finite and the  $f_j(\mathfrak{p}) = f_{K^{(j)}}(\mathfrak{p})$  are powers of two times  $f_{\mathfrak{p}}^0$ , we may pass to a subsequence along which, for each  $\mathfrak{p} \in \mathcal{A}$ , either  $f_j(\mathfrak{p}) = f_{\infty}(\mathfrak{p})$  is constant or  $f_j(\mathfrak{p}) \rightarrow \infty =: f_{\infty}(\mathfrak{p})$ , and  $\rho_j(\mathfrak{p}) = \rho_{K^{(j)}}(\mathfrak{p}) \rightarrow \rho_{\infty}(\mathfrak{p})$ ; and then, as in Lemma 4.13, to one

along which the  $\beta_q$  exist, so that (a) and (b) of that lemma hold. Then  $R_{\mathfrak{p}}(f_j) \rightarrow R_{\mathfrak{p}}(f_{\infty})$  and  $\rho_j I_{\mathfrak{p}}(f_j) \rightarrow \rho_{\infty} I_{\mathfrak{p}}(f_{\infty})$ .

Fix  $s \in (1, 2]$ . By the proof of Lemma 4.8,  $d^{-1} \log L_F(1) \leq d^{-1} \log L_F(s) + \Upsilon(s-1, \theta)$ , and by Lemma 12.1, dropping the inert primes above primes outside  $\mathcal{A}$ ,

$$\frac{1}{d} \log L_F(s) \leq \frac{\log \zeta_K(s)}{[K : \mathbb{Q}]} - \sum_{\mathfrak{p} \in \mathcal{A}} \frac{\rho_K(\mathfrak{p})}{f_K(\mathfrak{p})} \operatorname{artanh}(\mathrm{N}\mathfrak{p}^{-f_K(\mathfrak{p})s/2}).$$

Along the subsequence the right side tends to  $Z(s) - I_{\infty}(s)$ , with  $Z$  as in Lemma 4.13 and

$$I_{\infty}(s) = \sum_{\mathfrak{p} \in \mathcal{A}} \frac{\rho_{\infty}}{f_{\infty}} \operatorname{artanh}(\mathrm{N}\mathfrak{p}^{-f_{\infty}s/2}),$$

a term being zero when  $f_{\infty} = \infty$ . Hence

$$C' - \sum_{\mathfrak{p} \in \mathcal{A}} (R_{\mathfrak{p}}(f_{\infty}) + \rho_{\infty} I_{\mathfrak{p}}(f_{\infty})) \leq Z(s) - I_{\infty}(s) + \sup_{\theta} \Upsilon(s-1, \theta).$$

As  $s \downarrow 1$ ,  $Z(s) \rightarrow Z(1)$ ,  $I_{\infty}(s) \rightarrow \sum_{\mathfrak{p} \in \mathcal{A}} \rho_{\infty} I_{\mathfrak{p}}(f_{\infty})$  and the supremum tends to 0; so  $C' - \sum_{\mathcal{A}} R_{\mathfrak{p}}(f_{\infty}) \leq Z(1)$ . As in the proof of Proposition 4.15,  $Z(1) \leq Z(1+\varepsilon) + \varepsilon(\kappa_{\infty} + Y'_*)$ , and by (12.5) and Lemma 4.13(a),  $Z(1+\varepsilon) \leq Y_* - \sum_{\mathcal{A}} R_{\mathfrak{p}}(f_{\infty})$ . Together,  $C' - \sum_{\mathcal{A}} R_{\mathfrak{p}} \leq Y_* + \varepsilon(\kappa_{\infty} + Y'_*) - \sum_{\mathcal{A}} R_{\mathfrak{p}} < C' - \sum_{\mathcal{A}} R_{\mathfrak{p}}$ , a contradiction.  $\square$

**Lemma 12.7.** *Proposition 9.26 remains true if its hypothesis  $\log L_{F_j}(1) \leq d_j C$  is replaced by  $\log L_{F_j}(1) \leq d_j C_j$ , and  $C$  by  $C_j$  in the margin (9.27).*

*Proof.* In the proof of Proposition 9.26 the hypothesis enters only once, for the field at hand, in the lower bound for the first factor through (8.6). The choice of  $\eta$  and the Chebyshev step depend only on the infimum of the margins and on the finite set of parameters.  $\square$

**Proposition 12.8** (Adaptive margin). *Let  $\mathcal{A}$  be a finite set of free primes, let  $C'$  satisfy the hypotheses of Proposition 12.4, and let  $G_{\mathfrak{p}}$  be as in Definition 12.2. Let  $\mathcal{P}$  and  $\mathcal{R}$  be as in Definition 11.1(e), with the effective types  $(e_r, f_r)$  of Definition 11.2, and for  $r \in \mathcal{R}$  let  $g_r$  be a shell profile with parameters  $(Q_r, k_r, w^{(r)})$ , placed at the places of  $\mathcal{P}$  above  $r$ , where  $Q_r$  and  $k_r$  are those of Table 10 and only the weights  $w^{(r)}$  may differ from those of Definition 11.1. Let  $(f_{\mathbb{R}}, g_{\mathbb{C}})$  be an admissible pair whose Fourier constants satisfy (9.21) with  $H_f = H$ , the number  $H$  of Lemma 11.3. Let  $J_{\mathbb{C}}^* \leq J_{\mathbb{C}}$ , and let  $\mathcal{M}_*(\theta)$  be defined by the formula of Definition 11.5 from these data, with  $C'$  in place of  $C$ . If the slope  $-\log \pi - 2J_{\mathbb{R}} + J_{\mathbb{C}}^*$  of  $\mathcal{M}_*$  in  $\theta$  is positive and  $\mathcal{M}_*(\theta_*) + \sum_{\mathfrak{p} \in \mathcal{A}} G_{\mathfrak{p}} > 0$ , then there are finite sets  $U_j \subset \mathbb{R}^2$  with  $|U_j| \rightarrow \infty$  and  $u(U_j)/|U_j|^{1+\delta} \rightarrow \infty$ .*

*Proof.* Choose  $K_j \in \mathcal{K}$  with  $[K_j : B] \rightarrow \infty$  and  $[K_j : B] \geq m_0$  of Proposition 12.4. For  $\mathfrak{p} \in \mathcal{A}$  write  $f_{K_j} = f_{K_j}(\mathfrak{p})$  for the residue degree of  $\mathfrak{p}$  in  $K_j/B$  (not to be confused with the residue degrees  $f_r$  of the effective types or with the profile  $f_{\mathbb{R}}$ ) and  $\rho_j = \rho_{K_j}(\mathfrak{p})$ , and put  $C_j = C' - \sum_{\mathfrak{p} \in \mathcal{A}} (R_{\mathfrak{p}}(f_{K_j}) + \rho_j I_{\mathfrak{p}}(f_{K_j}))$ , so that  $\log L_{F_j}(1) \leq d_j C_j$ . Let  $\mathcal{P}_j$  consist of the places of  $\mathcal{P}$  for  $K_j$  and, for each  $\mathfrak{p} \in \mathcal{A}$  with  $S_{\mathfrak{p}}(f_{K_j}) > 0$ , of the places of  $F_j$  above  $\mathfrak{p}$  that split in  $K_j$ , with the unweighted shell profile with parameters  $(\mathrm{N}\mathfrak{p}^{f_{K_j}}, k)$ , where  $k$  attains the maximum in  $S_{\mathfrak{p}}(f_{K_j})$ . By Lemma 12.1 these places add the window credit  $(1 - \rho_j) S_{\mathfrak{p}}(f_{K_j})$  to  $d_j^{-1} \sum \log \mathcal{F}_{\delta, \mathfrak{p}}$ . Since  $S_{\mathfrak{p}}(f) = 0$  for large  $f$ , their parameters lie in a finite set. The Fourier condition still holds, because  $H_f$  only increases. By Lemma 11.3 and  $J_{\mathbb{C}} \geq J_{\mathbb{C}}^*$ , the margin of  $K_j/F_j$  is at least  $\mathcal{M}_*(\theta_j) + \sum_{\mathcal{A}} (R_{\mathfrak{p}} + \rho_j I_{\mathfrak{p}} + (1 - \rho_j) S_{\mathfrak{p}}) \geq \mathcal{M}_*(\theta_*) + \sum_{\mathcal{A}} G_{\mathfrak{p}} > 0$ , by the positive slope and Lemma 12.3, and Lemma 12.7 applies.  $\square$

**12.2. A refined Tsfasman–Vlăduț step with one abscissa.** This subsection records the one-abscissa version of Proposition 4.19, combined with the adaptive credits, used for the intermediate exponent 1.043116.

**Proposition 12.9.** *Let  $a \geq 1$  and  $b_{\text{TV}} \geq 0$  satisfy*

$$(12.10) \quad g_1(q) \leq a g_\sigma(q) + b_{\text{TV}} w(q) \quad \text{for every real } q \geq 2.$$

*Then Proposition 12.4, and hence Proposition 12.8, hold with any  $C' > Z_{\text{sel}}(1) + a(Y_* - Z_{\text{sel}}(\sigma)) + b_{\text{TV}}(2\kappa_\infty - T_{\text{sel}})$  in place of the condition  $C' > Y_* + \varepsilon(\kappa_\infty + Y_*)$ .*

*Proof.* In the proof of Proposition 12.4, keep everything up to  $C' - \sum_{\mathcal{A}} R_p(f_\infty) \leq Z(1)$ . Write  $\beta^{\text{free}} = \beta - \beta^{\text{sel}}$  as in the proof of Proposition 4.19. By (12.10), Lemma 4.13(b) and  $b_{\text{TV}} \geq 0$ ,

$$Z(1) = Z_{\text{sel}}(1) + \sum_q \beta_q^{\text{free}} g_1(q) \leq Z_{\text{sel}}(1) + a(Z(\sigma) - Z_{\text{sel}}(\sigma)) + b_{\text{TV}}(2\kappa_\infty - T_{\text{sel}}).$$

By (12.5),  $Z(\sigma) \leq Y_* - \sum_{\mathcal{A}} R_p(f_\infty)$ , and since  $a \geq 1$  and  $R \geq 0$  (Lemma 12.3),  $a \sum_{\mathcal{A}} R \geq \sum_{\mathcal{A}} R$ . So  $C' - \sum_{\mathcal{A}} R \leq Z_{\text{sel}}(1) + a(Y_* - Z_{\text{sel}}(\sigma)) + b_{\text{TV}}(2\kappa_\infty - T_{\text{sel}}) - \sum_{\mathcal{A}} R$ , a contradiction. The bound  $Y'_*$  is not needed.  $\square$

*Remark 12.11.* For  $q \geq q_{\min} = 41^4$ , condition (12.10) follows from  $h(x) \geq 0$  for  $x = \log q$ , where  $h(x) = ae^{-\varepsilon x} + 2b_{\text{TV}}x(1 - e^{-x}) - 1 - 2e^{-x}$ , by  $g_1(q) \leq 1/(q-1)$ ,  $g_\sigma(q) \geq q^{-\sigma}$ ,  $w(q) \geq 2 \log q/(q+1)$ ,  $q/(q+1) \geq 1 - 1/q$  and  $q/(q-1) \leq 1 + 2/q$ ; the program `dihedral/lptv.py` checks  $h \geq 0$  in Arb on cells, with bisection near the minimum, and in a closed form, and checks (12.10) directly on 5950 geometric cells of  $[2, 2q_{\min}]$ . Proposition 4.19 with  $n = 1$  and  $c_1 = a$  is this step without the adaptive credits; with several abscissae and coefficients of both signs it gains  $1.18 \cdot 10^{-4}$  in  $C$  on the same data.

**12.3. Intermediate results.** This subsection lists how the intermediate exponents of Table 2 were obtained, as special cases of the results above. Each has a witness file and a replay program in the directory `certificates` of [23].

- (1) 1.042925: Proposition 12.8 with  $C' = 0.04871285$ , the floors relative to  $E$  of Remark 4.36,  $\sigma = 301/300$ , and  $\mathcal{A}$  the free primes of norm at most  $X = 1.2 \cdot 10^7$  (`reproduce_adaptive.py`; the values of  $\sigma$  and  $X$  are in the witness file `witness_0.042925.json`).
- (2) 1.042965: the census of Proposition 5.12 up to  $10^{12}$  relative to  $E$ , which raises the floors of the detected primes of vector 0 from 1 to 2 (`reproduce_census.py`).
- (3) 1.043113 to 1.043124: Lemma 5.13 for the subspace  $W = \langle \psi_{10}, \psi_{23} \rangle \subset W''$  in place of  $W''$  (Remark 5.15), whose nonzero elements  $\psi_{10}, \psi_{23}, \psi_{24}$  are all of dihedral type, so that  $[E_W : \mathbb{Q}] = 2048$  and  $\zeta_{E_W}$  is  $\zeta_E$  times the squares of the 192  $L$ -functions of these three forms; with the census relative to  $E_W$  up to  $8.5 \cdot 10^{14}$ , and with Propositions 4.15, 12.9 and 4.19 in turn (`dihedral/reproduce_dihedral.py`). One review found that an earlier version of this step had credited the thirteen inert primes of vector 0 (Lemma 5.19) twice; the corrected value is in the table.
- (4) 1.043152: Lemma 5.13 for the subspace  $W' = \langle \psi_{10}, \psi_{23}, \psi_{19} \rangle \subset W''$  (Remark 5.15), whose seven nonzero elements are five forms of dihedral type and  $\psi_{19} + \psi_{23}, \psi_{19} + \psi_{24}$  of rank 4;  $[E_{W'} : \mathbb{Q}] = 4096$ , with 32  $L$ -functions of degree 8 (`dihedral/reproduce_w3.py`).

**12.4. Limits.** This subsection records what is known about how far the method can go, with the kind of evidence for each statement. The margin decreases by about 23.8 per unit of  $\delta$  and by 1 per unit of  $C$ , so  $2.38 \cdot 10^{-5}$  in  $C$  corresponds to  $10^{-6}$  in  $\delta$ .

*The next step (computation).* With general shell weights and profiles optimized at  $\delta = 0.043172$ , the margin is positive only if  $C \leq 0.0422631$ . The repository contains, unused by any witness, the census relative to  $E_{W''}$  extended to the limit  $2^{50} \approx 1.13 \cdot 10^{15}$  of the program `census_kv4.c`, and 35 further abscissae. With both the linear programme of Section 7 reaches only about 0.0422638, about  $7 \cdot 10^{-7}$  short.

*More dihedral forms (proved).* By Lemma 5.8, every space properly containing  $W''$  contains a form whose polar form has rank at least 6, whose irreducible representations have dimension at least

8 and whose  $L$ -functions have degree at least 16 over  $\mathbb{Q}$ , with conductors around  $10^{40}$ . So  $W''$  is the end of this route. The remaining part of  $C_{\text{eff}} - Z_{\text{sel}}(1) \approx 6.1 \cdot 10^{-4}$  comes from the primes of vector 0 in  $\ker W''$  that the census does not reach; the census gains only like the logarithm of its range.

*This design (proved, given the margin formula; numerical for the profiles).* By Remark 4.37, no bound of the kind of Proposition 4.19 is below  $Z_{\text{sel}}(1) = 0.0416685$ . With  $C = Z_{\text{sel}}(1)$  and profiles optimized by our programs, the margin is about  $+3.9 \cdot 10^{-4}$  at  $\delta = 0.04318$  and  $-8.8 \cdot 10^{-5}$  at  $\delta = 0.04320$ . So for this tower, these local types and this margin formula, the method cannot go beyond about  $\delta = 0.043196$ ; this assumes that the profile optimization is close to optimal.

*A fourth cap (evidence).* One more  $C_4$  cap would be worth about  $2.9 \cdot 10^{-4}$  in  $\delta$ , but it raises the value of the Golod–Shafarevich function at its minimum from  $-0.00211$  to  $+0.00288$ , so Proposition 2.43 no longer applies. Screens of weighted versions of the Golod–Shafarevich argument, of the index-two subgroups of  $G_B$ , and of further overlaps between the local modules did not recover the deficit. These are limits of the present arguments, not proofs that such a tower is finite.

*A larger conjugacy class (conditional).* The proof uses  $\theta \geq \theta_* = 1/2 - 2^{-17}$ , from the class of  $\iota_1$  in  $\overline{G}_B$ , of size  $2^{15}$  (Lemma 2.30(c)). A class of size  $2^{16}$  in a suitable quotient would give  $\theta \geq 1/2 - 2^{-18}$  and add about  $2.4 \cdot 10^{-6}$  to the margin; with the bound  $C \leq 0.04226506$ , which `signed3.py` certifies for  $E_{W''}$  with the census to  $8.5 \cdot 10^{14}$  and 36 abscissae (not packaged as a witness), this would give the exponent 1.043172. An argument for such a class, by an agent run of the Muse Spark system, is recorded in the directory `research/2026-10-muse-involution-class` of [23]. It has been checked only inside that run and is not used here.

## APPENDIX A. THE SHELL WEIGHTS

This appendix lists the exact weights of the shell profiles of Definition 11.1. At the places above 2, 3 and 5 the weights  $w_{r,ij}$ ,  $0 \leq i, j \leq 9$ , form symmetric matrices with  $w_{r,00} = 1$ ; every entry is a finite decimal with at most 16 significant digits, and the tables give each entry with  $i \leq j$  exactly. All entries are positive. At the places above 29 and above  $t_3$  the weights are  $w_{r,ij} = x_{r,i}x_{r,j}$  with

$$x_{29} = \left(1, \frac{13276052}{35795829844961}, \frac{3}{23203238073907}\right), \quad x_{41} = \left(1, \frac{7308532}{98816567518131}\right),$$

where, as everywhere in Definition 11.1(e), the index 41 refers to the places above the capped prime  $t_3$  (so  $x_{41}$  gives the weights there), and  $x_{r,i} = 0$  for larger  $i$ . The same data, as fractions, are in the witness file `dihedral/witness_0.043171.json`.

Table 12: The weights  $w_{2,ij}$ ,  $i \leq j$ , at the places above 2 ( $w_{2,00} = 1$ ).

| $(i, j)$ | $w_{2,ij}$                         | $(i, j)$ | $w_{2,ij}$                         | $(i, j)$ | $w_{2,ij}$                         |
|----------|------------------------------------|----------|------------------------------------|----------|------------------------------------|
| (0, 1)   | $4.716542764049956 \cdot 10^{-2}$  | (0, 2)   | $2.017700255868174 \cdot 10^{-3}$  | (0, 3)   | $8.7171631193548 \cdot 10^{-5}$    |
| (0, 4)   | $3.832741639457883 \cdot 10^{-6}$  | (0, 5)   | $1.713366666101093 \cdot 10^{-7}$  | (0, 6)   | $7.769825719821233 \cdot 10^{-9}$  |
| (0, 7)   | $3.566175278275845 \cdot 10^{-10}$ | (0, 8)   | $1.653239008386876 \cdot 10^{-11}$ | (0, 9)   | $7.722733350095041 \cdot 10^{-13}$ |
| (1, 1)   | $1.645028460654781 \cdot 10^{-3}$  | (1, 2)   | $6.071119236152628 \cdot 10^{-5}$  | (1, 3)   | $2.426182995561566 \cdot 10^{-6}$  |
| (1, 4)   | $1.021871969093163 \cdot 10^{-7}$  | (1, 5)   | $4.459640799339901 \cdot 10^{-9}$  | (1, 6)   | $1.995577896308062 \cdot 10^{-10}$ |
| (1, 7)   | $9.094119149275457 \cdot 10^{-12}$ | (1, 8)   | $4.201290473175303 \cdot 10^{-13}$ | (1, 9)   | $1.960291337481996 \cdot 10^{-14}$ |
| (2, 2)   | $2.030248259387722 \cdot 10^{-6}$  | (2, 3)   | $7.586231846572196 \cdot 10^{-8}$  | (2, 4)   | $3.051872880103719 \cdot 10^{-9}$  |
| (2, 5)   | $1.290998345568711 \cdot 10^{-10}$ | (2, 6)   | $5.660201090012336 \cdot 10^{-12}$ | (2, 7)   | $2.552979516714002 \cdot 10^{-13}$ |
| (2, 8)   | $1.168305153494076 \cdot 10^{-14}$ | (2, 9)   | $5.446327951003349 \cdot 10^{-16}$ | (3, 3)   | $2.681557347389803 \cdot 10^{-9}$  |
| (3, 4)   | $1.032328123582729 \cdot 10^{-10}$ | (3, 5)   | $4.248644257771646 \cdot 10^{-12}$ | (3, 6)   | $1.860469882653559 \cdot 10^{-13}$ |
| (3, 7)   | $8.253317346679757 \cdot 10^{-15}$ | (3, 8)   | $3.833900332458716 \cdot 10^{-16}$ | (3, 9)   | $1.906569808981989 \cdot 10^{-17}$ |
| (4, 4)   | $3.864148721154686 \cdot 10^{-12}$ | (4, 5)   | $1.608170600300334 \cdot 10^{-13}$ | (4, 6)   | $6.85644020094591 \cdot 10^{-15}$  |
| (4, 7)   | $3.153691455483686 \cdot 10^{-16}$ | (4, 8)   | $1.612575910723441 \cdot 10^{-17}$ | (4, 9)   | $7.382210403240122 \cdot 10^{-19}$ |
| (5, 5)   | $6.485650665137407 \cdot 10^{-15}$ | (5, 6)   | $2.902537221169398 \cdot 10^{-16}$ | (5, 7)   | $1.491950097494088 \cdot 10^{-17}$ |
| (5, 8)   | $6.758337574060917 \cdot 10^{-19}$ | (5, 9)   | $3.012045905428616 \cdot 10^{-20}$ | (6, 6)   | $1.457803752350815 \cdot 10^{-17}$ |
| (6, 7)   | $6.507195266639767 \cdot 10^{-19}$ | (6, 8)   | $2.864515429264146 \cdot 10^{-20}$ | (6, 9)   | $1.268794096264845 \cdot 10^{-21}$ |
| (7, 7)   | $2.820869821976192 \cdot 10^{-20}$ | (7, 8)   | $1.235370551054681 \cdot 10^{-21}$ | (7, 9)   | $5.450041852512307 \cdot 10^{-23}$ |

| $(i, j)$ | $w_{2,ij}$                         | $(i, j)$ | $w_{2,ij}$                         | $(i, j)$ | $w_{2,ij}$                         |
|----------|------------------------------------|----------|------------------------------------|----------|------------------------------------|
| (8, 8)   | $5.391075352742425 \cdot 10^{-23}$ | (8, 9)   | $2.370514582838326 \cdot 10^{-24}$ | (9, 9)   | $1.039240934676101 \cdot 10^{-25}$ |

Table 13: The weights  $w_{3,ij}$ ,  $i \leq j$ , at the places above 3 ( $w_{3,00} = 1$ ).

| $(i, j)$ | $w_{3,ij}$                         | $(i, j)$ | $w_{3,ij}$                         | $(i, j)$ | $w_{3,ij}$                         |
|----------|------------------------------------|----------|------------------------------------|----------|------------------------------------|
| (0, 1)   | $8.732208116272003 \cdot 10^{-2}$  | (0, 2)   | $7.115134059890987 \cdot 10^{-3}$  | (0, 3)   | $5.833874403583207 \cdot 10^{-4}$  |
| (0, 4)   | $4.842476742530829 \cdot 10^{-5}$  | (0, 5)   | $4.069175634869996 \cdot 10^{-6}$  | (0, 6)   | $3.45742827708316 \cdot 10^{-7}$   |
| (0, 7)   | $2.966191388483711 \cdot 10^{-8}$  | (0, 8)   | $2.565638229624465 \cdot 10^{-9}$  | (0, 9)   | $2.231095385027424 \cdot 10^{-10}$ |
| (1, 1)   | $5.953349622659513 \cdot 10^{-3}$  | (1, 2)   | $4.278035393286869 \cdot 10^{-4}$  | (1, 3)   | $3.269646189416048 \cdot 10^{-5}$  |
| (1, 4)   | $2.603831131537329 \cdot 10^{-6}$  | (1, 5)   | $2.133831899297518 \cdot 10^{-7}$  | (1, 6)   | $1.785504266459421 \cdot 10^{-8}$  |
| (1, 7)   | $1.517691095277542 \cdot 10^{-9}$  | (1, 8)   | $1.305661643629569 \cdot 10^{-10}$ | (1, 9)   | $1.132535432833965 \cdot 10^{-11}$ |
| (2, 2)   | $2.831402423526531 \cdot 10^{-5}$  | (2, 3)   | $2.045207095307688 \cdot 10^{-6}$  | (2, 4)   | $1.565598206260394 \cdot 10^{-7}$  |
| (2, 5)   | $1.247740007451327 \cdot 10^{-8}$  | (2, 6)   | $1.023702704344853 \cdot 10^{-9}$  | (2, 7)   | $8.581405731463887 \cdot 10^{-11}$ |
| (2, 8)   | $7.311032723102253 \cdot 10^{-12}$ | (2, 9)   | $6.302112093253326 \cdot 10^{-13}$ | (3, 3)   | $1.412064004229235 \cdot 10^{-7}$  |
| (3, 4)   | $1.042850254440393 \cdot 10^{-8}$  | (3, 5)   | $8.080622597627616 \cdot 10^{-10}$ | (3, 6)   | $6.486521877137696 \cdot 10^{-11}$ |
| (3, 7)   | $5.353973770335096 \cdot 10^{-12}$ | (3, 8)   | $4.532520020710062 \cdot 10^{-13}$ | (3, 9)   | $3.8751041544201 \cdot 10^{-14}$   |
| (4, 4)   | $7.462419427047034 \cdot 10^{-10}$ | (4, 5)   | $5.628236254292794 \cdot 10^{-11}$ | (4, 6)   | $4.443872035077034 \cdot 10^{-12}$ |
| (4, 7)   | $3.680564919377915 \cdot 10^{-13}$ | (4, 8)   | $3.079319637140479 \cdot 10^{-14}$ | (4, 9)   | $2.66856917128071 \cdot 10^{-15}$  |
| (5, 5)   | $4.179296801200473 \cdot 10^{-12}$ | (5, 6)   | $3.340076093096409 \cdot 10^{-13}$ | (5, 7)   | $2.717184103595908 \cdot 10^{-14}$ |
| (5, 8)   | $2.329757724566259 \cdot 10^{-15}$ | (5, 9)   | $2.169192539459492 \cdot 10^{-16}$ | (6, 6)   | $2.612625415806716 \cdot 10^{-14}$ |
| (6, 7)   | $2.190302021582062 \cdot 10^{-15}$ | (6, 8)   | $2.037467307219834 \cdot 10^{-16}$ | (6, 9)   | $1.751359516378403 \cdot 10^{-17}$ |
| (7, 7)   | $1.99821161009703 \cdot 10^{-16}$  | (7, 8)   | $1.696715317716563 \cdot 10^{-17}$ | (7, 9)   | $1.403489307168764 \cdot 10^{-18}$ |
| (8, 8)   | $1.384779695474179 \cdot 10^{-18}$ | (8, 9)   | $1.136784496999098 \cdot 10^{-19}$ | (9, 9)   | $9.29451613262518 \cdot 10^{-21}$  |

Table 14: The weights  $w_{5,ij}$ ,  $i \leq j$ , at the places above 5 ( $w_{5,00} = 1$ ).

| $(i, j)$ | $w_{5,ij}$                         | $(i, j)$ | $w_{5,ij}$                         | $(i, j)$ | $w_{5,ij}$                         |
|----------|------------------------------------|----------|------------------------------------|----------|------------------------------------|
| (0, 1)   | $2.82007539198962 \cdot 10^{-2}$   | (0, 2)   | $7.2979370292182 \cdot 10^{-4}$    | (0, 3)   | $1.921274651708653 \cdot 10^{-5}$  |
| (0, 4)   | $5.173699948390579 \cdot 10^{-7}$  | (0, 5)   | $1.421330341885401 \cdot 10^{-8}$  | (0, 6)   | $3.969840639942114 \cdot 10^{-10}$ |
| (0, 7)   | $1.1238039081556 \cdot 10^{-11}$   | (0, 8)   | $3.216049593941682 \cdot 10^{-13}$ | (0, 9)   | $9.281364615409621 \cdot 10^{-15}$ |
| (1, 1)   | $5.676221659347654 \cdot 10^{-4}$  | (1, 2)   | $1.250567753398034 \cdot 10^{-5}$  | (1, 3)   | $3.032884111737997 \cdot 10^{-7}$  |
| (1, 4)   | $7.821415458906757 \cdot 10^{-9}$  | (1, 5)   | $2.10008166964845 \cdot 10^{-10}$  | (1, 6)   | $5.796606717496382 \cdot 10^{-12}$ |
| (1, 7)   | $1.631590798533015 \cdot 10^{-13}$ | (1, 8)   | $4.658573239308564 \cdot 10^{-15}$ | (1, 9)   | $1.343966520432494 \cdot 10^{-16}$ |
| (2, 2)   | $2.469786567108323 \cdot 10^{-7}$  | (2, 3)   | $5.558766387089918 \cdot 10^{-9}$  | (2, 4)   | $1.363172114626402 \cdot 10^{-10}$ |
| (2, 5)   | $3.540359251000735 \cdot 10^{-12}$ | (2, 6)   | $9.589296275579796 \cdot 10^{-14}$ | (2, 7)   | $2.682343561104813 \cdot 10^{-15}$ |
| (2, 8)   | $7.585792459840756 \cdot 10^{-17}$ | (2, 9)   | $2.232780038099979 \cdot 10^{-18}$ | (3, 3)   | $1.174065143504555 \cdot 10^{-10}$ |
| (3, 4)   | $2.740552896947683 \cdot 10^{-12}$ | (3, 5)   | $6.992141327672552 \cdot 10^{-14}$ | (3, 6)   | $1.912331597280511 \cdot 10^{-15}$ |
| (3, 7)   | $5.245190160086881 \cdot 10^{-17}$ | (3, 8)   | $1.59952722788565 \cdot 10^{-18}$  | (3, 9)   | $4.832345916905165 \cdot 10^{-20}$ |
| (4, 4)   | $6.313542604776013 \cdot 10^{-14}$ | (4, 5)   | $1.645215011520643 \cdot 10^{-15}$ | (4, 6)   | $4.34477808086021 \cdot 10^{-17}$  |
| (4, 7)   | $1.34845993090695 \cdot 10^{-18}$  | (4, 8)   | $4.12144190632597 \cdot 10^{-20}$  | (4, 9)   | $1.142732634506229 \cdot 10^{-21}$ |
| (5, 5)   | $4.115344104070877 \cdot 10^{-17}$ | (5, 6)   | $1.259895127133043 \cdot 10^{-18}$ | (5, 7)   | $3.844437520964445 \cdot 10^{-20}$ |
| (5, 8)   | $1.052643039867518 \cdot 10^{-21}$ | (5, 9)   | $2.88587201206231 \cdot 10^{-23}$  | (6, 6)   | $3.766542905632356 \cdot 10^{-20}$ |
| (6, 7)   | $1.01675396793153 \cdot 10^{-21}$  | (6, 8)   | $2.756672564009575 \cdot 10^{-23}$ | (6, 9)   | $7.521881692941772 \cdot 10^{-25}$ |
| (7, 7)   | $2.718748510906178 \cdot 10^{-23}$ | (7, 8)   | $7.344353409675722 \cdot 10^{-25}$ | (7, 9)   | $1.997034421039592 \cdot 10^{-26}$ |
| (8, 8)   | $1.977978299668902 \cdot 10^{-26}$ | (8, 9)   | $5.363188536575443 \cdot 10^{-28}$ | (9, 9)   | $1.450559362987812 \cdot 10^{-29}$ |

## APPENDIX B. DEPENDENCY INDEX

For each numbered statement, this index lists the numbered statements that it or its proof cites (“uses”) and the statements whose proofs cite it (“used by”). A citation of an equation inside a statement counts as a citation of the statement; references that only point ahead, or say where a statement is used, are not counted. The index is generated from the sources by `tools/depgraph.py`,

so it records the citations made in the text: a use that is not cited by number does not appear. Figure 1 shows the main part of this graph.

| statement  | uses                                                                                                      | used by                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Thm. 1.1   | Thm. 4.2, Def. 11.1, Prop. 11.6,<br>Cor. 11.11, Lem. 11.12, Lem. 11.3,<br>Def. 9.7, Prop. 9.26, Thm. 2.46 | –                                                                                 |
| Def. 2.1   | –                                                                                                         | Lem. 2.9                                                                          |
| Thm. 2.2   | –                                                                                                         | Rem. 2.3, Lem. 2.9, Lem. 2.38, Lem. 2.39                                          |
| Rem. 2.3   | Thm. 2.2                                                                                                  | –                                                                                 |
| Lem. 2.5   | –                                                                                                         | Lem. 2.11, Lem. 2.14, Cor. 3.11, Def. 4.16                                        |
| Def. 2.7   | –                                                                                                         | –                                                                                 |
| Lem. 2.8   | –                                                                                                         | Lem. 2.9, Def. 2.13, Lem. 2.14, Lem. 2.19,<br>Lem. 2.24, Lem. 2.39, Lem. 3.5      |
| Lem. 2.9   | Def. 2.1, Thm. 2.2, Lem. 2.8                                                                              | Rem. 2.10, Def. 2.13, Lem. 2.25,<br>Lem. 2.39, Lem. 2.42, Thm. 2.46               |
| Rem. 2.10  | Lem. 2.9                                                                                                  | –                                                                                 |
| Lem. 2.11  | Lem. 2.5                                                                                                  | Lem. 2.20, Lem. 2.24, Lem. 3.2                                                    |
| Def. 2.12  | –                                                                                                         | –                                                                                 |
| Def. 2.13  | Lem. 2.8, Lem. 2.9                                                                                        | Thm. 2.46, Prop. 3.4, Def. 4.16                                                   |
| Lem. 2.14  | Lem. 2.5, Lem. 2.8                                                                                        | Lem. 2.30                                                                         |
| Lem. 2.17  | –                                                                                                         | Lem. 2.19                                                                         |
| Def. 2.18  | –                                                                                                         | –                                                                                 |
| Lem. 2.19  | Lem. 2.17, Lem. 2.8                                                                                       | Lem. 2.20, Cor. 2.21, Rem. 2.22,<br>Lem. 2.29                                     |
| Lem. 2.20  | Lem. 2.11, Lem. 2.19                                                                                      | Cor. 2.21, Rem. 2.22, Lem. 2.25                                                   |
| Cor. 2.21  | Lem. 2.20, Lem. 2.19                                                                                      | –                                                                                 |
| Rem. 2.22  | Lem. 2.20, Lem. 2.19                                                                                      | –                                                                                 |
| Def. 2.23  | –                                                                                                         | Lem. 2.24, Lem. 2.30, Lem. 3.2, Def. 4.1                                          |
| Lem. 2.24  | Def. 2.23, Lem. 2.11, Lem. 2.8                                                                            | Lem. 2.25, Lem. 3.2                                                               |
| Lem. 2.25  | Lem. 2.24, Lem. 2.20, Lem. 2.9                                                                            | Lem. 2.27, Lem. 2.29, Lem. 2.30,<br>Prop. 2.43, Rem. 2.47, Lem. 4.33,<br>Lem. 5.5 |
| Def. 2.26  | –                                                                                                         | –                                                                                 |
| Lem. 2.27  | Lem. 2.25                                                                                                 | Lem. 2.29, Lem. 2.30                                                              |
| Lem. 2.29  | Lem. 2.25, Lem. 2.27, Lem. 2.19                                                                           | Lem. 2.30, Lem. 4.33, Lem. 4.34,<br>Lem. 5.4                                      |
| Lem. 2.30  | Def. 2.23, Lem. 2.25, Lem. 2.27,<br>Lem. 2.29, Lem. 2.14                                                  | Prop. 2.43, Thm. 2.46, Rem. 2.47                                                  |
| Lem. 2.32  | –                                                                                                         | Prop. 2.43                                                                        |
| Def. 2.34  | –                                                                                                         | –                                                                                 |
| Lem. 2.35  | –                                                                                                         | –                                                                                 |
| Lem. 2.36  | –                                                                                                         | Lem. 2.38, Prop. 2.43                                                             |
| Def. 2.37  | –                                                                                                         | –                                                                                 |
| Lem. 2.38  | Lem. 2.36, Thm. 2.2                                                                                       | Lem. 2.39, Prop. 2.43                                                             |
| Lem. 2.39  | Lem. 2.38, Thm. 2.2, Lem. 2.8, Lem. 2.9                                                                   | Lem. 2.42, Prop. 2.43                                                             |
| Lem. 2.42  | Lem. 2.39, Lem. 2.9                                                                                       | Prop. 2.43                                                                        |
| Prop. 2.43 | Lem. 2.25, Lem. 2.42, Lem. 2.38,<br>Lem. 2.36, Lem. 2.32, Lem. 2.39,<br>Lem. 2.30                         | Thm. 2.46                                                                         |
| Def. 2.44  | –                                                                                                         | –                                                                                 |
| Def. 2.45  | –                                                                                                         | Cor. 3.7, Def. 8.7                                                                |

| statement  | uses                                                                                              | used by                                                                                         |
|------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Thm. 2.46  | Def. 8.7, Prop. 2.43, Def. 2.13, Lem. 2.9, Lem. 2.30                                              | Thm. 1.1, Lem. 3.2, Def. 4.1, Def. 4.16, Lem. 4.17, Lem. 5.22, Def. 11.1, Lem. 11.3, Rem. 11.13 |
| Rem. 2.47  | Lem. 2.25, Lem. 2.30                                                                              | Prop. 4.35, Rem. 4.36                                                                           |
| Rem. 2.48  | –                                                                                                 | –                                                                                               |
| Def. 3.1   | –                                                                                                 | –                                                                                               |
| Lem. 3.2   | Def. 2.23, Lem. 2.24, Thm. 2.46, Lem. 2.11                                                        | Lem. 4.33                                                                                       |
| Def. 3.3   | –                                                                                                 | Lem. 5.10                                                                                       |
| Prop. 3.4  | Def. 2.13                                                                                         | Lem. 3.5, Prop. 3.9, Cor. 3.11, Rem. 3.13, Prop. 4.31, Prop. 4.35                               |
| Lem. 3.5   | Prop. 3.4, Lem. 2.8                                                                               | Cor. 3.7, Prop. 3.9, Cor. 3.11                                                                  |
| Def. 3.6   | –                                                                                                 | Prop. 3.9                                                                                       |
| Cor. 3.7   | Lem. 3.5, Def. 2.45                                                                               | Lem. 5.23                                                                                       |
| Prop. 3.8  | –                                                                                                 | Prop. 3.9, Prop. 4.31, Lem. 5.13                                                                |
| Prop. 3.9  | Def. 3.6, Prop. 3.8, Lem. 3.5, Prop. 3.4                                                          | Def. 3.10, Rem. 3.13                                                                            |
| Def. 3.10  | Prop. 3.9                                                                                         | –                                                                                               |
| Cor. 3.11  | Lem. 3.5, Prop. 3.4, Lem. 2.5                                                                     | Rem. 3.13, Lem. 4.28                                                                            |
| Rem. 3.13  | Cor. 3.11, Prop. 3.9, Prop. 3.4                                                                   | –                                                                                               |
| Def. 4.1   | Def. 2.23, Thm. 2.46                                                                              | –                                                                                               |
| Thm. 4.2   | Lem. 4.17, Prop. 4.19, Lem. 7.2, Def. 7.1, Lem. 7.3, Def. 5.20, Lem. 5.21                         | Thm. 1.1, Lem. 7.3                                                                              |
| Lem. 4.6   | –                                                                                                 | Lem. 4.8                                                                                        |
| Lem. 4.8   | Lem. 4.6                                                                                          | Lem. 4.13, Prop. 12.4                                                                           |
| Lem. 4.10  | –                                                                                                 | Prop. 4.15, Rem. 4.36, Lem. 5.5, Lem. 5.21, Lem. 5.22, Lem. 5.23, Lem. 12.3, Rem. 12.6          |
| Lem. 4.13  | Lem. 4.8                                                                                          | Prop. 4.15, Prop. 4.19, Prop. 12.4, Prop. 12.9                                                  |
| Prop. 4.15 | Lem. 4.13, Lem. 4.10                                                                              | Rem. 4.36, Rem. 4.38, Rem. 7.4, Prop. 12.4                                                      |
| Def. 4.16  | Lem. 2.5, Thm. 2.46, Def. 2.13                                                                    | Prop. 4.19, Def. 11.1                                                                           |
| Lem. 4.17  | Thm. 2.46                                                                                         | Thm. 4.2, Prop. 4.19, Rem. 4.37, Lem. 5.22                                                      |
| Def. 4.18  | –                                                                                                 | Prop. 4.19, Lem. 5.21                                                                           |
| Prop. 4.19 | Def. 4.18, Lem. 4.13, Def. 4.16, Lem. 4.17                                                        | Thm. 4.2, Rem. 4.37, Lem. 7.2, Prop. 12.9, Rem. 12.11                                           |
| Rem. 4.20  | –                                                                                                 | –                                                                                               |
| Lem. 4.21  | –                                                                                                 | Lem. 4.29, Prop. 4.31, Lem. 6.1                                                                 |
| Lem. 4.22  | –                                                                                                 | Lem. 4.23, Lem. 4.24, Lem. 4.25, Prop. 4.31                                                     |
| Lem. 4.23  | Lem. 4.22                                                                                         | Lem. 4.28, Lem. 4.29, Prop. 4.31                                                                |
| Lem. 4.24  | Lem. 4.22                                                                                         | Lem. 4.25, Lem. 4.26, Prop. 4.31                                                                |
| Lem. 4.25  | Lem. 4.22, Lem. 4.24                                                                              | Prop. 4.31                                                                                      |
| Lem. 4.26  | Lem. 4.24                                                                                         | Lem. 4.28, Lem. 4.29, Prop. 4.31                                                                |
| Lem. 4.28  | Lem. 4.26, Lem. 4.23, Cor. 3.11                                                                   | –                                                                                               |
| Lem. 4.29  | Lem. 4.21, Lem. 4.26, Lem. 4.23                                                                   | Prop. 4.31                                                                                      |
| Prop. 4.31 | Lem. 4.21, Lem. 4.26, Lem. 4.25, Lem. 4.22, Lem. 4.29, Lem. 4.23, Lem. 4.24, Prop. 3.8, Prop. 3.4 | Lem. 5.13, Prop. 6.5, Lem. 7.3                                                                  |
| Def. 4.32  | –                                                                                                 | Lem. 4.34, Def. 5.20                                                                            |
| Lem. 4.33  | Lem. 3.2, Lem. 2.25, Lem. 2.29                                                                    | Rem. 4.36, Lem. 5.21                                                                            |

| statement  | uses                                                                                    | used by                                                                             |
|------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Lem. 4.34  | Def. 4.32, Lem. 2.29                                                                    | Prop. 4.35                                                                          |
| Prop. 4.35 | Lem. 4.34, Prop. 3.4, Rem. 2.47                                                         | –                                                                                   |
| Rem. 4.36  | Lem. 4.33, Lem. 4.10, Prop. 4.15, Rem. 2.47                                             | –                                                                                   |
| Rem. 4.37  | Lem. 4.17, Prop. 4.19                                                                   | –                                                                                   |
| Rem. 4.38  | Prop. 4.15                                                                              | –                                                                                   |
| Lem. 5.1   | –                                                                                       | Lem. 5.4                                                                            |
| Def. 5.2   | –                                                                                       | Lem. 5.4, Lem. 5.5                                                                  |
| Lem. 5.3   | –                                                                                       | Lem. 5.5, Lem. 5.13                                                                 |
| Lem. 5.4   | Def. 5.2, Lem. 5.1, Lem. 2.29                                                           | Lem. 5.6                                                                            |
| Lem. 5.5   | Lem. 4.10, Lem. 5.3, Def. 5.2, Lem. 2.25                                                | Lem. 5.6, Def. 5.7, Def. 5.9, Lem. 5.11, Lem. 5.13, Lem. 5.16, Lem. 5.17, Lem. 5.19 |
| Lem. 5.6   | Lem. 5.4, Lem. 5.5                                                                      | Def. 5.7, Lem. 5.8, Def. 5.9, Prop. 5.12, Lem. 5.17                                 |
| Def. 5.7   | Lem. 5.6, Lem. 5.5                                                                      | Def. 5.9, Prop. 5.12, Lem. 5.13, Lem. 5.18                                          |
| Lem. 5.8   | Lem. 5.6                                                                                | Lem. 5.13, Rem. 5.15, Lem. 5.16, Lem. 6.4                                           |
| Def. 5.9   | Def. 5.7, Lem. 5.6, Lem. 5.5                                                            | Lem. 5.11, Prop. 5.12                                                               |
| Lem. 5.10  | Def. 3.3                                                                                | Prop. 5.12                                                                          |
| Lem. 5.11  | Def. 5.9, Lem. 5.5                                                                      | Prop. 5.12, Lem. 5.21                                                               |
| Prop. 5.12 | Def. 5.7, Lem. 5.6, Def. 5.9, Lem. 5.11, Lem. 5.10                                      | Lem. 5.21, Lem. 7.3                                                                 |
| Lem. 5.13  | Prop. 4.31, Def. 5.7, Lem. 5.8, Lem. 5.5, Lem. 5.3, Prop. 3.8                           | Rem. 5.15, Lem. 5.16, Lem. 5.18, Lem. 5.21, Lem. 5.23, Prop. 6.5                    |
| Rem. 5.15  | Lem. 5.13, Lem. 5.8                                                                     | –                                                                                   |
| Lem. 5.16  | Lem. 5.13, Lem. 5.8, Lem. 5.5                                                           | Lem. 5.17, Lem. 5.19, Lem. 6.4, Prop. 6.5                                           |
| Lem. 5.17  | Lem. 5.16, Lem. 5.6, Lem. 5.5                                                           | Prop. 6.5                                                                           |
| Lem. 5.18  | Lem. 5.13, Def. 5.7                                                                     | Lem. 5.19, Lem. 5.21, Lem. 5.23                                                     |
| Lem. 5.19  | Lem. 5.16, Lem. 5.5, Lem. 5.18                                                          | Lem. 5.21                                                                           |
| Def. 5.20  | Def. 4.32                                                                               | Thm. 4.2, Lem. 5.22, Lem. 7.3                                                       |
| Lem. 5.21  | Lem. 4.33, Def. 4.18, Lem. 4.10, Lem. 5.13, Prop. 5.12, Lem. 5.19, Lem. 5.11, Lem. 5.18 | Thm. 4.2                                                                            |
| Lem. 5.22  | Lem. 4.10, Lem. 4.17, Def. 5.20, Thm. 2.46                                              | Lem. 7.3, Rem. 7.4                                                                  |
| Lem. 5.23  | Lem. 4.10, Lem. 5.13, Lem. 5.18, Cor. 3.7                                               | Lem. 7.3                                                                            |
| Lem. 6.1   | Lem. 4.21                                                                               | Prop. 6.5                                                                           |
| Lem. 6.2   | –                                                                                       | Lem. 6.3, Prop. 6.5                                                                 |
| Lem. 6.3   | Lem. 6.2                                                                                | Prop. 6.5                                                                           |
| Lem. 6.4   | Lem. 5.16, Lem. 5.8                                                                     | Prop. 6.5                                                                           |
| Prop. 6.5  | Prop. 4.31, Lem. 5.13, Lem. 5.16, Lem. 5.17, Lem. 6.1, Lem. 6.4, Lem. 6.2, Lem. 6.3     | Lem. 7.3                                                                            |
| Def. 7.1   | –                                                                                       | Thm. 4.2, Lem. 7.2, Lem. 7.3                                                        |
| Lem. 7.2   | Prop. 4.19, Def. 7.1                                                                    | Thm. 4.2                                                                            |
| Lem. 7.3   | Thm. 4.2, Prop. 4.31, Def. 7.1, Prop. 5.12, Lem. 5.23, Lem. 5.22, Def. 5.20, Prop. 6.5  | Thm. 4.2                                                                            |
| Rem. 7.4   | Prop. 4.15, Lem. 5.22                                                                   | –                                                                                   |
| Def. 8.1   | –                                                                                       | –                                                                                   |
| Lem. 8.2   | –                                                                                       | Prop. 8.5                                                                           |
| Def. 8.4   | –                                                                                       | –                                                                                   |

| statement  | uses                                                                                                                                                                                    | used by                                                                          |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Prop. 8.5  | Lem. 8.2                                                                                                                                                                                | Lem. 8.14, Prop. 8.32, Prop. 9.26, Lem. 12.7                                     |
| Def. 8.7   | Def. 2.45                                                                                                                                                                               | Thm. 2.46, Def. 8.9, Cor. 9.29                                                   |
| Lem. 8.8   | –                                                                                                                                                                                       | Def. 8.9, Lem. 8.11, Cor. 9.29                                                   |
| Def. 8.9   | Lem. 8.8, Def. 8.7                                                                                                                                                                      | Lem. 8.11, Prop. 8.32, Cor. 9.29                                                 |
| Lem. 8.11  | Def. 8.9, Lem. 8.8                                                                                                                                                                      | Lem. 8.22, Prop. 8.32, Lem. 9.25                                                 |
| Lem. 8.14  | Prop. 8.5                                                                                                                                                                               | Lem. 8.19, Prop. 9.26                                                            |
| Def. 8.16  | –                                                                                                                                                                                       | –                                                                                |
| Lem. 8.17  | –                                                                                                                                                                                       | Lem. 8.19, Prop. 9.26                                                            |
| Def. 8.18  | –                                                                                                                                                                                       | Prop. 8.32                                                                       |
| Lem. 8.19  | Lem. 8.17, Lem. 8.14                                                                                                                                                                    | Prop. 8.32, Prop. 9.26                                                           |
| Lem. 8.21  | –                                                                                                                                                                                       | Prop. 8.32, Prop. 9.26                                                           |
| Lem. 8.22  | Lem. 8.11                                                                                                                                                                               | Prop. 8.32, Lem. 9.20                                                            |
| Lem. 8.24  | –                                                                                                                                                                                       | Lem. 8.30, Prop. 8.32, Lem. 9.22, Cor. 9.29                                      |
| Lem. 8.27  | –                                                                                                                                                                                       | Prop. 10.14                                                                      |
| Def. 8.28  | –                                                                                                                                                                                       | Prop. 9.26                                                                       |
| Def. 8.29  | –                                                                                                                                                                                       | Lem. 8.30, Prop. 8.32, Lem. 9.22, Prop. 9.26, Cor. 9.29, Prop. 10.14, Cor. 11.11 |
| Lem. 8.30  | Def. 8.29, Lem. 8.24                                                                                                                                                                    | Prop. 8.32, Lem. 9.22                                                            |
| Lem. 8.31  | –                                                                                                                                                                                       | Prop. 8.32, Prop. 9.26                                                           |
| Prop. 8.32 | Def. 8.29, Lem. 8.31, Def. 8.18, Lem. 8.22, Def. 8.9, Lem. 8.19, Prop. 8.5, Lem. 8.21, Lem. 8.24, Lem. 8.11, Lem. 8.30                                                                  | Prop. 9.26, Rem. 9.28, Cor. 9.29                                                 |
| Def. 9.1   | –                                                                                                                                                                                       | –                                                                                |
| Lem. 9.2   | –                                                                                                                                                                                       | Def. 9.3                                                                         |
| Def. 9.3   | Lem. 9.2                                                                                                                                                                                | Prop. 9.26                                                                       |
| Lem. 9.5   | –                                                                                                                                                                                       | Lem. 9.11                                                                        |
| Def. 9.7   | –                                                                                                                                                                                       | Thm. 1.1, Def. 9.10, Prop. 9.26, Cor. 9.29                                       |
| Lem. 9.8   | –                                                                                                                                                                                       | Rem. 9.18, Prop. 9.26                                                            |
| Def. 9.10  | Def. 9.7                                                                                                                                                                                | Lem. 9.11, Cor. 9.14                                                             |
| Lem. 9.11  | Lem. 9.5, Def. 9.10                                                                                                                                                                     | Def. 9.13, Cor. 9.14, Rem. 9.18, Rem. 9.28, Cor. 9.29, Def. 11.1                 |
| Def. 9.13  | Lem. 9.11                                                                                                                                                                               | Prop. 9.26                                                                       |
| Cor. 9.14  | Def. 9.10, Lem. 9.11                                                                                                                                                                    | Rem. 9.18                                                                        |
| Rem. 9.16  | –                                                                                                                                                                                       | –                                                                                |
| Rem. 9.18  | Cor. 9.14, Lem. 9.8, Lem. 9.11                                                                                                                                                          | –                                                                                |
| Def. 9.19  | –                                                                                                                                                                                       | –                                                                                |
| Lem. 9.20  | Lem. 8.22                                                                                                                                                                               | Lem. 9.22, Prop. 9.26                                                            |
| Lem. 9.22  | Lem. 9.20, Def. 8.29, Lem. 8.24, Lem. 8.30                                                                                                                                              | Lem. 9.24, Prop. 9.26                                                            |
| Lem. 9.24  | Lem. 9.22                                                                                                                                                                               | Prop. 9.26                                                                       |
| Lem. 9.25  | Lem. 8.11                                                                                                                                                                               | Prop. 9.26                                                                       |
| Prop. 9.26 | Lem. 9.22, Def. 9.13, Lem. 9.20, Def. 9.3, Lem. 9.24, Lem. 9.25, Lem. 9.8, Def. 9.7, Def. 8.29, Lem. 8.31, Lem. 8.19, Prop. 8.5, Lem. 8.17, Lem. 8.21, Def. 8.28, Prop. 8.32, Lem. 8.14 | Thm. 1.1, Rem. 9.28, Cor. 9.29, Lem. 11.12, Rem. 11.14, Lem. 12.7                |
| Rem. 9.28  | Lem. 9.11, Prop. 9.26, Prop. 8.32                                                                                                                                                       | –                                                                                |

| statement   | uses                                                                                                            | used by                                                                                          |
|-------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Cor. 9.29   | Lem. 9.11, Def. 9.7, Prop. 9.26, Def. 8.29,<br>Def. 8.9, Lem. 8.24, Lem. 8.8, Prop. 8.32,<br>Def. 8.7           | –                                                                                                |
| Def. 10.1   | –                                                                                                               | Def. 11.1                                                                                        |
| Lem. 10.2   | –                                                                                                               | Lem. 10.13, Prop. 10.14, Prop. 10.21                                                             |
| Lem. 10.4   | –                                                                                                               | Prop. 10.14, Def. 11.1, Prop. 11.7                                                               |
| Lem. 10.6   | –                                                                                                               | Lem. 10.11                                                                                       |
| Lem. 10.8   | –                                                                                                               | Lem. 10.11, Prop. 10.14, Prop. 10.18                                                             |
| Def. 10.10  | –                                                                                                               | –                                                                                                |
| Lem. 10.11  | Lem. 10.8, Lem. 10.6                                                                                            | Prop. 10.14, Prop. 10.18                                                                         |
| Def. 10.12  | –                                                                                                               | –                                                                                                |
| Lem. 10.13  | Lem. 10.2                                                                                                       | Prop. 10.14, Prop. 11.7                                                                          |
| Prop. 10.14 | Def. 8.29, Lem. 8.27, Lem. 10.2,<br>Lem. 10.4, Lem. 10.8, Prop. 10.21,<br>Lem. 10.11, Lem. 10.13                | Cor. 11.11                                                                                       |
| Def. 10.16  | –                                                                                                               | –                                                                                                |
| Prop. 10.18 | Lem. 10.8, Lem. 10.11                                                                                           | Cor. 10.26, Def. 11.5, Prop. 11.6,<br>Prop. 11.7, Lem. 11.12                                     |
| Prop. 10.21 | Lem. 10.2                                                                                                       | Prop. 10.14, Rem. 10.25, Cor. 10.26,<br>Prop. 11.7, Lem. 11.12                                   |
| Rem. 10.25  | Prop. 10.21                                                                                                     | –                                                                                                |
| Cor. 10.26  | Prop. 10.21, Prop. 10.18                                                                                        | Def. 11.5, Prop. 11.7, Lem. 11.12                                                                |
| Lem. 10.28  | –                                                                                                               | Prop. 11.7                                                                                       |
| Def. 11.1   | Def. 4.16, Lem. 9.11, Lem. 10.4, Def. 10.1,<br>Thm. 2.46                                                        | Thm. 1.1, Lem. 11.3, Def. 11.5,<br>Prop. 11.6, Prop. 11.7, Cor. 11.11,<br>Lem. 11.12, Prop. 12.8 |
| Def. 11.2   | –                                                                                                               | Lem. 11.3, Prop. 12.8                                                                            |
| Lem. 11.3   | Def. 11.1, Def. 11.2, Thm. 2.46                                                                                 | Thm. 1.1, Prop. 11.7, Cor. 11.11,<br>Lem. 11.12, Prop. 12.8                                      |
| Def. 11.5   | Def. 11.1, Cor. 10.26, Prop. 10.18                                                                              | Prop. 11.7, Lem. 11.12, Prop. 12.8                                                               |
| Prop. 11.6  | Def. 11.1, Prop. 10.18                                                                                          | Thm. 1.1, Cor. 11.11, Lem. 11.12                                                                 |
| Prop. 11.7  | Def. 11.1, Def. 11.5, Lem. 11.3,<br>Lem. 10.28, Cor. 10.26, Lem. 10.4,<br>Prop. 10.21, Prop. 10.18, Lem. 10.13  | Cor. 11.11, Lem. 11.12                                                                           |
| Cor. 11.11  | Def. 11.1, Prop. 11.7, Prop. 11.6,<br>Lem. 11.3, Def. 8.29, Prop. 10.14                                         | Thm. 1.1                                                                                         |
| Lem. 11.12  | Def. 11.1, Prop. 11.7, Prop. 11.6,<br>Def. 11.5, Lem. 11.3, Prop. 9.26,<br>Cor. 10.26, Prop. 10.21, Prop. 10.18 | Thm. 1.1                                                                                         |
| Rem. 11.13  | Thm. 2.46                                                                                                       | –                                                                                                |
| Rem. 11.14  | Prop. 9.26                                                                                                      | –                                                                                                |
| Lem. 12.1   | –                                                                                                               | Lem. 12.3, Prop. 12.4, Prop. 12.8                                                                |
| Def. 12.2   | –                                                                                                               | Lem. 12.3, Prop. 12.4, Prop. 12.8                                                                |
| Lem. 12.3   | Lem. 4.10, Def. 12.2, Lem. 12.1                                                                                 | Prop. 12.8, Prop. 12.9                                                                           |
| Prop. 12.4  | Lem. 4.13, Prop. 4.15, Lem. 4.8,<br>Def. 12.2, Lem. 12.1                                                        | Rem. 12.6, Prop. 12.8, Prop. 12.9                                                                |
| Rem. 12.6   | Lem. 4.10, Prop. 12.4                                                                                           | –                                                                                                |
| Lem. 12.7   | Prop. 9.26, Prop. 8.5                                                                                           | Prop. 12.8                                                                                       |
| Prop. 12.8  | Def. 11.1, Def. 11.2, Def. 11.5, Lem. 11.3,<br>Prop. 12.4, Lem. 12.3, Def. 12.2,<br>Lem. 12.1, Lem. 12.7        | Prop. 12.9                                                                                       |

| statement  | uses                                                                   | used by |
|------------|------------------------------------------------------------------------|---------|
| Prop. 12.9 | Lem. 4.13, Prop. 4.19, Prop. 12.4, Rem. 12.11<br>Prop. 12.8, Lem. 12.3 |         |
| Rem. 12.11 | Prop. 4.19, Prop. 12.9                                                 | —       |

## 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. Tim Dokchitser, *Computing special values of motivic L-functions*, Experimental Mathematics **13** (2004), no. 2, 137–149.
3. 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>.
4. 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>.
5. 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>.
6. ———, *Some problems in number theory, combinatorics and combinatorial geometry*, Mathematica Pannonica **5** (1994), no. 2, 261–269.
7. Mikhail Ershov, *Golod–Shafarevich groups: a survey*, International Journal of Algebra and Computation **22** (2012), no. 5, 1230001, 68 pages.
8. Ralph H. Fox, *Free differential calculus. I: Derivation in the free group ring*, Annals of Mathematics **57** (1953), no. 3, 547–560.
9. 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>.
10. Farshid Hajir, Christian Maire, and Ravi Ramakrishna, *Cutting towers of number fields*, Annales mathématiques du Québec **45** (2021), no. 2, 321–345.
11. 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>.
12. Nicholas J. Higham, *Accuracy and stability of numerical algorithms*, second ed., SIAM, Philadelphia, 2002.
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. James S. Milne, *Lectures on étale cohomology*, 2013, Version 2.21, March 22, 2013; <https://www.jmilne.org/math/CourseNotes/LEC.pdf>.
17. ———, *Algebraic number theory*, 2020, Version 3.08, July 19, 2020; <https://www.jmilne.org/math/CourseNotes/ANT.pdf>.
18. ———, *Class field theory*, 2020, Version 4.03, August 6, 2020; <https://www.jmilne.org/math/CourseNotes/CFT.pdf>.
19. 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>.
20. 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>.
21. ———, *An exponent of 1.043 for the unit distance problem: Lean formalization at exponent 1.04315, conditional on one zeta inequality*, Palomar registry, PALOMAR-2026-10-01-000018, version 2, 2026, <https://palomar-registry.org/entry?id=PALOMAR-2026-10-01-000018&version=2>; Lean 4 source at <https://github.com/enaslund/unit-distance-bound-0.0427/tree/edd88c0c175ab4d18cf6115e2f6ddf3865d36b12/lean>.
22. ———, *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>.

23. ———, *Supplementary programs and data for “An exponent of 1.043 for the unit distance problem”*, GitHub repository [enaslund/unit-distance-bound-0.0427](https://github.com/enaslund/unit-distance-bound-0.0427), directories [papers/0.043171](https://github.com/enaslund/unit-distance-bound-0.0427/papers/0.043171), [papers/0.042901](https://github.com/enaslund/unit-distance-bound-0.0427/papers/0.042901), [papers/0.04273/certificates](https://github.com/enaslund/unit-distance-bound-0.0427/papers/0.04273/certificates), [papers/0.0418235/certificates](https://github.com/enaslund/unit-distance-bound-0.0427/papers/0.0418235/certificates) and [research](https://github.com/enaslund/unit-distance-bound-0.0427/research), 2026, <https://github.com/enaslund/unit-distance-bound-0.0427>.
24. 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/>.
25. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2 ed., Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, Berlin, Heidelberg, 2008.
26. 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>.
27. *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>.
28. 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>.
29. 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>.
30. 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).
31. J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, *Illinois Journal of Mathematics* **6** (1962), 64–94.
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. ———, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York, 1977.
35. 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.
36. 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>.
37. 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>.
38. 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.
39. The FLINT team, *FLINT: Fast Library for Number Theory*, 2026, Version 3.6.0, used through python-flint 0.9.0; <https://flintlib.org>.
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: [enaslund.math@gmail.com](mailto:enaslund.math@gmail.com)