SATO-TATE EQUIDISTRIBUTION OF CERTAIN FAMILIES OF

Citation for the original published paper (version of record):

Shankar, A., Södergren, A., Templier, N. (2019)
SATO-TATE EQUIDISTRIBUTION OF CERTAIN FAMILIES OF ARTIN L-FUNCTIONS
FORUM OF MATHEMATICS SIGMA, 7
http://dx.doi.org/10.1017/fms.2019.18

Forum of Mathematics, Sigma (2019), Vol. 7, e23, 62 pages
doi:10.1017/fms.2019.18

SATO–TATE EQUIDISTRIBUTION OF CERTAIN FAMILIES OF ARTIN L-FUNCTIONS

ARUL SHANKAR[1], ANDERS SÖDERGREN[2] and NICOLAS TEMPLIER[3]

[1] Department of Mathematics, University of Toronto, Toronto, ON, M5S 2E4, Canada;
email: arul.shnkr@gmail.com

[2] Department of Mathematical Sciences, Chalmers University of Technology and the University of Gothenburg, SE-412 96 Gothenburg, Sweden;
email: andesod@chalmers.se

[3] Department of Mathematics, Cornell University, Ithaca, NY 14853, USA;
email: templier@math.cornell.edu

Received 19 May 2016; accepted 24 May 2019

Abstract

We study various families of Artin L-functions attached to geometric parametrizations of number fields. In each case we find the Sato–Tate measure of the family and determine the symmetry type of the distribution of the low-lying zeros.

2010 Mathematics Subject Classification: 11R42, 11M41 (primary); 11M50 (secondary)

1. Introduction

The Katz–Sarnak heuristics [43] concern the arithmetic statistics of a family $\mathfrak{F}$ of L-functions. In this paper, we verify the heuristics for certain families arising from number fields. We shall follow the framework of the recent [61]. We recall that in [61] the authors distinguish two ways of forming a family: harmonic families, which can be studied with the trace formula; and geometric families arising from algebraic varieties defined over the rationals. In this paper we are concerned with the geometric families of zero-dimensional varieties, which give rise to number fields.

The first family we study comes from the space V of monic polynomials of degree n. To any $f \in V$ we associate its scheme X_f of zeros. This defines an affine subset $X \subset V \times \mathbb{A}^1$. If $f \in V(\mathbb{Z})$, then the ring $R_f := \mathbb{Z}[T]/f(T)$ of regular functions on X_f is *monogenic*, which means that it is generated by a single element called a *monogenizer* of R_f. The additive group $\mathbb{G}_a$ naturally acts on V and on $\mathbb{A}^1$ via translations $(m \cdot f)(T) := f(T+m)$ and the n-covering $X \to V$ is $\mathbb{G}_a$-equivariant.

The ramification locus of $X \to V$ is given by the equation $\Delta = 0$, where the discriminant Δ is a $\mathbb{G}_a$-invariant polynomial function on V. The covering is étale away from the ramification locus, thus in particular the ring R_f is reduced if and only if $\Delta(f) \neq 0$. The Galois group of the covering is the full permutation group S_n, which can be proved by identifying V with the GIT quotient $\mathbb{A}^n//S_n$ and similarly $X \simeq \mathbb{A}^n//S_{n-1}$ with the natural projections $X \to V$ and $X \to \mathbb{A}^1$; see Section 5.

If $f \in V(\mathbb{Z})^{\mathrm{irr}}$ is irreducible, then the field of fractions K_f of R_f is a number field of degree n. Let M_f denote the normal closure of K_f. The Galois group $\mathrm{Gal}(M_f/\mathbb{Q})$ embeds irreducibly into S_n. By composing with the standard representation of S_n, we obtain an Artin representation

$$\rho_{K_f} : \mathrm{Gal}(M_f/\mathbb{Q}) \hookrightarrow S_n \to \mathrm{GL}_{n-1}(\mathbb{C}).$$

We are interested in the L-functions $L(s, \rho_{K_f})$. Note that $\zeta(s)L(s, \rho_{K_f})$ is equal to the Dedekind zeta function $\zeta_{K_f}(s)$. In a precise sense to be explained in Section 5.2, for a 100% of elements $f \in V(\mathbb{Z})$, the polynomial f is irreducible and the normal closure M_f has Galois group S_n. This can be seen to follow from an application of Hilbert irreducibility.

We consider the subset $V(\mathbb{Z})^{\max}$ of $V(\mathbb{Z})^{\mathrm{irr}}$ consisting of irreducible polynomials f such that R_f is a maximal order in K_f. Imposing the condition of maximality requires the application of a sieve and a tail estimate developed and proved in [11]. The action of $\mathbb{G}_a(\mathbb{Z}) = \mathbb{Z}$ by translation preserves the subsets $V(\mathbb{Z})^{\mathrm{irr}}$ and $V(\mathbb{Z})^{\max}$ of $V(\mathbb{Z})$. Let the family $\mathfrak{F}$ consist of the $\mathbb{Z}$-orbits on $V(\mathbb{Z})^{\max}$. For a 100% of $f \in V(\mathbb{Z})^{\max}$, the representation ρ_{K_f} has image S_n, hence $L(s, \rho_{K_f})$ is orthogonal self-dual.

The family $\mathfrak{F}$ parametrizes monogenized number fields of degree n over $\mathbb{Q}$ up to isomorphism. If $R = \mathbb{Z}[\alpha]$ is a monogenic ring, then the pair (R, α) is called a *monogenized ring*. A pair (K, α) where K is a number field is said to be a *monogenized field* if α belongs to $\mathcal{O}_K$, the ring of integers of K, and the pair $(\mathcal{O}_K, \alpha)$ is a monogenized ring. Two monogenized fields (K, α) and (K', α') are said to be *isomorphic* if K is isomorphic to K' and this isomorphism carries α to $\alpha' + m$ for some integer $m \in \mathbb{Z}$. If a monic polynomial f is irreducible, then the field of fractions of R_f is a degree-n field $K_f = \mathbb{Q}[T]/f(T)$, and the pair (K_f, α) is a monogenized field, where α is the image of T in R_f. Conversely, if (K, α) is a monogenized field, then the characteristic polynomial of α is an element f belonging to $V(\mathbb{Z})^{\max}$, and the field of fractions of R_f is K.

It is possible for number fields to have more than one monogenizer. However, a result of Birch and Merriman [13] implies that a number field has only finitely many monogenizers, up to translation by a rational integer. Therefore, a number field K arises only finitely many times in the family $\mathfrak{F}$.

Since $V \simeq \mathbb{A}^n//S_n$ it is natural to consider the associated grading. More precisely, an element $(x_1, \ldots, x_n) \in \mathbb{A}^n//S_n$ gives rise to the polynomial $f(T) = \prod_i (T - x_i)$, hence considering the x_i to be elements of degree 1, it follows that for $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n \in V$, the coefficient a_i has degree i because it is $(-1)^i$ times the ith symmetric polynomial evaluated at the roots of f. The discriminant Δ is then homogeneous of degree $n(n-1)$. We order the family by the height $h(f) := \max_i\{|a_i|^{n(n-1)/i}\}$ on $V(\mathbb{R})$ which is also homogeneous of degree $n(n-1)$. We then prove the following theorem (see Sections 2 and 5):

THEOREM 1.1. *The family parametrizing monogenized degree-n number fields ordered by height has Sato–Tate group $S_n \subset \mathrm{GL}_{n-1}(\mathbb{C})$, rank zero, and Symplectic symmetry type. It satisfies Sato–Tate equidistribution in the sense of* [61, Conjecutre 1], *and the Katz–Sarnak heuristics for one-level density.*

If we let $\mathcal{T}_n$ be the set of conjugacy classes in S_n, then [61, parts (iii) and (iv) of Conjecture 1] translates to the following statement. Uniformly as $x, y \to \infty$ with $\log x/\log y$ large enough, the elements

$$\{\rho_K(\mathrm{Frob}_p) : K \in \mathfrak{F}(x),\, p < y\} \subset \mathcal{T}_n \tag{1}$$

become equidistributed for the Sato–Tate measure on $\mathcal{T}_n$ which is the pushforward of the normalized counting measure on S_n. This is to be compared with the Chebotarev equidistribution theorem that says that for any S_n-number field K, the elements $\{\rho_K(\mathrm{Frob}_p) : p < y\}$ are equidistributed in $\mathcal{T}_n$ as $y \to \infty$. Here the extra averaging over $K \in \mathfrak{F}(x)$ allows us to produce a quantitative power saving error term.

In general, for any given family the Sato–Tate equidistribution (1) has applications to sieving, zero density results, averaging of L-values, and low-lying zeros. In this paper we confine ourselves to the latter aspect. The assertion of Theorem 1.1 on the Symplectic symmetry type corresponds to the one-level density with restricted support of low-lying zeros (see Theorem 2.8). As explained in [61, Conjecture 2], the proof proceeds from the Sato–Tate equidistribution of (1) and from considering the following two additional quantities. First, the *root numbers* of $L(s, \rho_K)$ are always $+1$ because the root numbers of both $\zeta(s)$ and $\zeta_K(s)$ are $+1$. This also follows from ρ_K being an orthogonal representation, as a special case of a result of Fröhlich and Queyrut [37]. Second, the *rank of the family* is zero; see Section 2.5.

The proof of Theorem 1.1 proceeds as follows: first, we determine asymptotics for the number of $\mathbb{Z}$-orbits on $V(\mathbb{Z})^{\max}$ having bounded height, and whose coefficients satisfy any finite set of congruence conditions. It is here that we need the sieve methods of [11]. Next, note that $\rho_{K_f}(\mathrm{Frob}_p)$ is determined by $R_f \otimes \mathbb{F}_p$, which is the ring over $\mathbb{F}_p$ corresponding to the reduction of f modulo p. We then determine the density of elements in $V(\mathbb{Z})^{\max}$, such that the corresponding value of $\rho_{K_f}(\mathrm{Frob}_p)$ is fixed, via a local count of configurations of n points in $\mathbb{F}_p$.

Next, it is desirable to have families that count each number field at most once. This is achieved in the cubic case by further considering orbits under the GL_2 action. One forms the affine space $V \simeq \mathbb{A}^4$ of binary cubic forms, and construct a 3-covering $X \to V$ as above, except that now $X \subset V \times \mathbb{P}^1$ is quasi-projective. We consider the action by GL_2 on V and on $\mathbb{P}^1$ which induces an equivariant structure of the covering $X \to V$, that is, the action of GL_2 on $V \times \mathbb{P}^1$ preserves X and the map $X \to V$ is compatible with the actions of GL_2 on X and V. In fact V is a prehomogeneous vector space for this action and the discriminant Δ is a generator of the algebra of invariant polynomials. We then consider elements f in $\mathrm{GL}_2(\mathbb{Z})\backslash V(\mathbb{Z})^{\mathrm{smax}}$ as parameters for maximal S_3-orders. Since two maximal cubic forms give rise to the same cubic field K_f if and only if they belong to the same $\mathrm{GL}_2(\mathbb{Z})$-orbit, we obtain a family $\mathfrak{F}$ which parametrizes the S_3-fields exactly once. We shall order the family by discriminant so that $\mathfrak{F}(x)$ coincides with the set of S_3-fields with absolute discriminant less than x. It is a result of Davenport–Heilbronn that $|\mathfrak{F}(x)| \sim x/(3\zeta(3))$ as $x \to \infty$. Bhargava [7, 8] proved the analogous result for quartic and quintic fields. The following is due to Yang [79] in the cubic and quartic cases.

THEOREM 1.2. *The families parametrizing S_3-, S_4- and S_5-fields ordered by discriminant are homogeneous orthogonal, and have rank zero and Symplectic symmetry type. They satisfy Sato–Tate equidistribution, and the Katz–Sarnak heuristics for one-level density.*

The thesis [79] is unpublished. An account first appeared in [61] and Sections 2 and 3 of this paper provide more details. A different treatment is given in [19, 20]. The advantage of our treatment compared to [19, 20, 79] is to make transparent the relation between the symmetry type and the other statistical invariants of the families. As before, the equidistribution statement is to be interpreted in the sense of the quantitative equidistribution of (1), where the normalized counting measure on $\mathcal{T}_n$ arise as the limit as $p \to \infty$ of the pushforward of the normalized counting measure on $V(\mathbb{Z}_p)^{\max}$. We recall the concept of a homogeneous orthogonal family in Section 2. A key aspect of both Theorems 1.1 and 1.2 is the study of maps

$$V(\mathbb{Z}_p)^{\max} \supset V(\mathbb{Z}_p)^{\mathrm{unr}} \twoheadrightarrow V(\mathbb{F}_p)^{\Delta\neq 0} \twoheadrightarrow \mathcal{T}_n, \tag{2}$$

which gives the splitting type of an order unramified at p in terms of the reduction of the corresponding polynomial modulo p.

The proofs rely in an essential way on Bhargava's work on counting and parametrizing quartic and quintic fields. A rank n ring arises as the ring of functions of a projective set of n points defined over $\mathbb{Z}$, and conversely its spectrum is a set of n points. As explained in [6, Section 2], every rank n ring arises from a set of n points in $\mathbb{P}^{n-2}$. In the case $n = 3$, where three points in $\mathbb{P}^1$ are parametrized as the zero set of binary cubic forms, the above construction was sufficient. Binary n-ic forms parametrize sets of n points in $\mathbb{P}^1$ which, for $n \geqslant 4$, do not give rise to all rank n rings; see [76]. To parametrize all rank n rings for $n = 4, 5$, Bhargava writes the n points in $\mathbb{P}^{n-2}$ as the intersection of quadrics. For $n = 4$, a generic set of two quadrics in $\mathbb{P}^2$ intersect in four points. Furthermore, every set of four points in $\mathbb{P}^2$ arise this way. Thus quartic rings are naturally parametrized by pairs of ternary quadratic forms [5]. We denote the underlying space $V = 2 \otimes \mathrm{Sym}^2(3)$.

In the case $n = 5$, five quadrics are required to obtain an intersection of five points. However a generic set of five quadrics do not intersect at all in $\mathbb{P}^3$. Rather it is known from the work of Buchsbaum and Eisenbud [15] that five quadrics in $\mathbb{P}^3$ intersect in five points if and only if they arise as the 4×4 Pfaffians of an alternating 5×5 matrix of linear forms in four variables. The underlying space is $V = 4 \otimes \wedge^2 (5)$ which gives rise to a parametrization of quintic rings [6].

In both cases $n = 4, 5$ we obtain a quasi-projective scheme $X \subset V \times \mathbb{P}^{n-2}$ cut out by quadrics. This is a branched covering $X \to V$ of degree n. As in the case $n = 3$, the covering has an equivariant G-structure with $G = \mathrm{GL}_2 \times \mathrm{SL}_3$ if $n = 4$ and $G = \mathrm{GL}_4 \times \mathrm{SL}_5$ if $n = 5$. (Here, $\mathrm{GL}_2 \times \mathrm{SL}_3$ acts on $\mathbb{P}^2$ via the action of SL_3 and $\mathrm{GL}_4 \times \mathrm{SL}_5$ acts on $\mathbb{P}^3$ via the action of GL_4.) As before we let $V(\mathbb{Z})^{\max}$ (respectively $V(\mathbb{Z})^{\mathrm{smax}}$) be the set of forms that give rise to maximal rings (respectively maximal S_n-rings). As before, we consider elements f in $G(\mathbb{Z})\backslash V(\mathbb{Z})^{\mathrm{smax}}$ as parameters for maximal S_n-rings. These are the families $\mathfrak{F}$ studied by Bhargava which parametrize S_4- and S_5-fields. The sets $\mathfrak{F}(x)$ will be ordered by discriminant and the asymptotics $|\mathfrak{F}(x)| \sim cx$ as $x \to \infty$ are the celebrated results of [7, 8]. Compared to the counting in Theorem 1.1 ordered by height, a major difficulty for these families ordered by discriminant, overcome by Bhargava, is the presence of noncompact 'cusps', which means there are forms in a fundamental domain for the $G(\mathbb{Z})$-action on $V(\mathbb{Z})$ that have large coefficients but small discriminant. The Sato–Tate equidistribution (1) with a power saving error term is obtained in [4, 7, 8, 64].

For $n = 4, 5$, restricting to the nonsingular locus gives étale coverings $X^{\Delta \neq 0} \to V^{\Delta \neq 0}$. Quotienting G by the subgroup that acts trivially on X, we obtain an algebraic group H such that $H(\mathbb{C})$ acts transitively on $V^{\Delta \neq 0}(\mathbb{C})$ and acts simply transitively on $X^{\Delta\neq 0}(\mathbb{C})$. (See [12, Table 1] for an exact description of H.) The stabilizer in $H(\mathbb{C})$ of any element in $V^{\Delta\neq 0}(\mathbb{C})$ is known to be S_n, see [62, Section 7] for $n = 4$ and [78, Proposition 2.13] for $n = 5$. It then follows that the normal closure of the étale covering $X^{\Delta\neq 0}(\mathbb{C}) \to V^{\Delta\neq 0}(\mathbb{C})$ has Galois group S_n. For the first family of monic degree-n polynomials with $n \geqslant 2$, the subset $V^{\Delta\neq 0}(\mathbb{C})$ of polynomials with nonzero discriminant admits again an étale covering $X^{\Delta\neq 0}(\mathbb{C})$ defined by their zero locus in $\mathbb{C}$, and the normal closure of this covering has again Galois group S_n. For all these families, the Galois group being the full S_n is closely related to the equidistribution (1), as discussed in [42] and [61, Section 2.11].

As a side remark it is interesting to note that nonisomorphic S_n-number fields K_f and $K_{f'}$ have distinct Dedekind zeta functions (see [56]). Since each S_n-field occurs exactly once, we are counting the L-functions $L(s, \rho_{K_f})$ also with multiplicity one.

It is believed that for any S_n-number field K, the central value $\zeta_K(\frac{1}{2})$ is nonzero. This belief is reinforced by the Symplectic symmetry type of the families described above, which thereby exhibit a repulsion of the low-lying zeros at the central point. For quadratic fields the nonnegativity of $\zeta_K(\frac{1}{2})$ implies (see [40]) a strong effective lower bound on the class number of K. For S_5-number fields the nonvanishing of ζ_K for real $s \in (0, 1)$ is a useful hypothesis in establishing modularity in [16].

Unconditionally Soundararajan [67] has proved that a positive proportion of all quadratic number fields satisfy $\zeta_K(\frac{1}{2}) \neq 0$, which is also strengthened in [22] into a positive proportion of nonvanishing of $\zeta_K(s)$ for real $s \in (0, 1)$. The generalization to families of S_n-number fields with $n \geqslant 3$ is still open. Our Theorems 1.1 and 1.2 above are not yet strong enough to derive a result in this direction because of the restricted support of the one-level density statistics.

The families are homogeneous orthogonal because the Frobenius–Schur indicator of $S_n \subset \mathrm{GL}_{n-1}(\mathbb{C})$ is equal to $+1$, an observation which was also made in [47, Item 76] in relation to mass formulas [9]. Another interesting application to an analogue of the Erdös–Kac theorem appears in [50], and to average upper bounds for class numbers in [31]. Although not stated in [31], it can be verified that their sieving argument applies to any number field family ordered by discriminant that satisfies the Sato–Tate equidistribution in the sense of [61, Conjecture 1].

As stated above, the root number is $+1$ for any S_n-number field. In general the root number of a self-dual Artin representation may be -1, the first example was given by Armitage [1]. Thus one may wonder what happens for general families of Artin representations with a different root number. This motivates our study of families of quaternionic fields. Let K be a quaternionic field, that is a degree eight number field whose Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is the quaternion group Q of eight elements. There is a unique irreducible two-dimensional representation of Q and we can attach an Artin representation

$$\rho_K : \mathrm{Gal}(K/\mathbb{Q}) \simeq Q \to \mathrm{GL}_2(\mathbb{C})$$

which is symplectic. We can view ρ_K as induced from a Hecke character of order 4 in a quadratic extension of $\mathbb{Q}$ inside K. Furthermore, it is known to correspond to an automorphic form on PGL_2, precisely to a (dihedral) Maass form of weight 0, eigenvalue $\frac{1}{4}$ and trivial nebentypus; see [14, Section 3] and the references therein.

EXAMPLE 1.3.

(i) Dedekind found that $K = \mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{6})})$ is a quaternionic extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (see [26]). The root number of ρ_K is $+1$.

(ii) The field $K = \mathbb{Q}(\sqrt{(5+\sqrt{5})(41+6\sqrt{41})})$ is a quaternionic extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{5}, \sqrt{41})$. The root number of ρ_K is -1.

To form a family, we fix an arbitrary quaternionic field K. Let $q \equiv 0, 1 \pmod 4$ be a fundamental discriminant that is coprime with the discriminant of K. Let χ_q be the associated quadratic Dirichlet character which we may also view as an Artin representation onto $\{\pm 1\} \subset \mathrm{GL}_1(\mathbb{C})$. Consider the Artin representation that is the character twist $\rho_K \otimes \chi_q$. Since $\mathrm{Gal}(K(\sqrt{q})/\mathbb{Q}) \simeq Q \times \mathbb{Z}/2\mathbb{Z}$ and the representation factors through the unique nontrivial surjection $Q \times \mathbb{Z}/2\mathbb{Z} \to Q$, which defines a unique quaternionic field K_q, $\rho_K \otimes \chi_q$ is the same as ρ_{K_q}. We call the field K_q a quadratic twist of K and obtain in this way a one-parameter family of quaternionic fields.

In Section 8 we give an equivalent description of K_q using a theorem of Witt [73], and relate this to a similar construction by Fröhlich [36]. This description also shows that the family is geometric in the sense that it arises as before from an 8-covering of $\mathbb{A}^1$. The following is a special case of results of Rubinstein [59] who treated families of quadratic twists of an arbitrary automorphic form on GL_n.

THEOREM 1.4. *Let K be a quaternionic field and consider the above one-parameter family of quaternionic Artin representations of K_q parametrized by discriminants q. The family is homogeneous symplectic, and it has* SO(even) *symmetry type if ρ_K has root number $+1$ and* SO(odd) *symmetry type if ρ_K has root number -1.*

In contrast to the quadratic twists of an elliptic curve where the root numbers fluctuate, we note the interesting phenomenon that the root numbers of the quadratic twists K_q of a quaternionic field are constant. We verify this in Section 8 where we give a brief exposition of the arithmetic of quaternionic fields gathering several results scattered in the literature.

Suppose that ρ_K has root number -1. It is believed that $\mathrm{ord}_{s=1/2}L(s, \rho_K) = 1$ and similarly for K_q for all q. This belief is reinforced by the SO(odd) symmetry type of the family which defines the same determinantal point process as the union of $\mathrm{Sp}(\infty)$ and a single zero at $\frac{1}{2}$.

In Section 4 we investigate two situations where one constructs a geometric family starting from another. The first construction is due to Davenport–Heilbronn. Starting from a binary cubic form $f \in V(\mathbb{Z})$ we attach the quadratic field whose discriminant is $\Delta(f)$. Geometrically this is a branched covering of V of degree two which is again GL_2-equivariant (to be compared with the branched covering of degree three parametrizing cubic fields). It is famously used to determine asymptotically the average size of the 3-part of the class group of quadratic fields. Unsurprisingly, we show in Section 4 the Sato–Tate equidistribution in $\mathcal{T}_2$ for this family. Similarly the second construction comes from Bhargava's parametrization of the pairs of quartic rings together with their resolvent rings. This yields a $\mathrm{GL}_2 \times \mathrm{SL}_3$-equivariant covering of degree three which can be used to determine the average size of the 2-part of the class group of cubic fields [7]. We prove that the Sato–Tate equidistribution in $\mathcal{T}_3$ holds for this family.

In all of the above families, the rank of the family is zero in the sense of [61]. The average trace of Frobenius is a Weil number of integer weight which geometrically comes from the fact that we are counting orbits of points of varieties over finite fields. Thus it is always the case that the rank is zero for any geometric family of number fields because the construction involves the H^0 of the zero-dimensional fibers. This is consistent with the belief that Artin L-functions never vanish at the central point except when forced by the root number being -1.

It would be interesting to obtain similar results when $\mathfrak{F}(x)$ is the set of all S_n-number fields of discriminant at most x. It is possible to view $\mathfrak{F}(x)$ as a parametric set by considering the configuration of n points in $\mathbb{P}^{n-2}$ modulo the action by GL_{n-1}. For $n \geqslant 4$, this yields an algebraic variety V which can always be cut out by a certain number of quadrics [72, Theorem 138]. A conjecture of Bhargava [9] predicts an asymptotic $|\mathfrak{F}(x)| \sim c_n x$ as $x \to \infty$ and moreover the mass conjecture [9] would also imply the Sato–Tate equidistribution. For $n \leqslant 5$ the variety V can be parametrized by a prehomogeneous group action on a vector space by the results of Davenport and Heilbronn [24] and Bhargava [5, 6] as mentioned above and $\mathfrak{F}$ becomes a geometric family in the sense of [61].

For $n \geqslant 6$ this is not the case and thus the study of rational points in $V(\mathbb{Z})$ is an extremely delicate problem. For the same reason it is not possible to include such parameter spaces in the definition of geometric families in [61]; working in such complete generality would allow too many pathologies in the asymptotic of families; see [61, Section 3.1].

As explained above, the families are obtained by a sieving process of the forms $f \in V(\mathbb{Z})$. In this process we can extract the forms f that give rise to number fields with a constant S_n Galois group. It is interesting to study what happens if we form families starting from the same space but without sieving. Then the Galois group of $M_f/\mathbb{Q}$ can vary with f. So we call these mixed families. These mixed families fit in the framework of [61] if we parametrize the contribution of the cusp. We shall explain that the Sato–Tate equidistribution holds for them. Interestingly it is shown in [75] that the family of D_4-fields ordered by discriminant does not have a mass formula. The Sato–Tate measure is a linear combination of Sato–Tate measures attached to the Haar measures on different Galois groups which occur with positive proportion. Serre also describes the possible Sato–Tate measures in this way in his recent book [63]. One interesting case is the mixture of S_4- and D_4-fields arising from pairs of ternary quadratic forms; see Section 6. Incidentally the quantitative equidistribution for the family of D_4-fields is not yet established.

Let us also mention some other open questions that arise from our perspective on families and on which we hope to return elsewhere. Besides the one-parameter families explored in Section 8 it would be interesting to study other families of quaternionic fields (see [34, 46]). In this paper we do not consider lower order terms as in, for example, [33]; these can be seen to be related to the counting measures on $V(\mathbb{Z}/p^r\mathbb{Z})$ of Section 7. Finally, it should be possible to improve the remainder terms and support for one-level density using for example large sieve inequalities and Fourier transforms of orbital measures.

2. General setup for zeta functions of degree *n* number fields

Some familiarity with the Katz–Sarnak heuristics or with [61] is helpful to understand the general context of the paper, but not necessary. Indeed we shall introduce the relevant concepts gradually, so that the paper can be read independently. L-functions and splitting types are discussed in Section 2.1. The Sato–Tate group, Sato–Tate measure, and Frobenius–Schur indicator are defined in Section 2.2. The étale cohomology formalism is used in Section 2.2 only to make clear how the present constructions for families of number fields generalize to arbitrary families of higher-dimensional varieties. Then, in Section 2.3 we introduce the statistics of families and Sato–Tate equidistribution. Section 2.4 concerns the 1-level density of low-lying zeros for the relevant families.

We show in Theorem 2.8 how this density can be deduced from the Sato–Tate equidistribution together with the rank of the family defined in Section 2.5. The final Section 2.6 discusses two additional invariants i_1 and i_2 from [61] which are important, but less directly relevant in our context. Finally we note that some concepts from the theory of automorphic forms are mentioned, such as unitary dual, Satake parameter, and modularity conjectures. This is only for motivation and convenience, and to have a unified framework that works for many different types of families. No result about automorphic forms is actually used.

Let K be a degree-n number field with normal closure M. Then $\zeta_K(s)$ is the Artin L-function corresponding to the trivial representation of the absolute Galois group $\mathrm{Gal}(K) = \mathrm{Gal}(\overline{K}/K)$, which is an index n subgroup of $\mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and we have

$$\zeta_K(s) = L(s, \mathrm{Ind}_{\mathrm{Gal}(K)}^{\mathrm{Gal}(\mathbb{Q})} 1).$$

The representation $\mathrm{Ind}_{\mathrm{Gal}(K)}^{\mathrm{Gal}(\mathbb{Q})} 1$ of $\mathrm{Gal}(\mathbb{Q})$ factors through $\mathrm{Gal}(M/\mathbb{Q}) \hookrightarrow S_n$ and decomposes into the direct sum of the trivial representation and the composition with the standard representation $\rho : S_n \to \mathrm{GL}_{n-1}(\mathbb{C})$. Therefore, we have

$$\zeta_K(s) = \zeta(s) L(s, \rho_K), \tag{3}$$

where $\zeta(s)$ is the Riemann zeta function and $L(s, \rho_K)$ is the Artin L-function corresponding to

$$\rho_K : \mathrm{Gal}(\mathbb{Q}) \to \mathrm{Gal}(M/\mathbb{Q}) \hookrightarrow S_n \to \mathrm{GL}_{n-1}(\mathbb{C}). \tag{4}$$

Note that the conductor of $L(s, \rho_K)$ is equal to the conductor of $\zeta_K(s)$. We denote it by C_K. It follows from Artin's conductor-discriminant formula that C_K is equal to the absolute value of the discriminant $\Delta(K)$ of the number field K.

We will study the statistics of the low-lying zeros of $L(s, \rho_K)$ by summing these zeros against a test function always denoted by f. We pick f to be an even function on $\mathbb{R}$, such that its Fourier transform

$$\widehat{f}(x) := \int_{-\infty}^{\infty} f(y) e^{-2\pi i x y}\, dy \tag{5}$$

is smooth, and of compact support. If $\widehat{f}$ has support contained in $[-\alpha, \alpha]$, then f can be extended to an entire function of exponential type α. The first step toward understanding the statistics of the zeros of $L(s, \rho_K)$ is the explicit formula. For each $m \geqslant 1$, we write $\lambda_K(m)$ for the Dirichlet coefficients of $L(s, \rho_K)$. Note that λ_K is integer valued and that $\sum_{d|m} \lambda_K(d)$ is the number of ideals of K of norm m. We write the logarithmic derivative of $L(s, \rho_K)$ for $\Re(s) > 1$ as

$$-\frac{L'}{L}(s, \rho_K) = \sum_{m=1}^{\infty} \frac{\theta_K(m) \Lambda(m)}{m^s}, \tag{6}$$

where Λ is the von Mangoldt function. We state the explicit formula in the form of [60, Proposition 2.1]:

We write the nontrivial zeros of $L(s, \rho_K)$ as $\frac{1}{2} + i\gamma_K^{(j)}$, where the imaginary parts of $\gamma_K^{(j)}$ have absolute value bounded by $1/2$. (Under GRH, the $\gamma_K^{(j)}$ are real.) Similarly we denote the poles of $L(s, \rho_K)$ by $\frac{1}{2} + ir_K^{(j)}$.

Proposition 2.1. *With notation as above, if K is a degree-n number field and f is an even function whose Fourier transform is smooth and of compact support, then*

$$\sum_j f(\gamma_K^{(j)}) - \sum_j f(r_K^{(j)}) = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(t)(\log C_K + O(1))\,dt - \frac{1}{\pi}\sum_{m=1}^{\infty}\frac{\theta_K(m)\Lambda(m)}{\sqrt{m}}\widehat{f}\left(\frac{\log m}{2\pi}\right). \tag{7}$$

2.1. Frobenius and splitting types. Let p be a prime that is unramified in K. Let $\mathcal{O}_K$ denote the ring of integers of K and write

$$\mathcal{O}_K/(p) = \mathbb{F}_{p^{f_1}} \oplus \mathbb{F}_{p^{f_2}} \oplus \cdots \oplus \mathbb{F}_{p^{f_k}},$$

with $f_1 \geqslant f_2 \geqslant \cdots \geqslant f_k$. Then the *splitting type* of p in K is defined to be $(f_1 f_2 \cdots f_k)$. Thus, the set of possible splitting types for unramified primes can be naturally identified with the set of partitions of n, or equivalently with $\mathcal{T}_n$, the set of conjugacy classes of S_n.

Our goal now is to relate the splitting type $\tau \in \mathcal{T}_n$ of p to the coefficients of the Euler factor at p of the L-function $L(s, \rho_K)$. To this end, we need to relate it to the Frobenius conjugacy class of p in $\mathrm{Gal}(M/\mathbb{Q})$. We follow the short and elegant exposition of Wood [77].

Let $\mathfrak{p} \subset M$ be a fixed prime ideal lying above the unramified prime p, and let $G_{\mathfrak{p}}$ denote the decomposition group. This group is cyclic and is generated by $\mathrm{Frob}_{M/\mathbb{Q}}\mathfrak{p}$. The conjugacy class of $\mathrm{Frob}_{M/\mathbb{Q}}\mathfrak{p}$ is independent of the choice of $\mathfrak{p}$ above p and from now on we denote this class by Frob_p. Then the splitting type of p and the action of Frob_p correspond to the same partition of n. Equivalently $\rho(\tau)$ and $\rho(\mathrm{Frob}_p)$ are conjugate. We denote this by writing $\rho(\tau) \sim \rho(\mathrm{Frob}_p)$.

Lemma 2.2. *Let χ denote the character of the standard representation ρ of S_n. If p is unramified in K and its splitting type is $\tau \in \mathcal{T}_n$, then we have $\theta_K(p^k) = \chi(\tau^k)$ for all $k \geqslant 0$. Furthermore, for any rational prime p and $k \geqslant 0$, we have $|\theta_K(p^k)| \leqslant n - 1$.*

Proof. Suppose that the splitting type of p in K is $\tau \in \mathcal{T}_n$. Since p does not ramify in K, the Euler factor $L_p(s, \rho_K)$ at p is equal to

$$\det(I - p^{-s}\rho_K(\mathrm{Frob}_p))^{-1} = \det(I - p^{-s}\rho(\tau))^{-1} = \prod_{i=1}^{n-1}(1 - \alpha_i p^{-s})^{-1}$$

where $\alpha_1, \ldots, \alpha_{n-1}$ denote the eigenvalues of $\rho(\tau)$. The identity holds for $\Re(s) > 1$, since $|\alpha_i| = 1$ for all i and the eigenvalues of $\rho(\tau^k)$ are α_i^k. In particular $\lambda_K(p^k) = s_r(\alpha_1, \ldots, \alpha_{n-1}) = \mathrm{tr}(\mathrm{sym}^k \rho(\tau))$, where s_r is a Schur polynomial.

Computing the logarithmic derivative, we obtain

$$\begin{aligned}\frac{L_p'}{L_p}(s, \rho_K) &= \left(\sum_{i=1}^{n-1}\sum_{k\geqslant 1}\frac{1}{k}\alpha_i^k p^{-ks}\right)' = -\sum_{k\geqslant 1}\left(\sum_{i=1}^{n-1}\alpha_i^k\right)(\log p)p^{-ks}\\ &= -\log p \sum_{k\geqslant 1}\frac{\chi(\tau^k)}{p^{ks}}.\end{aligned}$$

Comparing this with (6) yields $\theta_K(p^k) = \sum_{i=1}^{n-1}\alpha_i^k = \chi(\tau^k)$ which is the first assertion of the lemma.

For any prime p, the Artin formula states that

$$L_p(s, \rho_K) = \det(1 - p^{-s}\rho_K(\mathrm{Frob}_p)|V^{\rho_K(I_p)})^{-1}$$

is the Euler factor of $L(s, \rho_K)$ at p, where $V = \mathbb{C}^{n-1}$ is the underlying space of ρ_K and $V^{\rho_K(I_p)}$ is the subspace of V where the inertia group I_p acts trivially. The second assertion now follows similarly as in the unramified case since the eigenvalues of $\rho_K(\mathrm{Frob}_p)$ have absolute value 1. □

Remark 2.3. The relation between the two arithmetic functions λ_K and θ_K follows either by computing the logarithmic derivative in (6), or by expressing elementary symmetric polynomials in terms of Schur polynomials. For example $\theta_K(p) = \lambda_K(p)$ for all primes p. Whereas, $\theta_K(p^2) = 2\lambda_K(p^2) - \lambda_K(p)^2$, and $\theta_K(p^3) = 3\lambda_K(p^3) - 3\lambda_K(p)\lambda_K(p^2) + \lambda_K(p)^3$, and similar formulas for higher powers.

If K is an S_n-number field we can illustrate the above construction further. The subfield K of M corresponds to a subgroup S_{n-1} of S_n, and the different embeddings $K \hookrightarrow M$ correspond to cosets $S_{n-1}\backslash S_n$. The group $G_{\mathfrak{p}}$ acts on the coset space $S_{n-1}\backslash S_n$. Let $O_1, \ldots, O_k$ be the corresponding set of orbits, ordered by size. Then the splitting type of p in K is $\tau = (\#O_1 \cdots \#O_k)$. We identify

Frob_p with a conjugacy class in S_n and can simply write $\mathrm{Frob}_p = \tau \in \mathcal{T}_n$ instead of $\rho_K(\mathrm{Frob}_p) = \rho(\tau)$.

2.2. Finite étale coverings and the Sato–Tate group.

For each of the families $\mathfrak{F}$ considered in this paper we have a branched covering $X \to V$ of degree n. The ramified locus on V is given by the equation $\Delta = 0$. The restriction of the covering to $V^{\Delta\neq 0}$ is finite étale and the normal closure has Galois group $H \hookrightarrow S_n$. The Sato–Tate group of $\mathfrak{F}$ is defined to be H.

REMARK 2.4. This is a special case of [42] and [61, Section 2.11] which treat the monodromy of general geometric families. For number field families, the formalism of étale cohomology is not directly needed because the action of $\mathrm{Gal}(\mathbb{Q})$ factors through a finite quotient, thus the relevant representations can be expressed in classical terms.

Indeed, for each $f \in V(\mathbb{Z})$ such that $\Delta(f) \neq 0$, the fiber X_f consists of n points defined over $\mathbb{Z}$. The individual points themselves are elements of $\mathbb{P}^k(\overline{\mathbb{Q}})$, for some k depending on V, but X_f considered as a scheme is defined over $\mathbb{Z}$. For example, when V is the space of binary cubic forms, the space X is the subset of $V \times \mathbb{P}^1$ consisting of elements (f, θ) such that $f(\theta) = 0$, and the fiber X_f can be identified with the three roots of f in $\mathbb{P}^1(\overline{\mathbb{Q}})$.

When V parametrizes S_n-fields for $n = 3$, 4, and 5, we have $k = 1$, 2, and 3, respectively. The action of $\mathrm{Gal}(\mathbb{Q})$ on $H^0_{\mathrm{et}}(X_f \times_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_\ell)$ factors through the standard representation of $\mathrm{Gal}(M_f/\mathbb{Q})$. The degree-$n$ field K_f is cut out by the stabilizer of this action. Moreover, the cohomology of fibers induces a lisse sheaf on $V^{\Delta\neq 0}$ of dimension $n-1$ whose stalk over each $f \in V(\mathbb{Q})^{\Delta\neq 0}$ is isomorphic to $K_f/\mathbb{Q}$. There is a monodromy action by $\pi_1(V^{\Delta\neq 0})$ and the image is $H \hookrightarrow S_n \subset \mathrm{GL}_{n-1}(\mathbb{Q}_\ell)$.

The Sato–Tate measure $\mu_{\mathrm{ST}}(\mathfrak{F})$ attached to the family is the pushforward of the Haar measure of H to the space $\mathbb{T} := (S^1)^{n-1}/S_{n-1}$ which we identify with the set of conjugacy classes of semisimple matrices in the compact unitary group $U_{n-1} \subset \mathrm{GL}_{n-1}(\mathbb{C})$. The measure is independent of the choices of the embeddings $H \hookrightarrow S_n$, and $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. By construction, it is supported inside $\mathcal{T}_n$, for the natural inclusion $\mathcal{T}_n \subset \mathbb{T}$. Let

$$i_3(\mathfrak{F}) := \int_{\mathbb{T}} \mathrm{tr}(t^2)\mu_{ST}(\mathfrak{F})(dt) = \frac{1}{|H|}\sum_{\tau\in H} \mathrm{tr}(\tau^2) \in \mathbb{Z}.$$

If $H \hookrightarrow \mathrm{GL}_{n-1}(\mathbb{C})$ acts irreducibly, then $i_3(\mathfrak{F}) \in \{-1, 0, 1\}$ is the Frobenius–Schur indicator. Depending on whether $i_3(\mathfrak{F}) = -1, 0, 1$, we say [61] that $\mathfrak{F}$ is homogeneous symplectic, respectively unitary, orthogonal.

EXAMPLE 2.5. If the normal closure of the covering $X \to V$ has Galois group $H \simeq S_n$, then we say that $\mathfrak{F}$ is an S_n-family. In this case,

$$\mu_{\mathrm{ST}}(\mathfrak{F})(\{\tau\}) = \frac{|\tau|}{|S_n|} \tag{8}$$

for every $\tau \in \mathcal{T}_n$, as follows from the definition of $\mu_{\mathrm{ST}}(\mathfrak{F})$. Hence $i_3(\mathfrak{F}) = 1$, because the indicator of $S_n \subset \mathrm{GL}_{n-1}(\mathbb{C})$ is $+1$, a result which goes back to Frobenius and Schur [35]; see [23, Theorem 3.1, p. 151] for a historical account. Indeed S_n acts irreducibly on $\mathbb{C}^{n-1}$, and preserves a symmetric bilinear form, which comes from the standard quadratic form on $\mathbb{C}^n$; equivalently the representation is real, which can be seen by representing elements of S_n by permutation matrices. (In fact all irreducible representations of S_n are defined over $\mathbb{Q}$.) Thus an S_n-family $\mathfrak{F}$ is homogeneous orthogonal, which is how one verifies the first claim of Theorem 1.1, and of Theorem 1.2.

For each prime p we can base change to the finite field $\mathbb{F}_p$. If $\Delta(f) \not\equiv 0 \pmod{p}$ then $X_f \otimes_{\mathbb{Z}} \mathbb{F}_p$ is reduced, and the same construction yields an action of $\mathrm{Gal}(\mathbb{F}_p)$. Since R_f is maximal at p, the action of Frobenius determines the splitting type of p in K_f. In particular the local L-factor $L_p(s, \rho_{K_f})$ is uniquely determined by the base change data of $R_f \otimes_{\mathbb{Z}} \mathbb{F}_p$. This is a fact that we shall use repeatedly and which is a special case of a theorem of Grothendieck [27]. If moreover the covering is G-equivariant for some algebraic group G, then the action carries over to the reductions mod p and we obtain a $G(\mathbb{F}_p)$-action on $V(\mathbb{F}_p)^{\Delta\neq 0}$.

It is possible to prove [42, 61] in this generality that

$$\{\rho_{K_f}(\mathrm{Frob}_p) : f \in V(\mathbb{F}_p)^{\Delta\neq 0}\} \tag{9}$$

is equidistributed as $p \to \infty$ with respect to the Sato–Tate measure $\mu_{\mathrm{ST}}(\mathfrak{F})$.

2.3. Families of degree-n number fields.

In this subsection, we assume that we start with a parametric family $\mathfrak{F}$ of degree-n number fields as above. Recall that we abuse notation and refer to both the family of number fields and the family of associated L-functions by $\mathfrak{F}$.

We order the elements of $\mathfrak{F}$ by a height function $h : \mathfrak{F} \to \mathbb{R}_{>0}$. When possible we choose $h(K)$ to be $|\Delta(K)|$ which is equal to the conductor C_K of the corresponding L-function $L(s, \rho_K)$. This happens in Sections 3 and 4. However, in some other cases where it is difficult to count elements in $\mathfrak{F}$ having bounded discriminant, we choose h to be an approximation of $|\Delta|$, such as in Section 5.2. For $x \in \mathbb{R}_{\geqslant 1}$ we define

$$\mathfrak{F}(x) = \{K \in \mathfrak{F} : h(K) < x\}.$$

Moreover for a prime p, and $\tau \in \mathcal{T}_n$, define

$$\begin{aligned}\mathfrak{F}^{p\nmid\Delta}(x) &= \{K \in \mathfrak{F}(x) : p \nmid \Delta(K)\},\\ \mathfrak{F}^{p,\tau}(x) &= \{K \in \mathfrak{F}^{p\nmid\Delta}(x) : \rho_K(\mathrm{Frob}_p) \sim \rho(\tau)\},\\ \mathfrak{F}^{p|\Delta}(x) &= \{K \in \mathfrak{F}(x) : p \mid \Delta(K)\}.\end{aligned}$$

Note that we have disjoint decompositions

$$\mathfrak{F}(x) = \mathfrak{F}^{p\nmid\Delta}(x) \sqcup \mathfrak{F}^{p|\Delta}(x) \quad \text{and} \quad \mathfrak{F}^{p\nmid\Delta}(x) = \bigsqcup_{\tau\in\mathcal{T}_n} \mathfrak{F}^{p,\tau}(x).$$

The main input will be a counting result that estimates the number of elements in $\mathfrak{F}^{p,\tau}(x)$ with a power saving error term that satisfies some uniformity over p. In the context of Theorems 1.1, 1.2, and 1.4, we shall establish that equidistribution holds for individual primes in the sense that there exist constants $\delta_1 < \delta_0 < 1$ and $0 < A, B < \infty$, and for each prime p and $\tau \in \mathcal{T}_n$ constants $0 < c_{p,\tau}, c_{p|\Delta} < 1$ such that for all $x \geqslant 1$:

$$\begin{aligned}|\mathfrak{F}^{p,\tau}(x)| &= c_{p,\tau}|\mathfrak{F}(x)| + O(|\mathfrak{F}(x)|^{\delta_0}) + O(|\mathfrak{F}(x)|^{\delta_1} p^A);\\ |\mathfrak{F}^{p|\Delta}(x)| &= c_{p|\Delta}|\mathfrak{F}(x)| + O(|\mathfrak{F}(x)|^{\delta_0}) + O(|\mathfrak{F}(x)|^{\delta_1} p^B).\end{aligned} \tag{10}$$

REMARK 2.6. The remainder terms in (10) are all dominated by $O(|\mathfrak{F}(x)|^{\delta_0} p^{\max(A,B)})$ which would be sufficient for our purpose to establish the statistics of low-lying zeros for some positive support. However, we write the formulas (10) in this more precise form because this is what the proof naturally produces for geometric families and this yields an improved support.

The constants $c_{p,\tau}$ in fact determine the unramified part of the probability measure $\mu_p(\mathfrak{F})$ from [61, Conjecture 1]. The ramified part of the measure $\mu_p(\mathfrak{F})$ is more complicated and will be discussed in Section 7. It is clear that for every prime p,

$$c_{p|\Delta} + \sum_{\tau\in\mathcal{T}_n} c_{p,\tau} = 1.$$

Recall from the previous Section 2.2 that the standard representation $S_n \hookrightarrow U_{n-1} \subset \mathrm{GL}_{n-1}(\mathbb{C})$ induces a natural inclusion $\mathcal{T}_n \subset \mathbb{T}$. Concretely, say that $\tau \in \mathcal{T}_n$ corresponds to the partition $(f_1 f_2 \cdots f_k)$ of the integer n. Then we form the n-tuple of f_ith roots of unity, for $1 \leqslant i \leqslant k$, which is an element of $(S^1)^n$, and we remove the trivial root 1 once, to obtain an element of $\mathbb{T} = (S^1)^{n-1}/S_{n-1}$.

Up to a scalar, $\mu_p(\mathfrak{F})$ is the counting measure on the set (9) of splitting types modulo p. Precisely, the unramified part $\mu_p(\mathfrak{F})_{|\mathbb{T}}$ is supported on $\mathcal{T}_n \subset \mathbb{T}$, and for every $\tau \in \mathcal{T}_n$,

$$\mu_p(\mathfrak{F})(\{\tau\}) = c_{p,\tau}.$$

Thus the unramified part $\mu_p(\mathfrak{F})_{|\mathbb{T}}$ is a measure of total mass $\mu_p(\mathfrak{F})(\mathbb{T}) = 1 - c_{p|\Delta}$.

For the families $\mathfrak{F}$ obtained by application of a square-free sieve to $V(\mathbb{Z})$, we have that $c_{p,\tau}$ is given by a p-adic density. In all such cases we have the identity

$$\frac{c_{p,\tau}}{1 - c_{p|\Delta}} = \frac{|V(\mathbb{F}_p)^{\tau}|}{|V(\mathbb{F}_p)^{\Delta\neq 0}|},$$

where $V(\mathbb{F}_p)^{\tau}$ is the set of all elements in $V(\mathbb{F}_p)$ having splitting type τ. Thus in view of Section 2.2, and the fact that $c_{p|\Delta} \to 0$, we have

$$\mu_p(\mathfrak{F})_{|\mathbb{T}} \rightharpoonup \mu_{\mathrm{ST}}(\mathfrak{F}).$$

Equivalently for each $\tau \in \mathcal{T}_n$, we have that $c_{p,\tau}$ converges to $\mu_{\mathrm{ST}}(\mathfrak{F})(\{\tau\})$ as $p \to \infty$. Hence, averaging over primes p less than y, we have that (10) implies Sato–Tate equidistribution of $\mathfrak{F}$ in the sense of [61]:

$$\lim_{y\to\infty} \lim_{x\to\infty} \frac{1}{|\mathfrak{F}(x)| \cdot \pi(y)} \sum_{p<y} |\mathfrak{F}^{p,\tau}(x)| = \mu_{\mathrm{ST}}(\mathfrak{F})(\{\tau\}), \tag{11}$$

and more precisely that the convergence of (11) holds uniformly as soon as $\log|\mathfrak{F}(x)|/\log y$ is greater than $A/(1-\delta_1)$.

REMARK 2.7. Above the limits are taken in the order $x \to \infty$ then $y \to \infty$. If we were to take the limits in the opposite order, then the equidistribution would follow from the Chebotarev density theorem, assuming that one knows most number fields $K \in \mathfrak{F}(x)$ have a fixed group as Galois group for their normal closure.

One quantity that is especially important in the study of $\mathfrak{F}$ is the average trace of unramified Frobenius. With the above notation it can be expressed as

$$t_{\mathfrak{F}}(p) := \sum_{\tau\in\mathcal{T}_n} c_{p,\tau}\chi(\tau) = \int_{\mathbb{T}} \mathrm{tr}(t)\mu_p(\mathfrak{F})(dt).$$

2.4. The 1-level density of low-lying zeros of S_n-families.

In this subsection we compute the 1-level density of the low-lying zeros of the Artin L-functions of the families considered in Sections 3, 4, and 5. We do this calculation in the 'traditional' way, and we explain at the same time how the main term can be found conceptually from the Sato–Tate measure as in [61, 65].

The above families are S_n-families, and thus the Sato–Tate measure $\mu_{\mathrm{ST}}(\mathfrak{F})$ is given by (8). In fact, in Sections 3, 4 and 5 we will establish that each of these S_n-families satisfy the Sato–Tate equidistribution (10) (with constants δ_0, δ_1, A, B) and that $|\mathfrak{F}(x)| \asymp x^\theta$ for some $\theta > 0$. Furthermore, in these cases we will also prove the following regarding the constants $c_{p,\tau}$ and $c_{p|\Delta}$: for any prime p and $\tau \in \mathcal{T}_n$, we have

$$c_{p,\tau} = \frac{|\tau|}{|S_n|} + O\left(\frac{1}{p}\right), \tag{12}$$

where $|\tau|$ denotes the size of the conjugacy class τ in S_n. In particular $c_{p|\Delta} = O(1/p)$ since $\sum_{\tau\in\mathcal{T}_n}(|\tau|/|S_n|) = 1$ and also we recover that $t_{\mathfrak{F}}(p) = O(1/p)$ since $\sum_{\tau\in\mathcal{T}_n}\chi(\tau)(|\tau|/|S_n|) = 0$.

One reason to refer to these families as S_n-families is that a consequence of (12) is that most $K \in \mathfrak{F}(x)$ are S_n-fields in the sense that S_n is the Galois group of their normal closure. Indeed this follows in the same way as Hilbert's irreducibility theorem by applying a sieve to construct Frobenius elements which are n-cycles and transpositions.

Let f be a fixed even function whose Fourier transform is smooth and of compact support, as in the beginning of Section 2. We are interested in evaluating

$$\lim_{x\to\infty}\frac{1}{|\mathfrak{F}(x)|}\sum_{K\in\mathfrak{F}(x)}\sum_j f\left(\frac{\gamma_K^{(j)}\mathcal{L}}{2\pi}\right),$$

where $\mathcal{L}$ will be picked so that we capture the statistics of the low-lying zeros. The natural choice for $\mathcal{L}$ is $\log C_K$, where C_K is the conductor of $L(s, \rho_K)$, because we expect the lowest zeros of $L(s, \rho_K)$ to be at height around $2\pi/\log C_K$. However, we pick $\mathcal{L} = \mathcal{L}(x)$ to be

$$\mathcal{L} := \frac{1}{|\mathfrak{F}(x)|}\sum_{K\in\mathfrak{F}(x)}\log C_K, \tag{13}$$

the average of these natural choices. In view of the counting asymptotic in (10), we have

$$\mathcal{L} = (1 + o(1))\log x \quad \text{as } x \to \infty \tag{14}$$

if $h(K)$ equals or closely approximates C_K, that is, if the family is ordered by a quantity that closely approximates the absolute discriminant. In all our examples, this will be true.

THEOREM 2.8. *Let $\mathfrak{F}$ be one of the S_n-families of Sections 3, 4 and 5. If f is a function whose Fourier transform is smooth and has support in $[-\alpha, \alpha]$ for*

$$\alpha < \min\left(2\theta(1-\delta_0), \frac{2\theta(1-\delta_1)}{2C+1}\right),$$

where $C := \max(A, B)$, *then*

$$\lim_{x\to\infty} \frac{1}{|\mathfrak{F}(x)|} \sum_{K\in\mathfrak{F}(x)} \sum_{j} f\left(\frac{\gamma_K^{(j)}\mathcal{L}}{2\pi}\right) = \widehat{f}(0) - \frac{f(0)}{2}. \tag{15}$$

The limit (15) is the Katz–Sarnak heuristics for the one-level density with restricted support. Note that $\alpha < 1$ in all these examples. The interpretation of the minus sign in the second term is that $\mathfrak{F}$ has Symplectic symmetry type.

REMARK 2.9. In later sections, we shall discuss other families $\mathfrak{F}$ for which the Sato–Tate measure $\mu_{\mathrm{ST}}(\mathfrak{F})$ is different from (8). For example, in Section 8 we investigate a family of quaternionic extensions where the Sato–Tate group is $Q_8 \subset \mathrm{GL}_2(\mathbb{C})$. Also, in Section 6 we investigate families where the Sato–Tate group is $D_4 \subset \mathrm{GL}_2(\mathbb{C})$ as well as the reducible examples $C_3 \subset \mathrm{GL}_2(\mathbb{C})$ and $D_4 \subset \mathrm{GL}_3(\mathbb{C})$. In those cases the right-hand side of (15) should be replaced by $\widehat{f}(0) - i_3(\mathfrak{F})(f(0)/2)$, where $i_3(\mathfrak{F})$ is the Frobenius–Schur indicator of $\mu_{\mathrm{ST}}(\mathfrak{F})$.

Proof. Without loss of generality we may assume that f is even because $L(s, \rho_K)$ is self-dual and thus γ is a zero if and only if $-\gamma$ is a zero. We use (7) to write the above as the limit as $x \to \infty$ of

$$\frac{1}{|\mathfrak{F}(x)|} \sum_{K\in\mathfrak{F}(x)} \left(\frac{1}{2\pi}\int_{-\infty}^{\infty} f\left(\frac{t\mathcal{L}}{2\pi}\right)(\log C_K + O(1))\,dt \right.$$
$$\left. - \frac{2}{\mathcal{L}} \sum_{m=1}^{\infty} \frac{\theta_K(m)\Lambda(m)}{\sqrt{m}} \widehat{f}\left(\frac{\log m}{\mathcal{L}}\right) + \sum_j f\left(\frac{r_K^{(j)}\mathcal{L}}{2\pi}\right)\right). \tag{16}$$

Here the contribution from the sum over poles of $L(s, \rho_K)$ is negligible (that is, $o(1)$) because the test function f is assumed to be of rapid decay and the only possible locations for poles of $L(s, \rho_K)$ are at the zeros of $\zeta(s)$ (cf. (3)). Furthermore, since $C_K \to \infty$ as $h(K) \to \infty$, we can evaluate the limit of the first part of (16) to be

$$\begin{aligned} &\lim_{x\to\infty} \frac{1}{|\mathfrak{F}(x)|} \sum_{K\in\mathfrak{F}(x)} \frac{1}{2\pi} \int_{-\infty}^{\infty} f\left(\frac{t\mathcal{L}}{2\pi}\right)(\log C_K + O(1))\,dt \\ &= \lim_{x\to\infty} \frac{1}{\mathcal{L}|\mathfrak{F}(x)|} \sum_{K\in\mathfrak{F}(x)} \log C_K \int_{-\infty}^{\infty} f(t)(1 + o(1))\,dt \\ &= \int_{-\infty}^{\infty} f(t)\,dt = \widehat{f}(0). \end{aligned} \tag{17}$$

To evaluate the limit of the second part of (16), we note that

$$\begin{aligned}\frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{K\in\mathfrak{F}(x)}\sum_{m=1}^{\infty}\frac{\theta_K(m)\Lambda(m)}{\sqrt{m}}\widehat{f}\left(\frac{\log m}{\mathcal{L}}\right)\\ =\frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p,k\geqslant 1}\frac{\log p}{p^{k/2}}\widehat{f}\left(\frac{k\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}(x)}\theta_K(p^k),\end{aligned}\tag{18}$$

where the change in the order of summation is justified because $\widehat{f}$ has compact support, and hence the sums over m, p and k are finitely supported. We write the right-hand side of the above equation as the limit as $x\to\infty$ of $\mathcal{S}_1+\mathcal{S}_2+\mathcal{S}_3+\mathcal{S}_{\text{ram}}$, where

$$\begin{aligned}\mathcal{S}_1 &:= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p}\frac{\log p}{\sqrt{p}}\widehat{f}\left(\frac{\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}^{p\nmid\Delta}(x)}\theta_K(p);\\ \mathcal{S}_2 &:= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p}\frac{\log p}{p}\widehat{f}\left(\frac{2\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}^{p\nmid\Delta}(x)}\theta_K(p^2);\\ \mathcal{S}_3 &:= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p,k\geqslant 3}\frac{\log p}{p^{k/2}}\widehat{f}\left(\frac{k\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}^{p\nmid\Delta}(x)}\theta_K(p^k);\\ \mathcal{S}_{\text{ram}} &:= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p,k\geqslant 1}\frac{\log p}{p^{k/2}}\widehat{f}\left(\frac{k\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}^{p|\Delta}(x)}\theta_K(p^k).\end{aligned}\tag{19}$$

To evaluate the sums (19), we begin by writing

$$\begin{aligned}\mathcal{S}_1 &= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p}\frac{\log p}{\sqrt{p}}\widehat{f}\left(\frac{\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}^{p\nmid\Delta}(x)}\theta_K(p)\\ &= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p}\frac{\log p}{\sqrt{p}}\widehat{f}\left(\frac{\log p}{\mathcal{L}}\right)\sum_{\tau\in\mathcal{T}_n}|\mathfrak{F}^{p,\tau}(x)|\chi(\tau)\\ &= \frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{p}\frac{\log p}{\sqrt{p}}\widehat{f}\left(\frac{\log p}{\mathcal{L}}\right)\\ &\quad\times(t_{\mathfrak{F}}(p)|\mathfrak{F}(x)|+O(|\mathfrak{F}(x)|^{\delta_0})+O(|\mathfrak{F}(x)|^{\delta_1}p^{A}))\\ &= O\left(\frac{1}{\mathcal{L}}\right)+O\left(\frac{e^{\mathcal{L}\alpha/2}}{|\mathfrak{F}(x)|^{1-\delta_0}\mathcal{L}}\right)+O\left(\frac{e^{\mathcal{L}\alpha(A+(1/2))}}{|\mathfrak{F}(x)|^{1-\delta_1}\mathcal{L}}\right),\end{aligned}\tag{20}$$

where the final equality follows by computing the third line of (20) using the fact that since $\widehat{f}$ is supported on $[-\alpha,\alpha]$, the sum over p can be restricted to the range $p \leqslant e^{\mathcal{L}\alpha}$; the bounds follow from Lemma 2.2, (10), and the fact that $t_{\mathfrak{F}}(p) = O(1/p)$. Similarly, we have

$$\begin{aligned}
\mathcal{S}_2 &= \frac{2}{\mathcal{L}} \sum_p \frac{\log p}{p} \widehat{f}\left(\frac{2\log p}{\mathcal{L}}\right) \sum_{\tau \in \mathcal{T}_n} \chi(\tau^2) \frac{|\tau|}{|S_n|} \\
&\quad + O\left(\frac{1}{|\mathfrak{F}(x)|^{1-\delta_0}}\right) + O\left(\frac{e^{(\mathcal{L}\alpha A)/2}}{|\mathfrak{F}(x)|^{1-\delta_1}\mathcal{L}}\right) + O\left(\frac{1}{\mathcal{L}}\right), \\
\mathcal{S}_3 &= O\left(\frac{1}{\mathcal{L}}\right), \\
\mathcal{S}_{\mathrm{ram}} &= O\left(\frac{1}{\mathcal{L}|\mathfrak{F}(x)|} \sum_{p,k \geqslant 1} \frac{\log p}{p^{k/2}} \left|\widehat{f}\left(\frac{k \log p}{\mathcal{L}}\right)\right| \right. \\
&\quad \left. \times \left(\frac{|\mathfrak{F}(x)|}{p} + |\mathfrak{F}(x)|^{\delta_0} + |\mathfrak{F}(x)|^{\delta_1} p^B\right)\right) \\
&= O\left(\frac{1}{\mathcal{L}}\right) + O\left(\frac{e^{(\mathcal{L}\alpha)/2}}{|\mathfrak{F}(x)|^{1-\delta_0}\mathcal{L}}\right) + O\left(\frac{e^{\mathcal{L}\alpha(B+(1/2))}}{|\mathfrak{F}(x)|^{1-\delta_1}\mathcal{L}}\right).
\end{aligned} \tag{21}$$

Therefore, in the limit $x \to \infty$, the only possible main term contribution to the right-hand side of (18) is from the sum $\mathcal{S}_2$.

The main term of $\mathcal{S}_2$ includes the sum

$$i_3(\mathfrak{F}) = \sum_{\tau \in \mathcal{T}_n} \chi(\tau^2) \frac{|\tau|}{|S_n|} = 1 \tag{22}$$

which is the Frobenius–Schur indicator of the representation $\rho : S_n \to \mathrm{GL}_{n-1}(\mathbb{C})$. (One advantage of our notation and setup is that this indicator arises naturally.) Therefore, the main term contribution from $\mathcal{S}_2$ is

$$\lim_{x \to \infty} \frac{2}{\mathcal{L}} \sum_p \frac{\log p}{p} \widehat{f}\left(\frac{2\log p}{\mathcal{L}}\right) = \int_0^\infty \widehat{f}(t)\, dt, \tag{23}$$

where the equality follows from the prime number theorem and integration by parts. Since the right-hand side of (23) is $f(0)/2$ by Fourier inversion, we have

$$\begin{aligned}
\frac{1}{|\mathfrak{F}(x)|} \sum_{K \in \mathfrak{F}(x)} \sum_j f\left(\frac{\gamma_K^{(j)}\mathcal{L}}{2\pi}\right) &= \widehat{f}(0) - \frac{f(0)}{2} + O\left(\frac{e^{(\mathcal{L}\alpha)/2}}{|\mathfrak{F}(x)|^{1-\delta_0}\mathcal{L}}\right) \\
&\quad + O\left(\frac{e^{\mathcal{L}\alpha(C+1/2)}}{|\mathfrak{F}(x)|^{1-\delta_1}\mathcal{L}}\right) + o(1),
\end{aligned} \tag{24}$$

where $C = \max(A, B)$. This indicates the symplectic symmetry type for the low-lying zeros of L-functions in these families.

Finally, we assume there exists $\theta > 0$ such that $|\mathfrak{F}(x)| \asymp x^{\theta}$. This will be true in all the S_n-families that we consider. Therefore, by (14), we have

$$\frac{e^{(\mathcal{L}\alpha)/2}}{|\mathfrak{F}(x)|^{1-\delta_0}\mathcal{L}} + \frac{e^{\mathcal{L}\alpha(C+1/2)}}{|\mathfrak{F}(x)|^{1-\delta_1}\mathcal{L}} = x^{(\alpha/2)-\theta(1-\delta_0)+o(1)} + x^{\alpha(C+1/2)-\theta(1-\delta_1)+o(1)}.$$

We conclude that the error terms in (24) will be bounded by $o(1)$ whenever

$$\alpha < \min\left(2\theta(1-\delta_0), \frac{2\theta(1-\delta_1)}{2C+1}\right).$$

This concluses the proof. □

2.5. Rank of families.

Recall that we used the estimate $t_{\mathfrak{F}}(p) = O(1/p)$, which follows from (12), in the proof of Theorem 2.8, specifically in the estimation of $\mathcal{S}_1$. The interpretation is that the rank of these number field families is zero, namely

$$\lim_{y\to\infty} \frac{1}{y} \sum_{p<y} -t_{\mathfrak{F}}(p) p^{1/2} \log p = 0.$$

This is consistent with the belief that each irreducible Artin L-function is nonvanishing at the central point unless the epsilon factor is -1 in which case it is believed to vanish with order one. The rank, defined by the above limit, can be nonzero for example in families of elliptic curves.

2.6. Other indicators of S_n-families.

The other indicators defined in [61], that is

$$i_1(\mathfrak{F}) := \int_{\mathbb{T}} |\mathrm{tr}(t)|^2 \mu_{ST}(\mathfrak{F})(dt), \quad i_2(\mathfrak{F}) := \int_{\mathbb{T}} \mathrm{tr}(t)^2 \mu_{ST}(\mathfrak{F})(dt),$$

are not directly used in the proof of Theorem 2.8. Suppose that $\mathfrak{F}$ is a family of Artin L-functions with Sato–Tate group $H \subset GL_{n-1}(\mathbb{C})$. Let χ be the trace character. Then note that i_1 exactly picks out the inner product

$$\langle \chi, \chi \rangle := \frac{1}{|H|} \sum_{h\in H} \chi(h)^2,$$

which is 1 if and only if H acts irreducibly. In that case, i_2, which in general is equal to $\langle \chi, \bar{\chi} \rangle$, is 1 if H is self-dual and 0 otherwise.

For families of zeta functions of degree-n S_n-fields, we have $H = S_n$, in the standard representation in $\mathrm{GL}_{n-1}(\mathbb{C})$. In this case, the indicators satisfy $i_1(\mathfrak{F}) = 1$ and $i_2(\mathfrak{F}) = 1$, expressing the fact that $S_n \subset \mathrm{GL}_{n-1}(\mathbb{C})$ acts irreducibly and is self-dual.

For S_n-families of Artin representations parametrized geometrically, one can establish by a sieve that most $K \in \mathfrak{F}(x)$ are S_n-fields. In particular most Artin L-functions $L(s, \rho_K)$ in an S_n-family are irreducible and self-dual orthogonal. The argument is unconditional taking advantage of the underlying algebraic structure and the finiteness of the Galois group. This is to be compared with [61] for general homogeneous families with $i_1(\mathfrak{F}) = i_2(\mathfrak{F}) = i_3(\mathfrak{F}) = 1$, where it is explained that this would also follow from the GRH by detecting the simple pole at $s = 1$ of the Rankin–Selberg product $L(s, \rho_K \times \tilde{\rho}_K)$ which implies irreducibility and similarly for $L(s, \mathrm{sym}^2 \rho_K)$ which implies orthogonality. The GRH is needed in [61] to truncate the Euler product to a small number of primes so that one can apply the quantitative Sato–Tate equidistribution for the family.

3. Parametrized families of cubic, quartic, and quintic fields

In this section, we consider parametrized families of cubic, quartic, and quintic fields. These families are constructed from certain prehomogeneous representations. A representation V of G is said to be *prehomogeneous* if V has a Zariski-dense G-orbit. Irreducible prehomogeneous representations of reductive groups over $\mathbb{C}$ were classified by Sato and Kimura [62]. The rational orbits of these representations were studied in the work of Wright and Yukie [78], who also explained their connection to field extensions. For our applications we need an interpretation of the $\mathbb{Z}$-orbits of these representations. For the representation $\mathrm{Sym}^3(\mathbb{Z}^2)$ of $\mathrm{GL}_2(\mathbb{Z})$, such an interpretation is due to Levi [51] and Delone and Faddeev [28], who show that the orbits having nonzero discriminant correspond bijectively to reduced cubic rings over $\mathbb{Z}$. This correspondence was refined by Gan *et al.* [38], and shown also to hold for orbits having discriminant 0. Analogous parametrizations of quartic and quintic rings over $\mathbb{Z}$ are developed by Bhargava in his landmark works [5, 6], respectively. His work also naturally recovers the cubic case, and provides a geometric view of it. We now briefly describe the parts of this theory necessary for us.

For $n = 3$, 4, and 5, consider the space of degree-n rings over $\mathbb{Z}$ along with the additional data of a resolvent ring. That is, consider the space of pairs (R_1, R_2), where R_1 is a degree-n ring, and R_2 is a resolvent ring of R_1. The resolvent ring of a cubic ring over $\mathbb{Z}$ is simply the unique quadratic ring having the same discriminant. For the definitions of resolvent rings of quartic and quintic rings over $\mathbb{Z}$, see [5, Section 2.3] and [6, Section 5], respectively. Bhargava proves that this space is parametrized by $G_n(\mathbb{Z})$-orbits on $V_n(\mathbb{Z})$, for $n = 3$, 4, and 5, where G_n is a reductive group and V_n is a prehomogeneous representation of G_n. The condition that a $G_n(\mathbb{Z})$-orbit of $v \in V_n(\mathbb{Z})$ corresponds to a maximal ring is given by congruence conditions on $V_n(\mathbb{Z})$. Bhargava also shows that a maximal ring has a *unique* resolvent ring!

An element in $V(\mathbb{Z})$ is said to be S_n*-irreducible* if it corresponds to an order in an S_n-field. Let $V_n(\mathbb{Z})^{\mathrm{smax}}$ denote the set of S_n-irreducible elements of $V_n(\mathbb{Z})$ that correspond to maximal rings. Therefore, the set of $G_n(\mathbb{Z})$-orbits on $V_n(\mathbb{Z})^{\mathrm{smax}}$ can be considered to be a parametrized family of degree-n fields. The ring of relative invariants for the action of G_n on V_n is freely generated by one invariant, which we call the *discriminant*. The discriminant of $v \in V_n(\mathbb{Z})$ is equal to the discriminant of the ring corresponding to v. Thus, to count the number of degree-n fields having discriminant bounded by x, it suffices to count the number of $G_n(\mathbb{Z})$-orbits on $V_n(\mathbb{Z})^{\mathrm{smax}}$ with discriminant bounded by x. This is carried out by Davenport and Heilbronn [24] in the case $n = 3$, and by Bhargava [7, 8] in the cases $n = 4, 5$, respectively.

The condition that $v \in V_n(\mathbb{Z})$ is S_n-irreducible is not a local condition and is imposed in two steps. First, the cuspidal regions of the fundamental domain $G_n(\mathbb{Z})\backslash V_n(\mathbb{R})$ containing integral points corresponding to non-S_n-irreducible rings are cut off. Next, the main ball is shown to contain predominantly S_n-irreducible points. The latter step follows from an application of Hilbert irreducibility; a power saving may be obtained using the Selberg sieve. The condition that $v \in V_n(\mathbb{Z})$ corresponds to a maximal ring is a local condition. A ring R that is a finitely generated $\mathbb{Z}$-module is maximal if and only if it is maximal at every prime p, that is, $R \otimes \mathbb{Z}_p$ is maximal over $\mathbb{Z}_p$. For $n = 3$, 4, and 5, degree-n ring extensions of $\mathbb{Z}_p$ are classified by $G_n(\mathbb{Z}_p)$-orbits on $V_n(\mathbb{Z}_p)$. We denote the set of elements in $V_n(\mathbb{Z}_p)$ corresponding to maximal $\mathbb{Z}_p$-extensions by $V_n(\mathbb{Z}_p)^{\mathrm{max}}$. For $n = 3$, 4, and 5, it is proven in [24], [5], and [6], respectively, that $V_n(\mathbb{Z}_p)^{\mathrm{max}}$ can be described by congruence conditions modulo p^2 on $V_n(\mathbb{Z}_p)$.

For our purpose of computing the symmetry type of the low-lying zeros of zeta functions arising from degree-n fields, we need to also count the number of degree-n fields with prescribed splitting type at a fixed prime p. This is done as follows: consider the injection $V_n(\mathbb{Z}) \to V_n(\mathbb{Z}_p)$. The splitting of p in the field corresponding to v is determined by the $G_n(\mathbb{Z}_p)$-orbit of v in $V_n(\mathbb{Z}_p)$. Furthermore, the set of all $v \in V_n(\mathbb{Z}_p)^{\mathrm{max}}$ having a fixed splitting type consists of finitely many $G_n(\mathbb{Z}_p)$-orbits. Given a splitting type τ, we denote the set of elements in $V_n(\mathbb{Z}_p)$ corresponding to τ by $V_n(\mathbb{Z}_p)^{\tau}$. For unramified splitting types τ, every element in $V_n(\mathbb{Z}_p)^{\tau}$ is maximal. Next consider the reduction modulo p map $V_n(\mathbb{Z}_p) \to V_n(\mathbb{F}_p)$. In fact, the splitting type τ of $v \in V_n(\mathbb{Z}_p)$ is determined by the image $\bar{v}$ of v in $V_n(\mathbb{F}_p)$. Moreover, the set of all $\bar{v} \in V_n(\mathbb{F}_p)$ corresponding to a fixed splitting type consists of a *single* $G_n(\mathbb{F}_p)$-orbit. We will use the map $V(\mathbb{Z}) \to V(\mathbb{Z}_p)$ as well as the map $V(\mathbb{Z}) \to V(\mathbb{F}_p)$; the first is necessary to detect maximality at p, while the second suffices to determine the splitting type at an unramified prime p.

From this, it is possible to see why we expect Equation (12) to be true. Let τ denote a fixed splitting type, $\mathcal{O}_\tau \subset V_n(\mathbb{F}_p)$ denote the corresponding $G(\mathbb{F}_p)$-orbit, and let $\mathbb{F}_p(\tau)$ denote the corresponding extension of $\mathbb{F}_p$. We expect that

$$\begin{aligned}|\mathfrak{F}^{p,\tau}(x)| &\sim \frac{\mathrm{Vol}(V_n(\mathbb{Z}_p)^\tau)}{\mathrm{Vol}(V_n(\mathbb{Z}_p)^{\max})}\cdot|\mathfrak{F}(x)|\\ &\sim \frac{\mathrm{Vol}(V_n(\mathbb{Z}_p))}{\mathrm{Vol}(V_n(\mathbb{Z}_p)^{\max})}\cdot\frac{|\mathcal{O}_\tau|}{|V(\mathbb{F}_p)|}\cdot|\mathfrak{F}(x)|.\end{aligned} \tag{25}$$

Next we expect the estimate

$$\frac{\mathrm{Vol}(V_n(\mathbb{Z}_p))}{\mathrm{Vol}(V_n(\mathbb{Z}_p)^{\max})} = 1 + O\left(\frac{1}{p^2}\right) \tag{26}$$

to hold since a proportion of roughly $1/p^2$ of elements in $V(\mathbb{Z}_p)$ are nonmaximal. Indeed, if a ring R is nonmaximal at p then p^2 divides the discriminant of R.

Thus, it is only required to check that $|\mathcal{O}_\tau|/|V(\mathbb{F}_p)| = |\tau|/|S_n| + O(1/p)$, for $\tau \in \mathcal{T}_n$, where we are abusing notation by considering τ both as a splitting type and as the corresponding conjugacy class in S_n. Let $\bar{v} \in \mathcal{O}_\tau$ denote any element, and let $\sigma_\tau \in S_n$ denote any element in the conjugacy class τ. Our representations (G, V) satisfy the property $\mathrm{Stab}_{G(\mathbb{F}_p)}(\bar{v}) \cong \mathrm{Aut}(\mathbb{F}_p(\tau)) \cong \mathrm{Stab}_{S_n}(\sigma_\tau)$ (see, for example, [12, Theorem 6]). By two applications of the orbit-stabilizer formula, we obtain

$$\frac{|\mathcal{O}_\tau|}{|V(\mathbb{F}_p)|} = \frac{|G(\mathbb{F}_p)|}{|\mathrm{Stab}_{G(\mathbb{F}_p)}(\bar{v})||V(\mathbb{F}_p)|} = \frac{1}{|\mathrm{Stab}_{S_n}(\sigma_\tau)|} + O\left(\frac{1}{p}\right) = \frac{|\tau|}{|S_n|} + O\left(\frac{1}{p}\right), \tag{27}$$

as required. To see why we expect $c_{p|\Delta} = O(1/p)$, note that p ramifies in the field corresponding to $v \in V(\mathbb{Z})$ if and only if the discriminant of $\bar{v} \in V(\mathbb{F}_p)$ is zero. Furthermore, the number of elements in $V(\mathbb{F}_p)$ having discriminant 0 is bounded by $O(|V(\mathbb{F}_p)|/p)$.

For $n = 3$, 4, and 5, the estimates (25), (26), (27) are known to be true. Indeed, in the rest of this section, we give detailed references and explain how to obtain Sato–Tate equidistribution and (12) for the families of cubic, quartic, and quintic fields, and describe the error terms that we obtain. The purpose of the above discussion is to give a heuristic explanation for why we expect (12) to hold in greater generality.

3.1. The family of cubic fields. Let V denote the space of binary cubic forms. The group $G = \mathrm{GL}_2$ acts on V via the twisted action

$$g \cdot f(x, y) := \frac{1}{\det g} f((x, y) \cdot g).$$

A result of Delone and Faddeev [28], refined by Gan *et al.* [38], states that isomorphism classes of cubic orders are parametrized by $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$. The congruence conditions defining maximality is a result of Davenport and Heilbronn [24].

THEOREM 3.1.

(1) *There is a natural bijection between the set of $G(\mathbb{Z})$-equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings. A cubic ring corresponding to the $G(\mathbb{Z})$-orbit of f is an order if and only if $f(x, y)$ is irreducible over $\mathbb{Q}$.*

(2) *A cubic order corresponding to $f \in V(\mathbb{Z})$ fails to be maximal at p if either f is a multiple of p or if some $G(\mathbb{Z})$-translate $ax^3 + bx^2y + cxy^2 + dy^3$ of $f(x, y)$ satisfies $p^2 \mid a$ and $p \mid b$.*

The discriminant Δ of a binary cubic form is G-invariant. Furthermore, the discriminant of f equals the discriminant of the cubic ring corresponding to f.

EXAMPLE 3.2. If $f = x^3 + 7y^3$ then the cubic ring is $R = \mathbb{Z}[x]/(x^3 + 7)$. The form f is irreducible over $\mathbb{Q}$ and R is the maximal order in the field $\mathbb{Q}(\sqrt[3]{7})$. (To check maximality, it is only necessary to verify the conditions in [4, Lemma 2.10].) Let $p = 3$. Then the form $\bar{f}(x, y)$ is irreducible. Therefore, the splitting type of p in $\mathbb{Q}(\sqrt[3]{7})$ is (3).

To count cubic fields, we directly use [68, Theorem 1.3].

THEOREM 3.3. *Let $\mathfrak{F}$ be the parametrized family of cubic S_3-fields ordered by discriminant. For any prime p, conjugacy class $\tau \in \mathcal{T}_3$ and $\epsilon > 0$, we have*

$$\begin{aligned} |\mathfrak{F}(x)| &= \frac{1}{3\zeta(3)}x + O(x^{5/6}), \\ |\mathfrak{F}^{p,\tau}(x)| &= \frac{c_{p,\tau}}{3\zeta(3)}x + O(x^{5/6}) + O_\epsilon(x^{7/9+\epsilon}p^{8/9}), \\ |\mathfrak{F}^{p|\Delta}(x)| &= \frac{c_{p|\Delta}}{3\zeta(3)}x + O(x^{5/6}) + O_\epsilon(x^{7/9+\epsilon}p^{16/9}), \end{aligned} \tag{28}$$

where $c_{p,\tau} = (|\tau|/6)(p^2/(p^2 + p + 1))$ and $c_{p|\Delta} = (p + 1)/(p^2 + p + 1)$.

This concludes the proof of the Sato–Tate equidistribution for the family $\mathfrak{F}$ of cubic fields, namely the equation (10) with $\delta_0 = 5/6$ and $\delta_1 = 7/9 + \epsilon$, together with (12). Note that in the two estimates in (10) the exponents $A = 8/9$ and

$B = 16/9$ differ. Also the exponent $\delta_0 = 5/6$ is sharp by [10, 68], which independently establish a secondary main term for the counting function of cubic fields. We obtain the bound on the support to be $\alpha < 4/41$ in Theorem 2.8.

3.2. The family of quartic fields. Let $V = 2 \otimes \mathrm{Sym}^2(3)$ denote the space of pairs of ternary quadratic forms. We represent elements in V by a pair of symmetric 3×3-matrices A and B. The group $G = \mathrm{GL}_2 \times \mathrm{SL}_3$ acts on V via the action

$$(g_2, g_3) \cdot (A, B) := (g_3^t A g_3, g_3^t B g_3) \cdot g_2^t.$$

A result of Bhargava [5] states that isomorphism classes of pairs (Q, C), where Q is a quartic ring and C is a cubic resolvent ring of Q, are parametrized by $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$. The definition of the cubic resolvent is not important for this section.

THEOREM 3.4. *There is a natural bijection between the set of $G(\mathbb{Z})$-equivalence classes on $V(\mathbb{Z})$ and the set of isomorphism classes of pairs (Q, C), where Q is a quartic ring and C is a cubic resolvent ring of Q.*

The congruence conditions defining maximality may be found in [7]. The action of G on V has a unique polynomial invariant Δ called the *discriminant*. If $(A, B) \in V(\mathbb{Z})$ corresponds to the pair (Q, C), then we have $\Delta(A, B) = \Delta(Q) = \Delta(C)$.

To count S_4-quartic fields having prescribed splitting conditions, we directly use a result of Ellenberg *et al.* [31, Theorem 4.1], which improves on the results of [4], which in turn builds on the work of Bhargava [7] determining asymptotics for the counting function of S_4-quartic fields.

THEOREM 3.5. *Let $\mathfrak{F}$ be the parametrized family of quartic S_4-fields ordered by discriminant. Let $\epsilon > 0$. Then, for any prime p and conjugacy class $\tau \in \mathcal{T}_4$, we have*

$$|\mathfrak{F}(x)| = \frac{5\beta}{24} x + O_\epsilon(x^{23/24+\epsilon}),$$

$$|\mathfrak{F}^{p,\tau}(x)| = \frac{5c_{p,\tau}\beta}{24} x + O_\epsilon(x^{23/24+\epsilon} p^{1/2+\epsilon}), \tag{29}$$

$$|\mathfrak{F}^{p|\Delta}(x)| = \frac{5c_{p|\Delta}\beta}{24} x + O_\epsilon(x^{23/24+\epsilon} p^{1/2+\epsilon}),$$

where $\beta = \prod_p (1 + p^{-2} - p^{-3} - p^{-4})$, $c_{p,\tau} = (|\tau|/24)(p^3/(p^3 + p^2 + 2p + 1))$ for every $\tau \in \mathcal{T}_4$, and $c_{p|\Delta} = (p + 1)^2/(p^3 + p^2 + 2p + 1)$.

This verifies Equations (10) and (12) for the parametrized family of S_4-fields with $\delta_0 = \delta_1 = 23/24 + \epsilon$ and $A = B = 1/2 + \epsilon$, and yields the bound $\alpha < 1/24$ of the support in Theorem 2.8.

3.3. The family of quintic fields. Let $V = 4 \otimes \wedge^2 (5)$ denote the space of quadruples of 5×5-skew symmetric matrices. We represent elements in V as (A, B, C, D). The group $G = \mathrm{GL}_4 \times \mathrm{SL}_5$ acts on V via the action

$$(g_1, g_2) \cdot (A, B, C, D) := (g_2^t A g_2, g_2^t B g_2, g_2^t C g_2, g_2^t D g_2) \cdot g_1^t.$$

A result of Bhargava [6] states that isomorphism classes of pairs (Q, R), where Q is a quintic ring and R is a sextic resolvent ring of Q, are parametrized by $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$. Given an element $(A, B, C, D) \in 4 \otimes \wedge^2 (5)$, the corresponding five points in $\mathbb{P}^3$ are obtained as the intersection of the five 4×4-Pfaffians of $Ax + By + Cz + Dt$.

Again, the definition of a sextic resolvent ring is not important for us. See [6] for a precise description.

THEOREM 3.6. *There is a natural bijection between the set of $G(\mathbb{Z})$-equivalence classes on $V(\mathbb{Z})$ and the set of isomorphism classes of pairs (Q, R), where Q is a quintic ring and R is a sextic resolvent ring of Q.*

The congruence conditions defining maximality may be found in [8]. The action of G on V has a unique polynomial invariant Δ called the *discriminant*. If $(A, B, C, D) \in V(\mathbb{Z})$ corresponds to the pair (Q, R), then we have $\Delta(A, B, C, D) = \Delta(Q) = \Delta(R)$.

To count S_5-quintic fields having prescribed splitting, we directly use [31, Theorem 5.1].

THEOREM 3.7. *Let $\mathfrak{F}$ be the parametrized family of quintic S_5-fields ordered by discriminant. Let $\epsilon > 0$. Then, for any prime p and conjugacy class $\tau \in \mathcal{T}_5$, we have*

$$|\mathfrak{F}(x)| = \frac{13\beta}{120} x + O(x^{199/200+\epsilon}),$$

$$|\mathfrak{F}^{p,\tau}(x)| = \frac{13 c_{p,\tau}\beta}{120} x + O(x^{199/200+\epsilon}) + O(x^{79/80+\epsilon} p^{1/2+\epsilon}), \tag{30}$$

$$|\mathfrak{F}^{p|\Delta}(x)| = \frac{13 c_{p|\Delta}\beta}{120} x + O(x^{199/200+\epsilon}) + O(x^{79/80+\epsilon} p^{1/2+\epsilon}),$$

where $\beta = \prod_p (1 + p^{-2} - p^{-4} - p^{-5})$, $c_{p,\tau} = (|\tau|/120)(p^4/(p^4 + p^3 + 2p^2 + 2p + 1))$, *and* $c_{p|\Delta} = ((p+1)(p^2+p+1))/(p^4+p^3+2p^2+2p+1)$.

The additional error of $O(X^{199/200+\epsilon})$ (in comparison with the quartic case) arises from the bound on the number of quintic orders that are not S_5-orders obtained in [64]. Both [31, Theorem 5.1] and [64] use the methods in [8] used to determine asymptotics for the counting function of quintic fields.

This verifies Equations (10) and (12) for the parametrized family of S_5-fields, this time with $\delta_0 = 199/200 + \epsilon$, $\delta_1 = 79/80 + \epsilon$ and $A = B = 1/2 + \epsilon$. This yields the bound $\alpha < 1/100$ of the support in Theorem 2.8.

4. Other parametric families of quadratic and cubic fields

In this section, we consider families of quadratic and cubic fields obtained by different parametrizations. The quadratic fields will be constructed as quadratic resolvents of S_3-fields. The cubic fields will be constructed as resolvents of S_4-fields. Thus this section provides examples of constructing one family from another. We shall verify the Sato–Tate equidistribution for these families and show that the assumptions of Theorem 2.8 are satisfied which enables us to determine that the symmetry type of the low-lying zeros is Symplectic.

4.1. A parametric family of quadratic fields. Every quadratic field can be written uniquely in the form $K = \mathbb{Q}(\sqrt{d})$, where d is a fundamental discriminant. The discriminant of such a field K is equal to d. Let ζ_K denote the zeta function of K. It factors as $\zeta_K(s) = \zeta(s)L(s,\chi)$, where $\zeta(s)$ is the Riemann zeta function and $L(s,\chi)$ is the Dirichlet L-function corresponding to the quadratic character χ defined by the Kronecker symbol $\chi(n) = (d/n)$. The conductor of this L-function is equal to $|d|$.

We consider the family $\mathfrak{F}$ of quadratic fields arising as the quadratic resolvents of nowhere totally ramified cubic fields. A cubic field K_3 is said to be *nowhere totally ramified* if no prime p factors as $\mathfrak{p}^3$ in K_3. Suppose that K_3 is a nowhere totally ramified cubic S_3-extension of $\mathbb{Q}$ having discriminant D. Let K_6 denote the Galois closure of K_3, and K denote the unique quadratic subfield of K_6. The field K is called the *quadratic resolvent field* of K_3. It follows that K_6 is an unramified cubic extension of K and that the discriminant of K is D. Thus the family $\mathfrak{F}$ is parametrized as

$$\mathfrak{F} = \{\mathbb{Q}(\sqrt{\Delta(f)}) : f \in \mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{Sym}^3(\mathbb{Z}^2)^{\mathrm{ntr}}\},$$

where f ranges over $\mathrm{GL}_2(\mathbb{Z})$-orbits of maximal integral binary cubic forms that are nowhere totally ramified. We order elements in $\mathfrak{F}$ by discriminant. For each

$x \geqslant 1$, the set $\mathfrak{F}(x)$ consists of the quadratic fields in $\mathfrak{F}$ having discriminant less than x in absolute value. Note that the quadratic fields in $\mathfrak{F}$ occur with multiplicities. In fact, [24] implies that quadratic fields K appear in $\mathfrak{F}$ with a multiplicity of $(\#\mathrm{Cl}(K)[3]-1)/2$, where $\mathrm{Cl}(K)$ denotes the class group of K. Therefore, it is also possible to think of $\mathfrak{F}$ as a weighted family of quadratic fields, where each field K is weighted with $(\#\mathrm{Cl}(K)[3]-1)/2$. However, we prefer to consider $\mathfrak{F}$ as a geometric family arising from the space of integral binary cubic forms.

Recall the branched covering $X \to V$ of degree three (described in the introduction), where $V \simeq \mathbb{A}^4$ is the space of binary cubic forms and $X \subset V \times \mathbb{P}^1$ is the zero locus. We construct $Y \subset V \times \mathbb{P}^1$ defined by the zero locus of the polynomial $x^2 - \Delta(f)y^2$. This is a branched covering $Y \to V$ of degree two. Clearly it is GL_2-equivariant. Restricting to $V^{\Delta\neq 0}$ we obtain an étale covering. The étale covering $Y \to V^{\Delta\neq 0}$ is obtained from the étale covering $X \to V^{\Delta\neq 0}$ by the resolvent construction applied to this relative situation (that is, applied to each fiber). Our parametric family $\mathfrak{F}$ is attached to the covering $Y \to V$ as in Section 2. Alternatively, we could have constructed the family $\mathfrak{F}$ starting from $X \to V$, but using the one-dimensional Artin representation $\mathrm{Gal}(K_6/\mathbb{Q}) \to S_3 \to \mathrm{GL}_1(\mathbb{C})$ (the sign character).

4.2. Symmetry type corresponding to this family of quadratic fields.

For our purposes it will be necessary to relate the splitting type of p in a nowhere totally ramified cubic field K_3 to the splitting type of p in the quadratic resolvent of K_3. The splitting type of a prime p in K_3 determines the splitting type of p in K_6, the Galois closure of K_3, and hence determines the splitting type of p in K_2, the quadratic resolvent of K_3. These splitting types can be immediately computed by applying the method of [77], yielding the following lemma.

LEMMA 4.1. *Let K_3 be a cubic field that is nowhere totally ramified, and let K_2 denote its quadratic resolvent field. If p has splitting type* (111) *or* (3) *in K_3 then p has splitting type* (11) *in K_2 and if p has splitting type* (21) *in K_3 then p has splitting type* (2) *in K_2.*

The asymptotics of $|\mathfrak{F}(x)|$ is the result of Davenport and Heilbronn [24, Theorem 3] on the average 3-part of the class group of quadratic fields (this result is restated in [10, Theorem 2], and a simpler proof is provided). The counting result [68, Theorem 1.4], in conjunction with Lemma 4.1, implies the analogues of Equations (10) and (12) for $\mathfrak{F}$, with $\delta_0 = 5/6$, $\delta_1 = 18/23 + \epsilon$, $A = 20/23$, and $B = 40/23$. Thus $\mathfrak{F}$ is an S_2-family in the sense that for a fixed prime p, the splitting types (11) and (2) occur equally often in $\mathfrak{F}$.

As in Section 2, we define the average conductor $\mathcal{L}$ which in fact coincides with the average conductor of the family of cubic fields. Theorem 2.8 then follows for an even function f whose Fourier transform is smooth and supported in the interval $[-\alpha, \alpha]$, with $\alpha < \frac{10}{103}$.

Since $(\#\mathrm{Cl}(K)[3] - 1)/2$ is equal to the number of index-3 subgroups of $\mathrm{Cl}(K)$, $\mathfrak{F}(x)$ can be viewed as a weighted set of L-functions $L(s, \chi_d)$ arising from all quadratic fields $K = \mathbb{Q}(\sqrt{d})$, where each field is counted with multiplicity $(\#\mathrm{Cl}(d)[3] - 1)/2$. Since the Sato–Tate measure of the unweighted family of quadratic fields also arises from the splitting types (11) and (2) occurring equally often, we deduce the same Sato–Tate equidistribution when the fields are counted with multiplicity $\#\mathrm{Cl}(d)[3]$. The same holds for the symplectic symmetry type of low-lying zeros, so we can for example deduce, when summing over positive fundamental discriminants d, that

$$\lim_{x\to\infty} \frac{\pi^2}{4x} \sum_{0<d<x} \#\mathrm{Cl}(d)[3] \sum_j f\left(\frac{\gamma_d^{(j)}\mathcal{L}}{2\pi}\right) = \widehat{f}(0) - f(0)/2. \tag{31}$$

Note that $\#\mathrm{Cl}(d)[3]$ is $\frac{4}{3}$ on average over asymptotically $3x/\pi^2$ positive fundamental discriminants $0 < d < x$.

4.3. A parametric family of cubic fields. We now consider a family of cubic fields arising as cubic resolvents of certain quartic fields. First we collect some results on cubic resolvent fields of quartic fields (see [7, Section 3.1] for more details). Given a quartic S_4-field K_4, let K_{24} denote its Galois closure. The field K_6, corresponding to the subgroup $V_4 \subset S_4$ generated by the double transpositions in S_4, is Galois and its Galois group is $S_4/V_4 \cong S_3$. Let K_3 denote a cubic S_3-field contained in K_6 (K_3 is unique up to conjugation). Then K_3 is called the *cubic resolvent field* of K_4.

A quartic field K_4 is said to be *nowhere overramified* if no rational prime p has splitting type $(1^2 1^2)$, (2^2), or (1^4) in K_4. If K_4 is a nowhere overramified quartic field and its cubic resolvent field is K_3, then the discriminant of K_4 is equal to the discriminant of K_3. To give a description of the family of cubic resolvents of nowhere overramified quartic fields as a geometric family, we have the following theorem that is a result of Bhargava [5].

THEOREM 4.2. *Let (Q, C) be a pair of rings, where Q is the maximal order of a nowhere overramified quartic field K_4 and C is the (unique) cubic resolvent ring of Q. Let (A, B) be a pair of integral ternary quadratic forms such that the* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$*-orbit of (A, B) corresponds to (Q, C) under the bijection of* [5, Theorem 1]. *Then, under the Delone–Faddeev parametrization* [28], *the* *cubic ring C corresponds to the binary cubic form* $\mathrm{Res}(A, B) := 4\det(Ax - By)$. *Furthermore, C is the maximal order of the cubic resolvent field of K_4.*

We now define our family $\mathfrak{F}$ of cubic fields as follows:

$$\mathfrak{F} := \{K(\mathrm{Res}(A, B)) : (A, B) \in (\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}))\backslash(\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^3))^{\mathrm{nor}}\},$$

where $K(\mathrm{Res}(A, B))$ denotes the cubic field that is the field of fractions of the cubic ring corresponding to $f(x, y)$, the cubic resolvent form of (A, B), and (A, B) runs over $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-orbits of maximal integral pairs of ternary quadratic forms that are nowhere overramified. Note that Theorem 4.2 implies that the discriminant of $K(f)$ is equal to the discriminant of (A, B). We order elements in $\mathfrak{F}$ by discriminant and denote the set of elements in $\mathfrak{F}$ with discriminant less than x by $\mathfrak{F}(x)$.

Let V denote the space of pairs of ternary quadratic forms. Given a generic element $(A, B) \in V$, we obtain four points in $\mathbb{P}^2$, namely, the four points of intersection of the quadrics corresponding to A and B. We also obtain three points in $\mathbb{P}^1$, namely, the three roots of the cubic resolvent form $4\det(Ax-By)$ of (A, B). We thus obtain the natural space $Z \subset V \times \mathbb{P}^2 \times \mathbb{P}^1$, and a degree-12 branched covering $Z \to V$. Taking the intersection of Z with $V \times \mathbb{P}^2$, we obtain a branched covering $X \to V$ of degree four, and taking the intersection of Z with $V \times \mathbb{P}^1$, we obtain a branched covering $Y \to V$ of degree three. All three branched coverings are $\mathrm{GL}_2 \times \mathrm{SL}_3$-equivariant.

Consider the family of L-functions associated to $\mathfrak{F}$, where for each cubic S_3-field $K_3 \in \mathfrak{F}$, we take the Artin L-function $L(s, \rho_{K_3})$ corresponding to the standard representation of S_3. This family arises naturally from the branched covering $Y \to V$. However, we note that we may also form this family of L-functions from the branched covering $X \to V$. Indeed, for an S_4-quartic field K_4 with Galois closure K_{24}, we associate to it the two-dimensional Artin representation $\mathrm{Gal}(K_{24}/\mathbb{Q}) \cong S_4 \to S_3 \to \mathrm{GL}_2(\mathbb{C})$, where $S_4 \to S_3$ is the map in which we quotient out by the subgroup generated by double transpositions. The corresponding family of L-functions is the same as the family associated to the branched cover $Y \to V$. This is because the field in K_{24} fixed by the double transpositions of S_4 is the degree-6 Galois closure K_6 of the cubic resolvent K_3 of K_4. Hence the Artin L-function corresponding to the representation $\mathrm{Gal}(K_{24}/\mathbb{Q}) \cong S_4 \to S_3 \to \mathrm{GL}_2(\mathbb{C})$ is the same as the Artin L-function corresponding to the standard representation $\mathrm{Gal}(K_6/\mathbb{Q}) \cong S_3 \to \mathrm{GL}_2(\mathbb{C})$.

As in the case of the family of quadratic resolvents of cubic fields, cubic fields $K \in \mathfrak{F}$ arise with multiplicities. The following theorem, due to Heilbronn [39], shows that the multiplicity of K is $\#\mathrm{Cl}(K)[2] - 1$:

Table 1. Densities of splitting types.

Splitting type of p in Q	Splitting type of p in C	Density in $\mathfrak{F}$
(1111)	(111)	$\frac{1}{24} + O\left(\frac{1}{p}\right)$
(22)	(111)	$\frac{1}{8} + O\left(\frac{1}{p}\right)$
(211)	(21)	$\frac{1}{4} + O\left(\frac{1}{p}\right)$
(4)	(21)	$\frac{1}{4} + O\left(\frac{1}{p}\right)$
(31)	(3)	$\frac{1}{3} + O\left(\frac{1}{p}\right)$

THEOREM 4.3. *Let K be a fixed cubic S_3-field. Then index-2 subgroups of* $\mathrm{Cl}(K)$ *are in bijective correspondence with quartic fields that are nowhere overramified and have K as a cubic resolvent field.*

Therefore, it is possible to interpret $\mathfrak{F}$ as a family of weighted cubic fields, where each cubic field K is weighted by $\#\mathrm{Cl}(K)[2] - 1$. However, as before, we prefer to consider $\mathfrak{F}$ as a geometric family.

4.4. Symmetry type corresponding to this family of cubic fields. We will need to relate the splitting type of an unramified prime p in a nowhere overramified quartic field Q to the splitting type of p in the cubic resolvent field C of Q. This is done in the following proposition:

PROPOSITION 4.4. *Let Q be a quartic order, and let C be a cubic resolvent of Q. Fix a prime p that does not ramify in Q. The splitting type of p in Q determines the splitting type of p in C. Table 1 lists the different possible pairs of splitting types.*

Proof. Let K_4 and K_3 denote $Q \otimes_{\mathbb{Z}} \mathbb{Q}$ and $C \otimes_{\mathbb{Z}} \mathbb{Q}$, respectively. Since K_4 is a quartic field and Q is an order in K_4, we deduce that K_3 is also a field and C is an order in K_3. Since p is unramified in K_4, it remains unramified in the Galois closure of K_4, and hence in K_3. The splitting types of p in K_4 and K_3 are the same as the splitting types of p in Q and C, respectively. The theorem now follows by applying the method of [77]. □

The counting results of Theorem 3.5 imply the analogue of (10) with $\delta_0 = \delta_1 = 23/24 + \epsilon$ and $A = B = 1/2 + \epsilon$. The analogue of (12) follows from Table 1 because $1/24 + 1/8 = 1/6$, $1/4 + 1/4 = 1/2$, and $1/3 = 1/3$. Thus $\mathfrak{F}$ is an S_3-family in the sense that the Frobenius elements are uniformly distributed in $\mathcal{T}_3$.

As in Section 2, if we define $\mathcal{L}$ to be the average conductor, then Theorem 2.8 follows for an even function f whose Fourier transform is smooth and supported in the interval $[-\alpha, \alpha]$, with $\alpha < \frac{1}{24}$. Since $\#\mathrm{Cl}(K)[2] - 1$ is equal to the number of index-2 subgroups of $\mathrm{Cl}(K)$, $\mathfrak{F}(x)$ can be viewed as a weighted set of Artin L-functions arising from S_3-fields K, where each S_3-field is counted with multiplicity $\#\mathrm{Cl}(K)[2] - 1$. Therefore, in conjunction with Section 3, we deduce equidistribution results for cubic fields counted with multiplicity $\#\mathrm{Cl}(K)[2]$.

The main ingredient that we use in order to consider these weighted families (of quadratic fields K weighted by $\#\mathrm{Cl}(K)[3]$ and of cubic fields L weighted by $\#\mathrm{Cl}(L)[2]$) is that these weighted families can be parametrized in terms of integral orbits of reductive groups on certain representations. Let us also note that it is possible to obtain analogous results for the families of quadratic and cubic fields weighted by $\#\mathrm{Cl}(K) \cdot \mathrm{Reg}(K)$. One way to obtain such a result is to use geometric families that parametrize quadratic and cubic fields, with these weights. For quadratic fields, we use the space of binary quadratic forms modulo the SL_2-action, and for cubic fields, we use the space $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ modulo the $\mathrm{GL}_2 \times \mathrm{SL}_3 \times \mathrm{SL}_3$-action (see [6]). Though integral orbits on these representations parametrize simply the class groups of quadratic (respectively cubic) fields, the fundamental domains that can be most naturally constructed for these spaces weigh each quadratic (respectively cubic) field K by $\#\mathrm{Cl}(K) \cdot \mathrm{Reg}(K)$. The latter construction can be seen in [66] for the case of quadratic fields and [72, Ch. 2] for cubic fields. Alternatively, we can use the fact that the Dirichlet class number formula expresses this quantity as a residue at $s = 1$ of $\zeta_K(s)$ which can be well approximated by a short Dirichlet polynomial. On the other hand arithmetic weights such as $L(\frac{1}{2}, \chi_d)$ could change the answer.

5. S_n-families

In this section, we consider the parametric family of monogenized degree-n number fields and prove Theorem 1.1 concerning the Sato–Tate equidistribution. We will let $V \simeq \mathbb{A}^n$ denote the space of monic polynomials of degree n. The ring of functions of V is $\mathbb{Z}[a_1, \dots, a_n]$, which we can identify via the fundamental theorem of algebra with $\mathbb{Z}[x_1, \dots, x_n]^{S_n}$. Thus we can identify V with the GIT quotient $\mathbb{A}^n//S_n$, which simply amounts to factor the monic polynomial

$$f(T) = T^n + a_1 T^{n-1} + \cdots + a_n = (T - x_1)(T - x_2) \cdots (T - x_n).$$

Equivalently V is the Hilbert scheme of n points in $\mathbb{A}^1$. The ring of functions of the cartesian product $V \times \mathbb{A}^1$ is $\mathbb{Z}[x_1, \ldots, x_n]^{S_n}[T]$. The subscheme $X \subset V \times \mathbb{A}^1$ corresponding to the zero set of f is defined by the principal ideal generated by $(T - x_1)(T - x_2) \cdots (T - x_n)$.

LEMMA 5.1. *There is a ring isomorphism between the quotient ring*

$$\mathbb{Z}[x_1, \ldots, x_n]^{S_n}[T]/\langle (T - x_1)(T - x_2) \cdots (T - x_n) \rangle,$$

and $\mathbb{Z}[x_1, \ldots, x_n]^{S_{n-1}}$, induced by specializing $T \mapsto x_n$.

Proof. The map is clearly a ring homomorphism. Since the image contains the polynomial x_n, to prove surjectivity it suffices to show that the image contains the subring $\mathbb{Z}[x_1, \ldots, x_{n-1}]^{S_{n-1}}$. Let $g(x_1, \ldots, x_{n-1})$ be an S_{n-1}-invariant polynomial. Then $g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0)$ for some S_n-invariant polynomial f. This can be proved by using the elementary symmetric polynomials; see, for example, [52, Section 1.1]. Then g is the image of $f(x_1, \ldots, x_n - T) \in \mathbb{Z}[x_1, \ldots, x_n]^{S_n}[T]$. To prove that the map is injective, it is sufficient to prove that if a polynomial in $\mathbb{Z}[x_1, \ldots, x_n][T]$ is such that each of the specializations $T \mapsto x_1$, $T \mapsto x_2, \ldots, T \mapsto x_n$ vanishes, then it is divisible by $(T - x_1)(T - x_2) \cdots (T - x_n)$. Since the ring $\mathbb{Z}[x_1, \ldots, x_n]$ is an integral domain, this follows from the factor theorem, which we recall in Lemma 5.2 for convenience. □

LEMMA 5.2 (Factor theorem for polynomial rings).

(i) *Let R be a commutative ring. If a polynomial $f \in R[T]$ has a root $f(\alpha) = 0$, then it is divisible by $T - \alpha$.*

(ii) *Let R be an integral domain. If a polynomial $f \in R[T]$ has distinct roots $\alpha_1, \ldots, \alpha_n \in R$, then it is divisible by $(T - \alpha_1)(T - \alpha_2) \cdots (T - \alpha_n)$.*

Proof. (i) Since $T - \alpha$ is monic, it follows from the polynomial division algorithm that $f(T) = (T - \alpha)g(T) + a$ for some $g \in R[T]$ and $a \in R$. Since R is commutative, we can specialize $T \mapsto \alpha$, which yields $a = 0$.

(ii) We proceed by induction on n. By (i), we can factor $f(T) = (T - \alpha_n)g(T)$ for some $g \in R[T]$. For each $i \neq n$, the difference $\alpha_i - \alpha_n$ is nonzero, hence $g(\alpha_i) = 0$ because R is a domain. We may then factor g thanks to the induction hypothesis. □

From Lemma 5.1, we deduce that the ring of functions of X can be identified with $\mathbb{Z}[x_1, \ldots, x_n]^{S_{n-1}}$. Equivalently X is the Hilbert scheme of n points in $\mathbb{A}^1$, one of which is marked. Similarly the Galois closure $\widetilde{X}$ of $X \to V$ is identified with $\mathbb{A}^n$, which parametrizes n marked points in $\mathbb{A}^1$, and with ring of functions $\mathbb{Z}[x_1, \ldots, x_n]$.

In this section, the family $\mathfrak{F}$ consists of the degree-n fields corresponding to $\mathbb{Z}$-orbits on $V(\mathbb{Z})^{\max}$, the set of elements f in $V(\mathbb{Z})$ such that $\mathbb{Z}[x]/f(x)$ is a maximal order in a degree-n field.

5.1. Monogenized fields arising from monic integer polynomials. Recall from the introduction the notion of monogenized rings and fields. A polynomial $f(T) \in V(\mathbb{Z})$ gives rise to the monogenized ring $(\mathbb{Z}[T]/f(T), T)$. Conversely, a monogenized ring (R, α), where R has rank n over $\mathbb{Z}$, gives rise to a polynomial $f \in V(\mathbb{Z})$, namely, the characteristic polynomial of α. The group $\mathbb{Z}$ acts on $V(\mathbb{Z})$ via the action $(m \cdot f)(T) = f(T + m)$. Since the characteristic polynomial of $\alpha + m$ is $f(T - m)$, where f is the characteristic polynomial of α, it follows that the isomorphism classes of monogenized rank-n rings are in bijection with the $\mathbb{Z}$-orbits on $V(\mathbb{Z})$.

In this section, we shall consider the family $\mathfrak{F}$ of degree-n fields K_f that arise as the fraction fields of *maximal* orders R_f corresponding to $\mathbb{Z}$-orbits of integer monic degree-n polynomials. These fields are said to be *monogenic*. This family is distinct from the family of fields arising from *all* orders corresponding to integer monic degree-n polynomials (see [48]). The latter family would capture all S_n-fields since every number field is generated by a single element over $\mathbb{Q}$ and thus every number field is the field of fractions of some (possibly nonmaximal) order corresponding to an integer monic degree-n polynomial. Moreover, every degree-n field arises in the latter family infinitely often.

It is expected that for $n \geqslant 3$, most maximal orders (in fact, most rings) are not monogenic. Thus, we expect that our family of monogenic fields is thin in the full set of degree-n fields, though this is not known to be the case for any $n \geqslant 3$. For example, a cubic ring corresponding to the binary cubic form f under the Delone–Faddeev correspondence [28] is monogenic if and only if f represents 1 over $\mathbb{Z}$. So in the case $n = 3$, the thinness of the family of monogenic cubic rings reduces to the open question of showing that 100% of integral binary cubic forms do not represent 1.

In the next subsection, we consider the family $\mathfrak{F}$ of monogenized fields and define an appropriate height function on it. We then determine asymptotics for the number of monogenized fields having prescribed splitting conditions at a fixed prime p, and use these asymptotics to determine the symmetry type of the low-lying zeros of the corresponding family of L-functions.

5.2. Counting results. Every $\mathbb{Z}$-orbit on $V(\mathbb{Z})$ has a unique representative whose T^{n-1}-coefficient is between 0 and $n-1$. Let $V(\mathbb{Z})_k$ denote the set of monic integer polynomials whose T^{n-1}-coefficient is k. Then the set $\bigsqcup_{k=0}^{n-1} V(\mathbb{Z})_k$ is a set of orbit representatives for the action of $\mathbb{Z}$ on $V(\mathbb{Z})$.

Let $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ be an element of $V(\mathbb{Z})$. The coefficients a_i are the ith symmetric polynomials evaluated on the roots of f. Hence we consider a_i to be a degree-i function on V. The discriminant Δ is a degree $n(n-1)$ function on V. We then define the following height on $V(\mathbb{R})$:

$$h(T^n + a_1 T^{n-1} + a_2 T^{n-2} + \cdots + a_n) = \max_i\{|a_i|^{n(n-1)/i}\}.$$

For $x > 0$, we consider the set of elements in $V(\mathbb{R})_k$ (respectively $V(\mathbb{Z})_k$) having height less than x. Then

$$\begin{aligned}
&|\{f \in V(\mathbb{Z})_k : h(f) < x\}| \\
&\quad = \mathrm{Vol}(\{f \in V(\mathbb{R})_k : h(f) < x\}) + O(x^{((n+2)/2n)-(2/n(n-1))}) \\
&\quad = 2^{n-1} x^{(n+2)/2n} + O(x^{((n+2)/2n)-(2/n(n-1))}).
\end{aligned}$$

See also [29] for the related count of rational points on weighted projective spaces.

An application of Hilbert irreducibility proves that 100% of elements f in $V(\mathbb{Z})$ yield $\mathbb{Q}$-algebras $K_f = \mathbb{Q}[T]/f(T)$ which are S_n-number fields. Indeed, an application of the Selberg sieve yields the upper bound

$$|\{f \in V(\mathbb{Z})_k : K_f \text{ not } S_n\text{-field}, h(f) < x\}| = O_\epsilon(x^{((n+2)/2n)-(2/5n(n+1))+\epsilon}). \tag{32}$$

This bound is essentially due to Gallagher. See the recent article [30] for more general results via a different approach based on resolvent rings and the method of Bombieri–Pila for counting integer points on high degree curves.

Next, we consider the subsets $V(\mathbb{F}_p)^{(\tau)} \subset V(\mathbb{F}_p)$ of polynomials having splitting type $\tau \in \mathcal{T}_n$ and the subset $V(\mathbb{F}_p)^{\Delta=0} \subset V(\mathbb{F}_p)$ of polynomials that have discriminant 0. As in Section 3, we denote the set of elements in $V(\mathbb{Z}_p)$ corresponding to maximal degree-n extensions of $\mathbb{Z}_p$ by $V(\mathbb{Z}_p)^{\max}$. We also let $V(\mathbb{Z}_p)^{p|\Delta}$ denote the set of elements in $V(\mathbb{Z}_p)$ whose discriminants are divisible by p, and let $V(\mathbb{Z}_p)^{p|\Delta,\max}$ denote $V(\mathbb{Z}_p)^{\max} \cap V(\mathbb{Z}_p)^{p|\Delta}$.

LEMMA 5.3. *Let p be a prime such that $(p, n) = 1$. Then we have*

$$\begin{aligned}
c_{p,\tau} &:= \frac{|V(\mathbb{F}_p)^{(\tau)}|}{p^n} \cdot \frac{1}{\mathrm{Vol}(V(\mathbb{Z}_p)^{\max})} = \frac{|\tau|}{|S_n|} + O\left(\frac{1}{p}\right), \\
c_{p|\Delta} &:= \frac{|V(\mathbb{F}_p)^{\Delta=0}|}{p^n} \cdot \frac{\mathrm{Vol}(V(\mathbb{Z}_p)^{p|\Delta,\max})}{\mathrm{Vol}(V(\mathbb{Z}_p)^{p|\Delta})\mathrm{Vol}(V(\mathbb{Z}_p)^{\max})} = O\left(\frac{1}{p}\right).
\end{aligned} \tag{33}$$

The values of $c_{p,\tau}$ (respectively $c_{p|\Delta}$) are the p-adic densities of the set of elements in $V(\mathbb{Z}_p)$ that have splitting type τ (respectively discriminant divisible by p) within the set of maximal elements in $V(\mathbb{Z}_p)$. We have defined them in this way so that the leading term follows from a computation over $\mathbb{F}_p$.

As mentioned in [61, Section 2.2] the lemma follows from the analogue of the Chebotarev equidistribution for étale coverings which can be established with the Lang–Weil bound. Below we give an elementary proof.

Proof. A set S of n points in $\mathbb{A}^1(\overline{\mathbb{F}}_p)$ is said to be *defined over* $\mathbb{F}_p$ if the set S is fixed by the Galois group of $\overline{\mathbb{F}}_p$ over $\mathbb{F}_p$. A monic degree-n polynomial with coefficients in $\mathbb{F}_p$ yields a set of n points in $\mathbb{A}^1(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$, namely its roots. Conversely, given a set of n points in $\mathbb{A}^1(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$, it determines a unique monic degree-n polynomial with coefficients in $\mathbb{F}_p$.

The number of sets of n points in $\mathbb{A}^1(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ is p^n. If $\Delta(f) = 0$ for $f \in V(\mathbb{F}_p)$, then the corresponding set of n points contains at least one point counted with multiplicity greater than 1. The number of such sets is $\sim p^{n-1}$ which proves the second part of the lemma.

Now consider an unramified splitting type $\tau = (n)^{n_n} \cdots (2)^{n_2}(1)^{n_1}$, where $\sum jn_j = n$. If $f \in V(\mathbb{F}_p)$ has splitting type τ, then the corresponding set of n points consists of n_1 distinct points in $\mathbb{A}^1(\mathbb{F}_p)$, n_2 distinct pairs of conjugate points in $\mathbb{A}^1(\mathbb{F}_{p^2})\backslash\mathbb{A}^1(\mathbb{F}_p)$, and so on. Up to an error term of $O(p^{n_1-1})$, the number of sets of n_1 distinct points in $\mathbb{A}^1(\mathbb{F}_p)$ is $p^{n_1}/n_1!$. Similarly, the number of sets of n_k distinct k-tuples of conjugate points in

$$\mathbb{A}^1(\mathbb{F}_{p^k}) \Bigg\backslash \Bigg(\bigcup_{\substack{d|k\\ d\neq k}} \mathbb{A}^1(\mathbb{F}_{p^d})\Bigg)$$

is $p^{kn_k}/(k^{n_k} \cdot n_k!) + O(p^{kn_k-1})$, since the number of k-tuples of conjugate points in $\mathbb{A}^1(\mathbb{F}_{p^k})$ is p^k/k. Thus, the number of sets of n points in $\mathbb{A}^1(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ corresponding to the splitting type τ is equal to

$$\frac{p^{n_1}}{n_1!}\frac{p^{2n_2}}{2^{n_2}\cdot n_2!}\cdots\frac{p^{kn_k}}{k^{n_k}\cdot n_k!}\cdots\frac{p^{nn_n}}{n^{n_n}\cdot n_n!}+O(p^{n-1}) = \frac{p^n}{|\mathrm{Stab}_{S_n}(\tau)|}+O(p^{n-1}), \quad (34)$$

where the equality follows since the cardinality of the stabilizer of τ in S_n is exactly equal to the denominator of the main term in the left-hand side of the above equation.

Next, we note that conditions of maximality for $f \in V(\mathbb{Z}_p)$ are listed in [2, Corollary 3.2]. In particular, if $f \in V(\mathbb{Z})$ is nonmaximal, then either the reduction of f modulo p has a double root $\alpha \in \mathbb{F}_p$ such that $p^2 \mid f(\tilde{\alpha})$ for any lift $\tilde{\alpha} \in \mathbb{Z}_p$ of α, or f has multiple repeated roots. In either case it follows that $p^2 \mid \Delta(f)$ for nonmaximal elements $f \in V(\mathbb{Z}_p)$. Indeed, the claim for the former case follows simply from the identity $\Delta(f) = (-1)^{n(n-1)/2}\mathrm{Res}(f, f')$, the *resultant* of f and its derivative. For the latter case, the claim follows from the description of the discriminant as the product of differences of roots.

Hence, we see that the volume of the set of nonmaximal elements is bounded by $O(1/p^2)$. Therefore, we obtain

$$\begin{gathered}\frac{1}{\mathrm{Vol}(V(\mathbb{Z}_p)^{\max})} = 1 + O\left(\frac{1}{p^2}\right),\\ \frac{\mathrm{Vol}(V(\mathbb{Z}_p)^{p|\Delta,\max})}{\mathrm{Vol}(V(\mathbb{Z}_p)^{p|\Delta})\mathrm{Vol}(V(\mathbb{Z}_p)^{\max})} = 1 + O\left(\frac{1}{p}\right).\end{gathered} \tag{35}$$

The lemma follows from (34), (35), and the orbit-stabilizer formula which gives $|\mathrm{Stab}_{S_n}(\tau)||\tau| = |S_n|$. □

LEMMA 5.4. *For any prime p, we have*

$$\rho(p) := \frac{\#V(\mathbb{Z}/p^2\mathbb{Z})^{\max}}{\#V(\mathbb{Z}/p^2\mathbb{Z})} = 1 - \frac{1}{p^2}.$$

Proof. This is [2, Proposition 3.5] combined with [2, Corollary 3.2]. □

The asymptotics for the number of elements in $V(\mathbb{Z})$ having bounded height and square-free discriminant is computed in [11]. The key ingredient in that result is the following ‘tail estimate’ proved in [11, Theorem 1.5]:

$$\begin{aligned}&\sum_{\substack{m>M\\ \mu^2(m)=1}} |\{f \in V(\mathbb{Z}) : m^2|\Delta(f), h(f) < x\}|\\ &\ll_\epsilon \frac{x^{((n+1)/(2n-2))+\epsilon}}{M} + x^{((n+1)/(2n-2))-(1/5n(n-1))+\epsilon}.\end{aligned} \tag{36}$$

Recall that $\mathfrak{F}$ denotes the family of $\mathbb{Z}$-orbits in $V(\mathbb{Z})^{\max}$. Thus for $x \geqslant 1$, $\mathfrak{F}(x)$ is in bijection with the set of monogenized fields in $\mathfrak{F}$ arising from irreducible integer monic polynomials having height bounded by x. Let $\mathfrak{F}^{p,\tau}(x)$ and $\mathfrak{F}^{p|\Delta}(x)$ correspond to the set of fields K in $\mathfrak{F}(x)$ such that the splitting type of p in K is τ and such that $p \mid \Delta(K)$, respectively. Using arguments identical to those in [11], we estimate the number of elements in $\mathfrak{F}(x)$, $\mathfrak{F}^{p,\tau}(x)$, and $\mathfrak{F}^{p|\Delta}(x)$.

THEOREM 5.5. *Let $c_{p,\tau}$ and $c_{p|\Delta}$ be as in Lemma 5.3. We have*

$$\begin{aligned} |\mathfrak{F}(x)| &= \frac{2^{n-1}n}{\zeta(2)}x^{(n+2)/2n} + O_\epsilon(x^{((n+2)/2n)-(1/5n(n-1))+\epsilon}),\\ |\mathfrak{F}^{p,\tau}(x)| &= c_{p,\tau}|\mathfrak{F}(x)| + O_\epsilon(x^{((n+2)/2n)-(1/5n(n-1))+\epsilon}p^n),\\ |\mathfrak{F}^{p|\Delta}(x)| &= c_{p|\Delta}|\mathfrak{F}(x)| + O_\epsilon(x^{((n+2)/2n)-(1/5n(n-1))+\epsilon}p^{n-1}). \end{aligned} \tag{37}$$

Proof. We start by computing the number of elements $f \in V(\mathbb{Z})_k$ having height less than x. The coefficients a_i of such an f are as follows: $a_1 = k$ and $|a_i| < x^{i/(n(n-1))}$ for $2 \leqslant i \leqslant n$. Thus there are a total of $\sim 2^{n-1}x^\delta$ such elements f, where $\delta = (n(n+1)/2 - 1)/(n(n-1)) = (n+2)/(2n)$.

For square-free positive m, let $\mathcal{U}_{k,m}(x)$ denote the set of elements $f \in V(\mathbb{Z})_k$ such that R_f is nonmaximal at every prime dividing m and $h(f) < x$. Let $\mathcal{U}_m(x)$ denote $\bigsqcup_{k=0}^{n-1}\mathcal{U}_{k,m}(x)$. Note that if R_f is nonmaximal at a prime p, then $p^2 \mid \Delta(f)$. Since the discriminant of $f(T)$ is equal to the discriminant of $f(T+a)$ for integers a, (36) immediately implies the following estimate:

$$\sum_{\substack{m>M\\ \mu^2(m)=1}} |\mathcal{U}_m(x)| = O_\epsilon(x^{((n+2)/2n)+\epsilon}/M) + O_\epsilon(x^{((n+2)/2n)-(1/5n(n-1))+\epsilon}). \tag{38}$$

(We exclude the factors of n in the error terms since n is assumed to be fixed.)

The set $\mathcal{U}_{k,m}$ is defined via congruence conditions modulo m^2. Let $V(\mathbb{Z}/m^2\mathbb{Z})_k^{\text{nmax}}$ denote the set of elements whose lifts to $V(\mathbb{Z})_k$ are nonmaximal at every prime dividing m. Then for $m \leqslant x^{1/n(n-1)}$ and

$$\rho_k(m) := \frac{\#V(\mathbb{Z}/m^2\mathbb{Z})_k^{\text{nmax}}}{\#V(\mathbb{Z}/m^2\mathbb{Z})_k},$$

we have

$$|\mathcal{U}_{k,m}(x)| = \rho_k(m)2^{n-1}x^{(n+2)/2n} + O(x^{((n+2)/2n)-(2/n(n-1))}).$$

Above, the error term is uniform in m since m^2 is forced to be smaller than the smallest range of the coefficients of the elements in V, namely the range of a_2.

Since the condition of maximality (and hence of nonmaximality) is $\mathbb{Z}$-invariant, it follows that the density of nonmaximal elements in $\bigsqcup_{k=0}^{n-1}V(\mathbb{Z}/m^2\mathbb{Z})_k$ is equal to the density of nonmaximal elements in $V(\mathbb{Z}/m^2\mathbb{Z})$. Furthermore, the size of $V(\mathbb{Z}/m^2\mathbb{Z})_k$ is equal to m^{2n-2} independent of k. It therefore follows that the average of $\rho_k(m)$ is equal to the density of nonmaximal elements in $\bigsqcup_{k=0}^{n-1}V(\mathbb{Z}/m^2\mathbb{Z})_k$, and can be computed from Lemma 5.4 using the multiplicativity over m of this density:

$$\frac{1}{n}\sum_{k=0}^{n-1}\rho_k(m) = \prod_{p\mid m} 1/p^2 = 1/m^2.$$

Therefore, from (32) and (38), we have for $\delta > 0$,

$$\begin{aligned}
|\mathfrak{F}(x)| &= \sum_{m\geqslant 1}\mu(m)|\mathcal{U}_m(x)| + O_\epsilon(x^{((n+2)/2n)-(2/5n(n+1))+\epsilon})\\
&= \sum_{k=0}^{n-1}\sum_{m\geqslant 1}\mu(m)|\mathcal{U}_{k,m}(x)| + O_\epsilon(x^{((n+2)/2n)-(2/5n(n+1))+\epsilon})\\
&= \sum_{k=0}^{n-1}\sum_{m=1}^{x^\delta}\mu(m)\rho_k(m)2^{n-1}x^{(n+2)/2n} + O\left(\sum_{m=1}^{x^\delta} x^{((n+2)/2n)-(2/n(n-1))}\right)\\
&\quad + O_\epsilon(x^{((n+2)/2n)-\delta+\epsilon} + x^{((n+2)/2n)-(1/5n(n-1))+\epsilon})\\
&= \frac{2^{n-1}n}{\zeta(2)}x^{(n+2)/2n} + O_\epsilon(x^{((n+2)/2n)-\delta} + x^{((n+2)/2n)-(2/n(n-1))+\delta}\\
&\quad + x^{((n+2)/2n)-\delta+\epsilon} + x^{((n+2)/2n)-(1/5n(n-1))+\epsilon}).
\end{aligned}$$

We pick $\delta = 1/n(n-1)$ and obtain the first estimate of the theorem. The proofs of the other two estimates are identical. We simply count points in the translates of $pV(\mathbb{Z})$ corresponding to Lemma 5.3. (Here we have chosen not to optimize the exponent of p in the error terms; using the methods in [31] would yield significantly improved error bounds.) □

This concludes the proof of the Sato–Tate equidistribution for this family of monogenized degree-n fields. Therefore, by the results of Section 2 in conjunction with Lemma 5.3 and Theorem 5.5, we see that the symmetry type of the family is symplectic and that the bound on the support given by Theorem 2.8 is $\alpha < 2/(5n(n-1)(2n+1))$.

5.3. Fields arising from binary n-ic forms. Let $W = \mathrm{Sym}^n(2)$ denote the space of all binary n-ic forms. A construction of Nakagawa [54] attaches a degree-n ring R_f to a nondegenerate integral binary n-ic form f. The following geometric construction of R_f is due to Wood [76, Theorem 2.4]: to an integral binary n-ic form $f \in W(\mathbb{Z})$, we associate its scheme X_f of zeros and the ring R_f of regular functions on X_f. This produces a quasi-projective scheme $X \subset W \times \mathbb{P}^1$ which is also a branched covering $X \to W$ of degree n. We may consider the family of fields arising from integral binary n-ic forms that correspond to maximal orders in S_n-fields. This yields a family of L-functions as before. The Sato–Tate equidistribution for this family would follow in identical fashion from a tail estimate, analogous to (36) but for binary n-ic forms $f \in W(\mathbb{Z})$ such that $m^2|\Delta(f)$.

6. Mixed families

In this section, we consider geometric families that are mixed, that is, the fields yielding the L-functions in the families do not all have the same Galois group. However, each family we consider can be naturally partitioned into disjoint subfamilies where the Galois group is constant. The Sato–Tate group of the subfamily is then equal to this Galois group embedded into some linear group $\mathrm{GL}_n(\mathbb{C})$. The Sato–Tate measure of the mixed family is the linear combination of the pushforward measures to the torus of the Sato–Tate groups of all the subfamilies. We thus verify [61, part (ii) of Conjecture 1].

6.1. Binary cubic forms and S_2-, C_3- and S_3-fields. Let $\mathfrak{F}$ denote the family of étale cubic extensions of $\mathbb{Q}$ arising as $R \otimes \mathbb{Q}$, where R corresponds to $\mathrm{GL}_2(\mathbb{Z})$-orbits on the set of maximal integral binary cubic forms that have nonzero discriminant and do not factor as the product of three linear forms over $\mathbb{Q}$. (We omit the cases of $\mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}$ which corresponds to binary cubic forms which split completely over $\mathbb{Q}$.) We have a disjoint decomposition $\mathfrak{F} = \mathfrak{F}_C \sqcup \mathfrak{F}_S \sqcup \mathfrak{F}_Z$, where the family $\mathfrak{F}_C$ corresponds to C_3-fields, the family $\mathfrak{F}_S$ corresponds to S_3-fields (and has been studied in Section 3), and the family $\mathfrak{F}_Z$ corresponds to the direct sums $K \oplus \mathbb{Q}$ of quadratic fields K and $\mathbb{Q}$.

The Sato–Tate group of $\mathfrak{F}_S$ is $S_3 \subset \mathrm{GL}_2(\mathbb{C})$ embedded via the standard representation. For $\mathfrak{F}_C$ the Sato–Tate group is $C_3 \subset S_3 \subset \mathrm{GL}_2(\mathbb{C})$, and for $\mathfrak{F}_Z$ the Sato–Tate group is $S_2 \subset S_3 \subset \mathrm{GL}_2(\mathbb{C})$. Recall that $\mathbb{T} = (S^1)^2/S_2$ consists of pairs of unit complex numbers modulo permutation of the two coordinates. We shall use the notation $\delta(a, b)$, where $a, b \in S^1$, to denote the Dirac delta measure supported at the point $(a, b) \in \mathbb{T}$. Let ρ denote a nontrivial cube root of unity, and let $\bar{\rho}$ denote the complex conjugate of ρ. Then the Sato–Tate measures and the indicators i_1, i_2, and i_3 for the families $\mathfrak{F}_C$, $\mathfrak{F}_S$, and $\mathfrak{F}_Z$ are listed in Table 2.

Note that S_2 and C_3 do not act irreducibly on $\mathbb{C}^2$; as a consequence $i_1(\mathfrak{F}_Z) = i_1(\mathfrak{F}_C) = 2$. This is apparent since the L-function attached to $K \oplus \mathbb{Q} \in \mathfrak{F}_Z$ is $\zeta_K(s) = \zeta(s)L(s, \chi)$, where χ is a Dirichlet character. Similarly, the L-function corresponding to a cyclic cubic field in $\mathfrak{F}_C$ is a product of two Dirichlet L-functions $L(s, \chi)L(s, \overline{\chi})$, where χ is a cubic character. The family of cubic character L-functions $L(s, \chi)$ is itself of unitary symmetry type since it has Sato–Tate group $C_3 \subset \mathrm{GL}_1(\mathbb{C})$. It has been studied for example in [25].

Table 2. Sato–Tate measures and the corresponding indicators for the families in Section 6.1.

Family	Sato–Tate measure	Indicators		
		i_1	i_2	i_3
$\mathfrak{F}_C$	$\frac{1}{3}\delta(1,1)+\frac{2}{3}\delta(\rho,\overline{\rho})$	2	2	0
$\mathfrak{F}_Z$	$\frac{1}{2}\delta(1,1)+\frac{1}{2}\delta(1,-1)$	2	2	2
$\mathfrak{F}_S$	$\frac{1}{6}\delta(1,1)+\frac{1}{2}\delta(1,-1)+\frac{1}{3}\delta(\rho,\overline{\rho})$	1	1	1

It is a consequence of the work of Davenport–Heilbronn that the families $\mathfrak{F}_S$ and $\mathfrak{F}_Z$ occur with positive proportion c_S and c_Z inside $\mathfrak{F}$, while $\mathfrak{F}_C$ has zero proportion. Thus the family $\mathfrak{F}$ satisfies Sato–Tate equidistribution for the measure

$$\mu_{\mathrm{ST}}(\mathfrak{F}) := c_S \cdot \mu_{\mathrm{ST}}(\mathfrak{F}_S) + c_Z \cdot \mu_{\mathrm{ST}}(\mathfrak{F}_Z).$$

The indicators are easily calculated and in fact Table 2 shows that all three are equal to $c_S + 2c_Z$. Similarly, the statistics of the low-lying zeros of $\mathfrak{F}$ are simply the superposition of those of the family $\mathfrak{F}_S$ of S_3-fields and the family $\mathfrak{F}_Z$ of S_2-fields, weighted with the respective proportions c_S and c_Z.

6.2. Pairs of ternary quadratic forms and S_4- and D_4-fields. Recall that $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-orbits on the space of pairs of integral ternary quadratic forms correspond bijectively to isomorphism classes of pairs (Q, R), where Q is a quartic ring and R is a cubic resolvent ring of Q. We may use this parametrization to construct a mixed family $\mathfrak{F}$ of S_4 and D_4 quartic fields. Given a pair (A, B) of integral ternary quadratic forms given in Gram-matrix form and corresponding to a pair of rings (Q, R) as above, the cubic resolvent form is defined to be $f(x, y) = 4\det(Ax - By)$. Then, under the Delone–Faddeev correspondence [28], the integral binary cubic form f corresponds to the cubic resolvent ring R of Q (see [5]). In particular, if Q is an S_4-, D_4-, or A_4-ring, then R is an S_3-ring, an order contained in a direct sum of $\mathbb{Q}$ and a quadratic field, or a C_3-ring, respectively.

When quartic fields are ordered by discriminant, D_4-fields occur with a positive proportion. This is related to the shape of a fundamental domain for the $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-action on $V(\mathbb{R})$, and the presence of 'cusps'. More precisely, one of the cusps of this fundamental domain contains only integral elements (A, B) with $\det(A) = 0$ (see Case II in the proof of [7, Lemma 11]). This implies that if the corresponding quartic ring is nondegenerate, then it is either a D_4-ring or an order contained within the direct sum of two quadratic fields. A 100% of D_4-rings are contained in this cusp, and they make up a positive proportion of irreducible quartic rings.

To construct a geometric family of quartic fields that are either S_4 or D_4, we must restrict to pairs of integral ternary quadratic forms that have nonzero discriminant and are maximal. Furthermore, in order to exclude A_4-rings and reducible rings, we impose the condition that the prime 2 stays inert. That is, we consider the family of fields $\mathfrak{F}$ arising as the field of fractions of rings corresponding to the set of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-orbits on maximal nondegenerate elements of $V(\mathbb{Z})$ whose splitting type at 2 is (4). We then have the decomposition $\mathfrak{F} = \mathfrak{F}_S \sqcup \mathfrak{F}_D$, where $\mathfrak{F}_S$ consists of S_4-fields and $\mathfrak{F}_D$ consists of D_4-fields. This is one instance where one can perform rigorously the decomposition alluded to in the remarks concerning [61, assertion (ii) of Conjecture 1].

Quartic D_4-orders may also be distinguished from S_4-orders using the property that a cubic resolvent of a D_4-order is a suborder of $\mathbb{Q} \oplus K$, where K is a quadratic field. In contrast, the cubic resolvent of an S_4-order is an order in an S_3-cubic field. Exploiting this difference, Wood [74, Section 7.3] parametrizes quartic rings with reducible resolvent rings as G-orbits, where G is a subgroup of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$, on the space of pairs (A, B) of integral ternary quadratic forms such that A has top row zero and $a_{12} \neq 0$. The quartic rings that arise include all D_4-orders but no S_4-orders. Let U be the space of quadruples (A, B, x, y) of two integral ternary quadratic forms A and B as above and two integers x and y such that $\det(Ax - By) = 0$. Geometrically the cusp containing D_4-fields arises from the natural equivariant map $U \to V$. Indeed, the common zero locus of A and B in $\mathbb{P}^2$ yields branched 4-covers of V and U whose normal closures have Galois groups S_4 and D_4 respectively. The family $\mathfrak{F}_D$ is parametrized by the $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ orbits in $U(\mathbb{Z})$.

The Sato–Tate group for $\mathfrak{F}_S$ is $S_4 \subset \mathrm{GL}_3(\mathbb{C})$ embedded via its standard representation, and the Sato–Tate group for $\mathfrak{F}_D$ is $D_4 \subset S_4 \subset \mathrm{GL}_3(\mathbb{C})$. We identify $\mathbb{T}$ with $(S^1)^3$ modulo permutation of the three coordinates and use the notation $\delta(a, b, c)$ to denote the Dirac delta measure supported at the point (a, b, c). Then the Sato–Tate measures and the indicators i_1, i_2, and i_3 for the families $\mathfrak{F}_S$ and $\mathfrak{F}_D$ are listed in Table 3. The computations of the indicators are elementary, and only require the character of the standard representation of S_4. The proof of Sato–Tate equidistribution follows from Baily's [3] and Bhargava's [7] counting results on D_4- and S_4-fields, respectively.

Since D_4 does not act irreducibly on $\mathbb{C}^3$, the family $\mathfrak{F}_D$ is not essentially cuspidal. In fact $\mathbb{C}^3$ decomposes as the direct sum of the standard 2-dimensional representation of D_4 and the character of D_4 whose kernel is generated by the two transpositions of D_4, so we can write $\mathfrak{F}_D = \mathfrak{F}_{\mathrm{dih}} \oplus \mathfrak{F}_{\mathrm{char}}$. Geometrically we can describe $\mathfrak{F}_{\mathrm{char}}$ as a branched 2-cover constructed as follows: for $(A, B, x, y) \in U$,

Table 3. Sato–Tate measures and the corresponding indicators for the families in Section 6.2.

Family	Sato–Tate measure	Indicators		
		i_1	i_2	i_3
$\mathfrak{F}_S$	$\frac{1}{24}\delta(1,1,1)+\frac{1}{4}\delta(1,1,-1)+\frac{1}{3}\delta(1,\rho,\overline{\rho})+\frac{1}{4}\delta(-1,i,-i)+\frac{1}{8}\delta(1,-1,-1)$	1	1	1
$\mathfrak{F}_D$	$\frac{1}{8}\delta(1,1,1)+\frac{1}{4}\delta(1,1,-1)+\frac{1}{4}\delta(-1,i,-i)+\frac{3}{8}\delta(1,-1,-1)$	2	2	2

the zero set of the degenerate ternary quadratic form $Ax - By$ is the union of two lines in $\mathbb{P}^2$. These two lines are joining opposite points of the common zero locus of A and B and the interpretation is that this picture is preserved by the action of D_4.

The Sato–Tate equidistribution for $\mathfrak{F}_D$ and $\mathfrak{F}_S$ follows from the methods in [**7**, **21**], respectively. We deduce this equidistribution for $\mathfrak{F}_D$ in the following proposition. Note that the equidistribution for the family $\mathfrak{F}_S$ follows from the results of Section 3.2.

PROPOSITION 6.1. *The family $\mathfrak{F}_D$ is equidistributed with respect to the measure given in Table 3.*

In other words and with the same notation as for (11), the proposition is saying that for every $\tau \in \mathcal{T}_4$ the value of

$$\lim_{y\to\infty}\lim_{x\to\infty}\frac{1}{|\mathfrak{F}_D(x)|\cdot\pi(y)}\sum_{p<y}|\mathfrak{F}_D^{p,\tau}(x)|$$

is given by Table 3. Namely, for $\tau = (1, 1, 1)$, the limit is equal to $\frac{1}{8}$, for $\tau = (1, 1, -1)$, the limit is equal to $\frac{1}{4}$, and so on. In relation to (1), this means that

$$\{\rho_L(\mathrm{Frob}_p) : L \in \mathfrak{F}_D(x),\ p < y\} \subset \mathcal{T}_4$$

is equidistributed as $x \to \infty$ and $y \to \infty$ (taking the limits in this order), for the measure given in Table 3, which coincides with the pushforward of the counting measure on $D_4 \subset S_4$.

Proof. The family of dihedral fields is contained in the union of quadratic extensions of quadratic fields: we write

$$\mathfrak{F}_D \subset \bigsqcup_K \mathfrak{F}_2(K) =: \mathfrak{F}_{2,2},$$

where the (disjoint) union is over quadratic fields K, ordered by the absolute values of $\mathrm{Disc}(K)$, and where $\mathfrak{F}_2(K)$ denotes the family of quadratic extensions of K (recall that a D_4-field contains a unique quadratic subfield). By the results of [21], it follows that there are negligibly many nondihedral fields contained within $\mathfrak{F}_2(K)$, for every K, and hence within $\mathfrak{F}_{2,2}$ as well. As a consequence, for the purpose of proving Sato–Tate equidistribution, we may replace the family $\mathfrak{F}_D$ with the family $\mathfrak{F}_{2,2}$ of quadratic extensions of quadratic fields. In what follows, we will prove Sato–Tate equidistribution for each subfamily $\mathfrak{F}_2(K)$, and then deduce the same equidistribution for $\mathfrak{F}_{2,2}$.

Let K be a fixed quadratic field, and let p be a prime in $\mathbb{Q}$ unramified in K. If the splitting type of p in K is (11), then in a proportion of $1/4 + O(1/p)$ (respectively $3/4 + O(1/p)$) of quadratic extensions L/K, the splitting type of p in L is (1111) (respectively (112)). On the other hand, if the splitting type of p in K is (2), then in a proportion of $1/2 + O(1/p)$ (respectively $1/2 + O(1/p)$) of quadratic extensions L/K, the splitting type of p in L is (22) (respectively (4)). In conjunction with the Chebotarev density theorem, it follows that the family $\mathfrak{F}_2(K)$ is equidistributed with respect to the measure as given in the second line of Table 3.

Fix a real number M. Then the Sato–Tate measure of the family

$$\mathfrak{F}_{2,2,M} := \bigsqcup_{|\Delta(K)|<M} \mathfrak{F}_2(K)$$

is a finite weighted sum over K of the Sato–Tate measures of $\mathfrak{F}_2(K)$. Since the measure is independent of K, the exact values of the weights are irrelevant; and the Sato–Tate measure of $\mathfrak{F}_{2,2,M}$ is as given in Table 3.

It is proven in [21] that the family $\mathfrak{F}_{2,2} \backslash \mathfrak{F}_{2,2,M}$ has density $\ll_\epsilon M^{-1+\epsilon}$ in $\mathfrak{F}_{2,2}$. In particular

$$\frac{|\mathfrak{F}_D^{p,\tau}(x)|}{|\mathfrak{F}_D(x)|} = \frac{|\mathfrak{F}_{2,2,M}^{p,\tau}(x)|}{|\mathfrak{F}_{2,2,M}(x)|} + O_\epsilon(M^{-1+\epsilon}),$$

uniformly in p and x. Therefore, the Sato–Tate measure of $\mathfrak{F}_{2,2}$ differs from the second row of Table 3 by a summand of $O_\epsilon(M^{-1+\epsilon})$. The result now follows by letting M tend to infinity. □

REMARK 6.2. In [21], the asymptotics of $\mathfrak{F}_D$ (equivalently, of $\mathfrak{F}_{2,2}$) is computed when the fields are ordered by discriminant:

$$|\{L \in \mathfrak{F}_D : |\Delta(L)| < X|\} \sim \frac{3}{\pi^2} \cdot \left(\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0<|\mathrm{Disc}(K)|<\infty}} \frac{2^{-i(K)}}{\mathrm{Disc}(K)^2} \cdot \frac{L(1, K/\mathbb{Q})}{L(2, K/\mathbb{Q})} \right) \cdot X$$

where $i(K)$ denotes the number of complex places of K. It is interesting to note that the rather complicated constant of asymptoticity plays no role either in the statement or the proof of Proposition 6.1. This is because the Sato–Tate measures of every fiber $\mathfrak{F}_2(K)$ of $\mathfrak{F}_{2,2}$ are the same.

Since the dihedral representation $D_4 \subset \mathrm{GL}_2(\mathbb{C})$ and the above character $D_4 \to \mathrm{GL}_1(\mathbb{C})$ are orthogonal, we expect both $\mathfrak{F}_{\mathrm{dih}}$ and $\mathfrak{F}_{\mathrm{char}}$ to have Symplectic symmetry type. The distribution of the low-lying zeros for the family $\mathfrak{F}_D$ will then be the independent direct sum of two $\mathrm{Sp}(\infty)$ ensembles. In particular, for restricted support of the level densities, we expect there to be no correlation between the zeros of $L(s, \mathrm{dih}_K)$ and $L(s, \mathrm{char}_K)$ as K ranges over D_4-fields. One step in the direction of establishing this is [21, Corollary 6.1]; however we have not verified whether the argument given there can be adapted to yield the desired quantitative equidistribution for $\mathfrak{F}_D$ (with a power saving error estimate for $\log x/\log y$ large enough). We also have not verified Sato–Tate equidistribution for individual primes in the sense of (10), which would be significantly more complicated, due to the nature of the leading constant in the asymptotic count of D_4-quartic fields ordered by discriminant.

As in Section 6.1, we find the family $\mathfrak{F}$ to satisfy Sato–Tate equidistribution for the measure

$$\mu_{\mathrm{ST}}(\mathfrak{F}) = c_S \cdot \mu_{\mathrm{ST}}(\mathfrak{F}_S) + c_D \cdot \mu_{\mathrm{ST}}(\mathfrak{F}_D),$$

where c_S and c_D denote the proportions of $\mathfrak{F}_S$ and $\mathfrak{F}_D$ inside $\mathfrak{F}$. It follows immediately from Table 3 that the corresponding indicators satisfy $i_1(\mathfrak{F}) = i_2(\mathfrak{F}) = i_3(\mathfrak{F}) = c_S + 2c_D$. Finally, the statistics of the low-lying zeros of $\mathfrak{F}$ are simply the superposition of those of the families $\mathfrak{F}_S$ and $\mathfrak{F}_D$, weighted with the respective proportions c_S and c_D.

7. Local equidistribution for S_n-families

Sections 3 and 5 were concerned with the splitting behavior of unramified primes in families of number fields. In the present section we investigate the ramified primes. We conclude the section with a reformulation of Bhargava's heuristics [9] for counting number fields, via a comparison with Peyre's constant [57] for the counting of rational points on Fano varieties.

7.1. Binary n-ic forms.

We begin with the family $\mathfrak{F} = \mathfrak{F}_{n\text{-ic}}$ of binary n-ic forms. Each field in this family can be thought of as arising from a set $S = X_f$ of n points in $\mathbb{P}^1(\overline{\mathbb{Q}})$ defined over $\mathbb{Q}$. The absolute Galois group of $\mathbb{Q}$ acts on this set, and the fixed subgroup of the Galois group cuts out the number field $M = M_f$

corresponding to these n points. Thus, we obtain an injection

$$\mathrm{Gal}(M/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(S) \cong S_n.$$

Fix a prime p. We may consider the reduction $\overline{S} = X_f \otimes_{\mathbb{Z}} \mathbb{F}_p$ of S modulo p which yields n points, counted with multiplicity, in $\mathbb{P}^1(\overline{\mathbb{F}_p})$. This set $\overline{S}$ is defined over $\mathbb{F}_p$, and the absolute Galois group of $\mathbb{F}_p$ acts on it. The splitting type of p is determined by the orbit decomposition of this action. More precisely, if $\overline{S}$ breaks up into orbits having size $a_1, a_2, \ldots, a_\ell$ (in decreasing order), then the splitting type of p in $K = K_f$ is $\sigma = \sigma(\overline{S}) = (a_1 a_2 \cdots a_\ell)$. In particular, p is unramified in K if and only if $\overline{S}$ consists of n distinct points. Motivated by this, we define the splitting type of such a set $\overline{S}$ to be $\sigma \in \mathcal{ST}_n$, where $\mathcal{ST}_n$ denotes the set of all possible splitting types on n points.

Consider the (finite) set of sets of n points, counted with multiplicity, in $\mathbb{P}^1(\overline{\mathbb{F}_p})$ that are defined over $\mathbb{F}_p$. We have seen in the proof of Lemma 5.3 that it is naturally identified with the set of nonzero forms $V(\mathbb{F}_p) - \{0\}$ modulo multiplication by $\mathrm{GL}_1(\mathbb{F}_p) = \mathbb{F}_p^\times$. Thus for every prime p we have a map $V(\mathbb{F}_p) - \{0\} \to \mathcal{ST}_n$. Pushing forward the counting measure on $V(\mathbb{Z}/p^2\mathbb{Z})^{p^2 \nmid \Delta}$ via

$$V(\mathbb{Z}/p^2\mathbb{Z})^{p^2 \nmid \Delta} \to V(\mathbb{F}_p) - \{0\} \twoheadrightarrow \mathcal{ST}_n, \tag{39}$$

we obtain a measure $\mu_{\text{n-ic},p}$ on $\mathcal{ST}_n$.

If $\mathfrak{F}$ is the family of fields arising from integral binary n-ic forms having squarefree discriminant, then each field $K_f \in \mathfrak{F}$, corresponding to f, arises from the set X_f of the n roots of f in $\mathbb{P}^1(\overline{\mathbb{Q}})$. We have natural reduction maps for every prime p,

$$\begin{aligned} \mathfrak{F}(x) &\to \mathcal{ST}_n \\ K_f &\mapsto \sigma(X_f \otimes_{\mathbb{Z}} \mathbb{F}_p). \end{aligned}$$

We expect that the image of $\mathfrak{F}(x)$ gets equidistributed in $V(\mathbb{Z}/p^2\mathbb{Z})^{p^2 \nmid \Delta}$ and therefore also in $\mathcal{ST}_n$, as $x \to \infty$, with respect to the measure $\mu_{\text{n-ic},p}$.

This statement would generalize (12) which is the unramified case. The unramified splitting types belong to the subset $\mathcal{T}_n \subset \mathcal{ST}_n$ defined in Section 2. The restriction of the measure $\mu_{\text{n-ic},p}$ to $\mathcal{T}_n$ takes the form of the pushforward of the normalized counting measure via the map

$$V(\mathbb{F}_p)^{\Delta \neq 0} \to \mathcal{T}_n \subset \mathcal{ST}_n,$$

which one may compare with (39). The natural normalization of the measure is $\mu_{\text{n-ic},p}(\mathcal{T}_n) = 1$.

Some of the analogous constructions are also valid for fields arising from n points in $\mathbb{P}^k$. However, in this case it is necessary to count ramified points along with the additional data of local tangent directions.

7.2. S_n-fields of bounded discriminant. We now consider the families $\mathfrak{F} = \mathfrak{F}_{\mathrm{univ}}$ of S_n-fields of bounded discriminants with $n = 3, 4, 5$ as in Section 3. In addition to Theorems 3.5 and 3.7, Bhargava also established the equidistribution at ramified primes.

Let $\mathcal{ET}_{n,p}$ denote the (finite) set of degree-n étale extensions of $\mathbb{Q}_p$, and let $\mu_{\mathrm{univ},p}$ be the measure where each étale extension K_p is weighted proportionally to $\mathrm{Disc}_p(K_p)^{-1}\#\mathrm{Aut}(K_p)^{-1}$, and normalized by $\mu_{\mathrm{univ},p}(\mathcal{T}_n) = 1$. The total sum of these relative proportions is computed in [9, Proposition 2.3] extending a mass formula for totally ramified extensions due to Serre. It is remarkable that the answer is independent of the prime p, including the primes p dividing $n!$ which may wildly ramify.

PROPOSITION 7.1 [9]. *For any prime p and integers $0 \leqslant k \leqslant n-1$ with $n \geqslant 1$,*

$$\sum_{\substack{[K_p:\mathbb{Q}_p]=n \\ \mathrm{Disc}_p(K_p)=p^k}} \frac{1}{\#\mathrm{Aut}(K_p)} = q(k, n-k),$$

where the sum in the left-hand side is over étale extensions of $\mathbb{Q}_p$ of discriminant p^k and $q(k, n-k)$ denotes the number of partitions of k into at most n − k parts.

We have a natural map from $\mathfrak{F}(x)$ to $\mathcal{ET}_{n,p}$ which sends K to $K \otimes \mathbb{Q}_p$. For $n = 3, 4, 5$, the respective works of Davenport–Heilbronn [24], and Bhargava [7, 8] show that, for a fixed local étale degree-n extension K_p of $\mathbb{Q}_p$, the relative proportion of S_n-fields K that satisfy $K \otimes \mathbb{Q}_p \equiv K_p$ is $\mathrm{Disc}_p(K_p)^{-1}\#\mathrm{Aut}(K_p)^{-1}$. Thus, as we range over fields in $\mathfrak{F}(x)$ and let $x \to \infty$, the images in $\mathcal{ET}_{n,p}$ are equidistributed with respect to this measure $\mu_{\mathrm{univ},p}$.

The proof involves, among other things, the relation between the measure $\mu_{\mathrm{univ},p}$ and the local counting of orbits. From the prehomogeneous vector spaces (G, V) we have a surjective map

$$V(\mathbb{Z}/p^\nu\mathbb{Z})^{\Delta\neq 0} \twoheadrightarrow \mathcal{ET}_{n,p},$$

where $\nu \in \mathbb{Z}_{\geqslant 1}$ is an absolute constant to be chosen large enough. (The existence of this ν is a concrete manifestation in this context of Grothendieck's base change theorem.) The measure $\mu_{\mathrm{univ},p}$ is equal to the pushforward of the normalized counting measure which is established by a local density calculation [5, 6] exploiting the $G(\mathbb{Z}/p^\nu\mathbb{Z})$-action.

It is interesting to compare the present situation with the one in Section 7.1. We relate the underlying sets as follows: for each choice of n and p, there is a natural surjective map

$$\mathcal{ET}_{n,p} \twoheadrightarrow \mathcal{ST}_n \supset \mathcal{T}_n,$$

where we associate to each degree-n étale extension K_p its splitting type. This is a local counterpart of (4), by choosing an embedding $\mathrm{Gal}(\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\mathbb{Q})$. The size of the fibers to $\mathcal{ST}_n$ can be read from the orbits of inertia as explained in [44, 77]. The pushforward of the measure $\mu_{\mathrm{univ},p}$ does *not* coincide with the measure $\mu_{\text{n-ic},p}$, although in the limit as $p \to \infty$ both measures converge to the Haar measure on $\mathcal{T}_n$. In fact, the restriction to $\mathcal{T}_n$ of the pushforward of $\mu_{\mathrm{univ},p}$ coincides up to a scalar with the Haar measure on $\mathcal{T}_n$ because the orbit-stabilizer formula shows that $|\tau||\mathrm{Stab}_{S_n}(\tau)| = |S_n|$.

We note that to understand the equidistribution in $\mathcal{ST}_n$, it is in general sufficient to consider $V(\mathbb{Z}/p^\nu\mathbb{Z})^{\Delta\neq 0}$ with $\nu = 2$, while to understand the equidistribution in $\mathcal{T}_n$ it is sufficient to take $\nu = 1$.

For general n, let $\mathfrak{F}_{\mathrm{univ}}(x)$ denote the set of S_n-number fields having discriminant bounded by x. Bhargava formulates in [9] conjectures for the asymptotics of $|\mathfrak{F}_{\mathrm{univ}}(x)|$ and for the proportion of fields with prescribed splitting at a prime p. For $n \geqslant 6$ the conjectures remain open. Note also that in these cases we cannot view $\mathfrak{F}_{\mathrm{univ}}(x)$ as a geometric family in the sense of [61] because the underlying parameter space is a set of integral points of a complicated algebraic variety which is believed to not be rational.

7.3. An analogue of Peyre's constant.

Consider the S_n-family $\mathfrak{F} = \mathfrak{F}_{\mathrm{univ}}$ of n points in $\mathbb{P}^{n-2}$ for $n = 3, 4, 5$ as in Section 7.2. The measure $\mu_{\mathrm{univ},p}$ on $\mathcal{ET}_{n,p}$ is normalized by $\mu_{\mathrm{univ},p}(\mathcal{T}_n) = 1$. It is established in [9] that the proportion of S_n-number fields that are unramified at p is the inverse of

$$|\mu_{\mathrm{univ},p}| := \mu_{\mathrm{univ},p}(\mathcal{ET}_{n,p}) = \sum_{k=0}^{n-1} q(k, n-k)p^{-k}.$$

As $p \to \infty$, this is $1 + (1/p) + O(1/p^2)$. By Proposition 7.1, the local density [9] of number fields of bounded discriminants can be written as

$$d_p(\mathfrak{F}_{\mathrm{univ}}) := |\mu_{\mathrm{univ},p}| \cdot \zeta_p(1)^{-1} = \sum_{k=0}^{n} \frac{q(k, n-k) - q(k-1, n-k+1)}{p^k}, \quad (40)$$

where $\zeta_p(1) = (1 - 1/p)^{-1}$ is the local factor of the Riemann zeta function. Similarly there is a local density at infinity $d_\infty(\mathfrak{F}_{\mathrm{univ}})$ which is equal to the proportion of 2-torsion elements in S_n. The theorems of Davenport–Heilbronn and Bhargava say that the number $|\mathfrak{F}_{\mathrm{univ}}(x)|$ of S_n-fields having absolute discriminant at most x is asymptotic to $c_n x$ as $x \to \infty$, where the constant $c_n = \frac{1}{2} \cdot d_\infty(\mathfrak{F}_{\mathrm{univ}}) \cdot \prod_p d_p(\mathfrak{F}_{\mathrm{univ}})$.

This may be compared with Peyre's constant attached to Fano varieties, as follows. The product of local densities is equal to the regularized product of local mass of the measures $\mu_{\mathrm{univ},p}$,

$$\prod_p d_p(\mathfrak{F}_{\mathrm{univ}}) = \prod_p{}^{*} |\mu_{\mathrm{univ},p}| := \mathrm{Res}_{s=1}\zeta(s) \cdot \prod_p |\mu_{\mathrm{univ},p}| \cdot \zeta_p(1)^{-1}.$$

The regularization by ζ is explained by the prehomogeneous vector space (G, V), having a ring of invariant functions generated by Δ, thus the GIT quotient is rational. The measures $\mu_{\mathrm{univ},p}$ are normalized globally by the condition $\mu_{\mathrm{univ},p}(\mathcal{T}_n) = 1$, which can be seen as the analogue of the global normalization of Tamagawa measures. In comparison with Peyre [57], the 'Picard rank' is interpreted to be 1, which is also the order of pole of $\zeta(s)$, the 'Tamagawa number' is 1, and Peyre's constant 'α' is interpreted to be $\frac{1}{2}$, which reflects the global constraint that, according to a classical result of Hasse, the discriminant of an S_n-field is always $\equiv 0, 1 \pmod 4$.

The same reasoning could be applied to the general geometric families $\mathfrak{F}$ described in [61], and also to the automorphic families, to produce a conjectural leading term of the asymptotic count of $|\mathfrak{F}(x)|$ as $x \to \infty$.

8. One-parameter families of quaternionic fields

In this section, we study families of quaternionic number fields, that is, Galois number fields K such that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the quaternion group Q. The group Q is a nonabelian group of order 8 with the presentation

$$\langle i, j, k \mid i^2 = j^2 = k^2 = ijk\rangle.$$

We denote the element $i^2 = j^2 = k^2 = ijk$ by -1.

The group Q has five irreducible representations. Apart from the trivial representation, Q has three 1-dimensional irreducible representations, coming from the maps which send one of i, j, and k to 1 and the other two to -1. We denote these three nontrivial characters by χ_1, χ_2, and χ_3, respectively. Finally, apart from these four representations, Q has an irreducible 2-dimensional representation which we denote by ρ and whose trace character we denote by χ. The character χ sends ± 1 to ± 2 and the other elements of Q to 0. We deduce that the Frobenius–Schur indicator of ρ is -1. In other words, ρ is a quaternionic representation (also called symplectic representation).

The zeta function $\zeta_K(s)$ factors into the product

$$\zeta_K(s) = \zeta(s)L(s, \chi_1)L(s, \chi_2)L(s, \chi_3)L(s, \rho_K)^2,$$

where

$$\rho_K : \mathrm{Gal}(\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \simeq Q \to \mathrm{SL}_2(\mathbb{C}) \subset \mathrm{GL}_2(\mathbb{C}).$$

Thus in comparison with Section 2, the Artin L-function of interest, that is, $L(s, \rho_K)$, is constructed in a slightly different way. The isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \simeq Q$ is not unique but ρ_K is nevertheless uniquely defined up to conjugation because Q has exactly one irreducible 2-dimensional representation. We also note that $L(s, \rho_K)$ can be realized as the L-function of a Hecke character of order four of a real quadratic extension of $\mathbb{Q}$, since the irreducible 2-dimensional representation of Q is induced from a character on any of its cyclic subgroups of order four. Therefore $L(s, \rho_K)$ is entire. Furthermore, the functions $L(s, \chi_i)$, $i \in \{1, 2, 3\}$, are Dirichlet L-functions corresponding to the three quadratic subfields of the unique biquadratic subfield M of K, which is also the subfield of elements of the extension K fixed by the center $\{\pm 1\} \subset Q$. For a treatment of all the above facts regarding Artin L-functions, see [18, Ch. 8].

We now examine the question of how a rational prime p splits in K and M. In this section we will use exponents outside parentheses as a convenient shorthand for repetitions in splitting types; we will for example, write $(1)^8$ and $(1^2)^4$ instead of (11111111) and $(1^2 1^2 1^2 1^2)$, respectively. In the case when p is unramified, the splitting is determined by the image of Frob_p in $\mathrm{Gal}(K/\mathbb{Q})$. If Frob_p has image 1 in Q, then the splitting type of p is $(1)^8$ in K and $(1)^4$ in M, since the size of the decomposition group is 1. Similarly, if Frob_p has image -1, then the splitting type of p is $(2)^4$ in K and $(1)^4$ in M. Otherwise, the splitting type of p is $(4)^2$ in K and $(2)^2$ in M. If p is tamely ramified, then we have the following possibilities for the pair (D, I) of the decomposition and inertia groups: (C_4, C_4), (C_4, C_2), and (C_2, C_2). The corresponding splitting types of p in K are $(1^4)^2$, $(2^2)^2$, and $(1^2)^4$, respectively.

THEOREM 8.1. *Let $a, b \in \mathbb{Q}^\times$ be such that none of a, b, ab is a perfect square. Then the following assertions are equivalent:*

(i) *There exists a quaternionic extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{a}, \sqrt{b})$.*

(ii) *For each prime p the relation $(-a, -b)_p = (-1, -1)_p$ of Hilbert symbols holds. (See* [55, Section III.5] *for the definition and basic properties of the Hilbert symbol.)*

(iii) *The quaternion algebra $(\frac{-a,-b}{\mathbb{Q}})$ is isomorphic to the Hamilton quaternions $(\frac{-1,-1}{\mathbb{Q}})$.*

(iv) *The ternary quadratic form $\langle a, b, ab\rangle$ is equivalent to $\langle 1, 1, 1\rangle$ over $\mathbb{Q}$. (Here we are denoting the ternary quadratic form $\alpha x^2 + \beta y^2 + \gamma z^2$ by $\langle \alpha, \beta, \gamma\rangle$.)*

(v) *There exist* $\alpha, \beta, \gamma, \lambda, \mu, \nu \in \mathbb{Q}$ *such that*

$$\begin{aligned} a &= \alpha^2 + \beta^2 + \gamma^2 \\ b &= \lambda^2 + \mu^2 + \nu^2 \\ 0 &= \alpha\lambda + \beta\mu + \gamma\nu. \end{aligned}$$

Moreover, if the above assertions are satisfied, and we define

$$\theta := 1 + \frac{\alpha}{\sqrt{a}} + \frac{\mu}{\sqrt{b}} + \frac{\alpha\mu - \beta\lambda}{\sqrt{ab}}, \tag{41}$$

then the quaternionic extensions of $\mathbb{Q}$ *containing* $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ *are exactly those of the form* $\mathbb{Q}(\sqrt{q\theta})$ *with* $q \in \mathbb{Q}^\times$.

Proof. The equivalence (ii) ⇔ (iv) follows from the theory of quadratic forms (from, for example, [17, Ch. 6, Theorem 1.2 and Ch. 4, Theorem 1.1]). The equivalence (iii) ⇔ (iv) follows from [49, Proposition 2.5 (page 57)] and the equivalence (ii) ⇔ (iii) follows from class field theory; see [71, Corollaire 1.2 (page 32)].

Assertion (v) is equivalent to $M^T M = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ where $M := \left(\begin{smallmatrix} \alpha & \lambda \\ \beta & \mu \\ \gamma & \nu \end{smallmatrix}\right)$, and assertion (iv) is equivalent to the existence of a 3×3 matrix N such that $N^T N = \left(\begin{smallmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{smallmatrix}\right)$. Thus (iv) ⇒ (v) is immediate by extracting the first two columns of N. Conversely, (v) ⇒ (iv) follows by completing M with the third column

$$(\beta\nu - \gamma\mu, \gamma\lambda - \alpha\nu, \alpha\mu - \beta\lambda)^T$$

to obtain the equivalence of the quadratic forms.

The equivalence (i) ⇔ (iii) ⇔ (iv) is Witt's theorem [73]. We outline Witt's original proof of the equivalence (i) ⇔ (iii) because it does not seem to be well-known. Witt first considers the nonsplit exact sequence

$$1 \to \{\pm 1\} \to Q \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to 1,$$

where $\{\pm 1\}$ is the center and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is given by the image of $\{1, i, j, k\}$. This yields a class $\xi \in H^2(\mathbb{Q}(\sqrt{a}, \sqrt{b}), \overline{\mathbb{Q}}^\times)$ of order two. Moreover ξ is trivial after inflating to $\mathbb{Q}$ if and only if (i) holds. Identifying Galois cohomology with the Brauer group, it can be verified that the inflation of ξ to $\mathbb{Q}$ corresponds to the central simple algebra

$$\left(\frac{-a, -b}{\mathbb{Q}}\right) \otimes \left(\frac{-1, -1}{\mathbb{Q}}\right)$$

of dimension 16 over $\mathbb{Q}$. By the properties of the Brauer group this algebra is split over $\mathbb{Q}$ if and only if $(\frac{-a,-b}{\mathbb{Q}})$ is isomorphic to $(\frac{-1,-1}{\mathbb{Q}})$, which concludes the proof of (i) $\Leftrightarrow$ (iii).

Let θ be given by (41). The final assertion of the theorem is [45, Theorem 4]. We outline the proof in our notation. Using (v), we find that the norm of θ in $\mathbb{Q}(\sqrt{a})$ is equal to $(1/b)(\nu+((\alpha\nu-\gamma\lambda)/\sqrt{a}))^2$. Hence b is a sum of two squares in $\mathbb{Q}(\sqrt{a})$ and furthermore $\mathbb{Q}(\sqrt{\theta})$ is a cyclic extension of $\mathbb{Q}(\sqrt{a})$. Similarly we find that $\mathbb{Q}(\sqrt{\theta})$ is a cyclic extension of $\mathbb{Q}(\sqrt{b})$ and a cyclic extension of $\mathbb{Q}(\sqrt{ab})$. Since Q is the only group of order 8 that contains three distinct cyclic subgroups of order 4 we deduce that $\mathbb{Q}(\sqrt{\theta})$ has Galois group Q.

Suppose that K is another quaternionic extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{a},\sqrt{b})$. From [36, Section 3], the composition of K with $\mathbb{Q}(\sqrt{\theta})$ is the field $K(\sqrt{\theta})$ which is biquadratic over $\mathbb{Q}(\sqrt{a},\sqrt{b})$ and has degree 16 over $\mathbb{Q}$ with Galois group $Q\times\mathbb{Z}/2\mathbb{Z}$. There are three intermediate extensions between $\mathbb{Q}(\sqrt{a},\sqrt{b})$ and $K(\sqrt{\theta})$: K, $\mathbb{Q}(\sqrt{\theta})$, and a third which has Galois group $(\mathbb{Z}/2\mathbb{Z})^3$ over $\mathbb{Q}$, and thus is of the form $\mathbb{Q}(\sqrt{a},\sqrt{b},\sqrt{c})$ for some $c\in\mathbb{Q}^\times$. Then we have $K(\sqrt{\theta})=\mathbb{Q}(\sqrt{\theta},\sqrt{c})$ and one verifies that $K=\mathbb{Q}(\sqrt{q\theta})$ for some $q\in\mathbb{Q}^\times$ which may differ from c in its factorization above primes dividing ab. □

REMARK 8.2. The last two paragraphs of the proof of Theorem 8.1 independently establish the implication (v) $\Rightarrow$ (i); see [41, 58] for variations of this argument. We also note that [58] shows how to establish the implication (i) $\Rightarrow$ (ii) in a case by case verification.

COROLLARY 8.3. *A necessary condition for the existence of a quaternionic extension of $\mathbb{Q}$ containing $\mathbb{Q}(\sqrt{a},\sqrt{b})$ is that each of a, b, ab is a sum of three squares.*

Proof. This follows immediately from the implication (i) $\Rightarrow$ (iv) of Theorem 8.1. □

REMARK 8.4. The converse of Corollary 8.3 does not hold in general. A counterexample is given by $a=163$ and $b=14$; see [70, Theorem 4]. However, it is true that $\mathbb{Q}(\sqrt{a})$ is embeddable in a quaternionic extension of $\mathbb{Q}$ if and only if a is a sum of three squares (see, for example, [41, (II.2.1)]).

We now describe the families of quaternionic number fields that we consider in this section. We shall choose a and b such that 2 is unramified in $\mathbb{Q}(\sqrt{a},\sqrt{b})$; that is, we assume that $a,b\equiv 1 \pmod 4$, are square-free and satisfy the assumptions of Theorem 8.1. Consider the family $\mathfrak{F}$ of quaternionic fields $K_q=\mathbb{Q}(\sqrt{q\theta})$ containing $\mathbb{Q}(\sqrt{a},\sqrt{b})$, where a and b are fixed, θ is provided by Theorem 8.1, and $q \equiv 0, 1 \pmod 4$ varies over fundamental discriminants relatively prime to ab.

LEMMA 8.5. *The conductor of the Artin representation corresponding to $\mathbb{Q}(\sqrt{q\theta})$ is $2^\alpha r(ab)^2(q^*)^2$, with $\alpha \in \{0, 4\}$, and where $r(ab)$ denotes the square-free part of ab, and q^* denotes the odd part of q.*

Proof. This is established by Fröhlich [36], and we provide here a somewhat more direct proof. The splitting pattern in the biquadratic field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ of an odd prime p dividing q is $(1)^4$ or $(2)^2$. The odd prime p is unramified in $\mathbb{Q}(\sqrt{\theta})$ and ramified in the quadratic extension $\mathbb{Q}(\sqrt{q})$ which is a subfield of $\mathbb{Q}(\sqrt{\theta}, \sqrt{q\theta})$, hence it is ramified in $\mathbb{Q}(\sqrt{q\theta})$. Thus the splitting pattern of p in $\mathbb{Q}(\sqrt{q\theta})$ is $(1^2)^4$ or $(2^2)^2$. In both cases the ramification is tame and the inertia subgroup is $\{\pm 1\}$. Since $\operatorname{tr} \rho(-1) = \chi(-1) = -2$ we find that the local Artin conductor at p is equal to 2.

The prime 2 can either be unramified in which case $\alpha = 0$, or have the same splitting pattern as above in which case the prime 2 is wildly ramified and $\alpha = 4$.

The primes dividing ab, which all have tame ramification, can in addition have splitting type $(1^4)^2$ in which case the inertia has order four. Since $\chi(i) = \chi(j) = \chi(k) = 0$ the Artin conductor is again equal to 2. □

The family $\mathfrak{F}$ can be interpreted as a geometric family in the following way. We consider the binary quadratic form $x^2 - q\theta y^2$ over $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ and construct the zero locus $x^2 - q\theta y^2 = 0$ inside $\mathbb{A}^1 \times \mathbb{P}^1$. Applying restriction and extension of scalars from $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ to $\mathbb{Q}$, we obtain a branched covering $X \to \mathbb{A}^1$ of degree eight defined over $\mathbb{Q}$. Our family $\mathfrak{F}$ is constructed from the covering $X \to \mathbb{A}^1$ in the same way as the families and coverings are constructed in Section 2.

The action of $\mathrm{Gal}(\mathbb{Q})$ on $K_q = \mathbb{Q}(\sqrt{q\theta})$ splits into the disjoint actions on $\sqrt{q}$ and $\sqrt{\theta}$. It follows that the Artin representations $\rho_{K_q} : \mathrm{Gal}(\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ differ by quadratic twists, that is, by twisting by the 1-dimensional representations $\mathrm{Gal}(\mathbb{Q}) \to \{\pm 1\}$ attached to the quadratic Dirichlet characters χ_q of discriminant q.

We order elements in $\mathfrak{F}$ by conductor, so $h(K) = C_K$. Let $\mathfrak{F}(x)$ denote the set of elements in $\mathfrak{F}$ with conductor less than x. Let $\mathcal{L} = \mathcal{L}(x)$ be defined by

$$\mathcal{L} := \frac{1}{|\mathfrak{F}(x)|} \sum_{K \in \mathfrak{F}(x)} \log C_K. \tag{42}$$

We write $M = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Before stating the theorem on low-lying zeros, we collect the information on splitting behavior of unramified primes in K and M discussed above, along with the corresponding densities in the family $\mathfrak{F}$.

Table 4. Densities of splitting types in $\mathfrak{F}$.

Splitting type in K	Splitting type in M	Average Density in $\mathfrak{F}$
$(1)^8$	$(1)^4$	$\frac{\delta_M(p)}{2}$
$(2)^4$	$(1)^4$	$\frac{\delta_M(p)}{2}$
$(4)^2$	$(2)^2$	$1-\delta_M(p)$

If a prime p has splitting type $(2)^2$ in M, then it must have splitting type $(4)^2$ in K. Otherwise, if p has splitting type $(1)^4$ in M, then its splitting type in $K=\mathbb{Q}(\sqrt{q\theta})$ is determined by whether or not q is a square in $\mathbb{Q}_p$. Hence in this case, the splitting types $(1)^8$ and $(2)^4$ happen equally often for fields $K\in\mathfrak{F}(x)$ as $x\to\infty$. We collect the average densities of splitting types in Table 4, where $\delta_M(p)=1$, respectively 0, if p splits in M, respectively does not split in M.

The Sato–Tate group of $\mathfrak{F}$ is $Q\subset\mathrm{GL}_2(\mathbb{C})$ embedded via the 2-dimensional representation ρ. As before in Sections 2.3 and 6.2, we identify $\mathbb{T}$ with $(S^1)^2$ modulo permutation of the coordinates. Then the Sato–Tate measure equals

$$\mu_{\mathrm{ST}}(\mathfrak{F})=\tfrac{1}{8}\delta(1,1)+\tfrac{1}{8}\delta(-1,-1)+\tfrac{3}{4}\delta(i,-i),$$

and the corresponding indicators are $i_1(\mathfrak{F})=1$, $i_2(\mathfrak{F})=1$ and $i_3(\mathfrak{F})=-1$. In particular it follows that the family $\mathfrak{F}$ is homogeneous symplectic.

Theorem 8.6. *Let $\mathfrak{F}$ be the one-parameter family of quaternionic fields described above. If f is an even function whose Fourier transform is smooth and supported in the interval $[-\alpha,\alpha]$ for $\alpha<\frac{4}{11}$, then*

$$\lim_{x\to\infty}\frac{1}{|\mathfrak{F}(x)|}\sum_{K\in\mathfrak{F}(x)}\sum_j f\left(\frac{\gamma_K^{(j)}\mathcal{L}}{2\pi}\right)=\widehat{f}(0)+\frac{f(0)}{2}.$$

Proof. As before, we can without loss of generality assume that f is even. Recalling (16), (17) and the fact that the L-functions $L(s,\rho_K)$ are entire, we write

$$\frac{1}{|\mathfrak{F}(x)|}\sum_{K\in\mathfrak{F}(x)}\sum_j f\left(\frac{\gamma_K^{(j)}\mathcal{L}}{2\pi}\right)=\widehat{f}(0)+o(1)-(\mathcal{S}_1+\mathcal{S}_2+\mathcal{S}_3+\mathcal{S}_{\mathrm{ram}}),$$

where the $\mathcal{S}_i$ are defined exactly as in (19).

In what follows, we will find it convenient to denote the splitting type of a prime p in the field K (respectively M) by $\sigma_K(p)$ (respectively $\sigma_M(p)$). To evaluate $\mathcal{S}_1$, note that the primes p that have splitting type $(2)^2$ in $\mathbb{Q}(\sqrt{a},\sqrt{b})$ do not contribute to the sum over primes because $\theta_K(p)=0$ for all such primes. Thus, we may restrict our sum to primes that split in $\mathbb{Q}(\sqrt{a},\sqrt{b})$, yielding

$$\begin{aligned}\mathcal{S}_1&=\frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{\substack{p\\ \sigma_M(p)=(1)^4}}\frac{\log p}{\sqrt{p}}\widehat{f}\left(\frac{\log p}{\mathcal{L}}\right)\sum_{K\in\mathfrak{F}^{p\nmid\Delta}(x)}\theta_K(p)\\&=\frac{2}{\mathcal{L}|\mathfrak{F}(x)|}\sum_{\substack{p\\ \sigma_M(p)=(1)^4}}\frac{\log p}{\sqrt{p}}\widehat{f}\left(\frac{\log p}{\mathcal{L}}\right)\left(\sum_{\substack{K\in\mathfrak{F}^{p\nmid\Delta}(x)\\ \sigma_K(p)=(1)^8}}2-\sum_{\substack{K\in\mathfrak{F}^{p\nmid\Delta}(x)\\ \sigma_K(p)=(2)^4}}2\right).\end{aligned}$$

Let p be a prime that splits in $\mathbb{Q}(\sqrt{a},\sqrt{b})$. We claim that the splitting type of p in the quaternionic field K_q corresponding to the parameter q depends only on whether or not q is a quadratic residue modulo p. Indeed, by assumption, we have $\mathbb{Q}(\sqrt{a},\sqrt{b})\otimes\mathbb{Q}_p=\mathbb{Q}_p^4$. So the splitting type of p in $K_q=\mathbb{Q}(\sqrt{q\theta})$ depends only on whether or not $q\theta$ is a square in $\mathbb{Q}_p$. The claim now follows since θ is fixed. Therefore, using the Burgess bound as in [53, Lemma 2.3], we have

$$\#\{K\in\mathfrak{F}^{p\nmid\Delta}(x):\sigma_K(p)=(1)^8\}=\frac{p-1}{2p}|\mathfrak{F}^{p\nmid\Delta}(x)|+O_\epsilon(x^{1/4}(\log x)p^{3/16+\epsilon}),$$
$$\#\{K\in\mathfrak{F}^{p\nmid\Delta}(x):\sigma_K(p)=(2)^4\}=\frac{p-1}{2p}|\mathfrak{F}^{p\nmid\Delta}(x)|+O_\epsilon(x^{1/4}(\log x)p^{3/16+\epsilon}).$$

Hence

$$\mathcal{S}_1=O_\epsilon\left(\frac{\log x}{x^{1/4}}\sum_{\log p\leqslant\mathcal{L}\alpha}\frac{1}{p^{5/16-\epsilon}}\right)=O_\epsilon\left(\frac{e^{(11/16+\epsilon)\mathcal{L}\alpha}}{x^{1/4}}\right).$$

To estimate $\mathcal{S}_2$, we note that $\theta_K(p^2)$ is 2 or -2 depending on whether the splitting type of p in $\mathbb{Q}(\sqrt{a},\sqrt{b})$ is $(1)^4$ or $(2)^2$, respectively. That is, $\theta_K(p^2)$ is independent of K and only depends on the splitting type of p in M. Set $\tau_M(p)$ to be 0 if p ramifies in M, 1 if $\sigma_M(p)=(1)^4$, and -1 if $\sigma_M(p)=(2)^2$. Then we have

$$\begin{aligned}\mathcal{S}_2&=\frac{4}{\mathcal{L}|\mathfrak{F}(x)|}\sum_p\tau_M(p)\frac{\log p}{p}\widehat{f}\left(\frac{2\log p}{\mathcal{L}}\right)|\mathfrak{F}^{p\nmid\Delta}(x)|\\&=\frac{4}{\mathcal{L}|\mathfrak{F}(x)|}\sum_p\tau_M(p)\frac{\log p}{p}\widehat{f}\left(\frac{2\log p}{\mathcal{L}}\right)|\mathfrak{F}(x)|(1+O(p^{-1}))\\&=\frac{4}{\mathcal{L}}\sum_p\tau_M(p)\frac{\log p}{p}\widehat{f}\left(\frac{2\log p}{\mathcal{L}}\right)+o(1).\end{aligned}$$

Hence, by the Chebotarev density theorem applied to M, or simply because $\tau_M(p)$ is determined by the quadratic residue symbols (a/p) and (b/p), we obtain

$$\mathcal{S}_2 = -\frac{f(0)}{2} + o(1),$$

from an argument identical to the one yielding (23).

Finally, bounding the quantities $\mathcal{S}_3$ and $\mathcal{S}_{\mathrm{ram}}$ in exactly the same way as in (21), we find that

$$\mathcal{S}_3 = o(1),$$
$$\mathcal{S}_{\mathrm{ram}} = o(1).$$

We conclude that

$$\frac{1}{|\mathfrak{F}(x)|}\sum_{K\in\mathfrak{F}(x)}\sum_j f\left(\frac{\gamma_K^{(j)}\mathcal{L}}{2\pi}\right) = \widehat{f}(0) + \frac{f(0)}{2} + O_\epsilon\left(\frac{e^{(11/16+\epsilon)\mathcal{L}\alpha}}{x^{1/4}}\right) + o(1),$$

from which the desired result readily follows. □

Let us remark that the condition $\alpha < \frac{4}{11}$ on the support in Theorem 8.6 can be relaxed. In fact, it follows from a result of Rubinstein [59] on more general families of quadratic twists that Theorem 8.6 holds with any $\alpha < \frac{1}{2}$. Rubinstein uses a large sieve type inequality due to Jutila instead of the Burgess bound to obtain this result. Furthermore, Katz and Sarnak [43, Appendix 1 (unpublished)] proved, assuming GRH, that the above result holds also in the doubled region $\alpha < 1$. For any integer $n \geqslant 1$, [59] further establishes the n-level density for test functions with support restricted to the region $\sum_{i=1}^n |x_i| < 1/m$ of low-lying zeros of families consisting of quadratic twists of a fixed automorphic cuspidal representation of $\mathrm{GL}_m(\mathbb{Q})$. It would be interesting to see if, similarly as done in [32] in the case $m = 1$, one could double the support (conditional on GRH) in the n-level result for the family $\mathfrak{F}$ considered in this section.

Proposition 8.7. *The root number of the Artin representation attached to $\mathbb{Q}(\sqrt{q\theta})$ is independent of q.*

Proof. See Fröhlich [36, Assertion XV]. We give here a proof based on the properties of local epsilon factors in [69]. Let ρ be the Artin representation attached to $\mathbb{Q}(\sqrt{\theta})$ and χ_q be the quadratic Dirichlet character attached to q. We want to prove that $\epsilon(\rho\otimes\chi_q) = \epsilon(\rho)$.

Fix the standard additive character ψ of $\mathbb{Q}\backslash\mathbb{A}$. Then the epsilon factor splits as a product of local epsilon factors $\epsilon_p(\rho\otimes\chi_q, \psi)$. We will verify that for every prime p, we have

$$\epsilon_p(\rho \otimes \chi_q, \psi) = \epsilon_p(\rho, \psi)\epsilon_p(\chi_q, \psi)^2.$$

Since globally $\epsilon(\chi_q) = 1$ this will finish the proof.

For $p = \infty$ this can be verified directly. For $p \nmid 2abq$ each epsilon factor is equal to one. For $p \mid ab$, we have $p \nmid q$ by assumption. Thus $\epsilon_p(\rho \otimes \chi_q, \psi) = \epsilon_p(\rho, \psi)\chi_q(p^{v_p(r(ab)^2)}) = \epsilon_p(\rho, \psi)$, where we have used (Lemma 8.5) that the conductor of ρ is equal to $2^\alpha r(ab)^2$ which is a perfect square. For $p \mid 2q$, we have $p \nmid ab$ by assumption. Since $\det \rho$ is trivial because ρ has image in $\mathrm{SL}_2(\mathbb{C})$, we find that $\epsilon_p(\rho \otimes \chi_q, \psi) = \epsilon_p(\chi_q, \psi)^2$. This concludes the claim. □

Acknowledgements

We thank Manjul Bhargava, Peter Sarnak and Jacob Tsimerman for many helpful discussions and Melanie Wood for comments and for sending us [31]. We thank the referee for a careful reading and helpful suggestions. Most of this work was done while the authors were at Princeton and it is a pleasure to thank the IAS for providing excellent working conditions. We also enjoyed the hospitality of Harvard University, Boston College, and Carleton University. The first author was partially supported by NSF grant DMS-1128155. The second author was supported by NSF grant DMS-1128155, and by a grant from the Danish Council for Independent Research and FP7 Marie Curie Actions-COFUND (grant id: DFF-1325-00058). The third author was supported by NSF grant DMS-1200684.

References

[1] J. V. Armitage, 'Zeta functions with a zero at $s = \frac{1}{2}$', *Invent. Math.* **15** (1972), 199–205.

[2] A. Ash, J. Brakenhoff and T. Zarrabi, 'Equality of polynomial and field discriminants', *Exp. Math.* **16**(3) (2007), 367–374.

[3] A. M. Baily, 'On the density of discriminants of quartic fields', *J. Reine Angew. Math.* **315** (1980), 190–210.

[4] K. Belabas, M. Bhargava and C. Pomerance, 'Error estimates for the Davenport-Heilbronn theorems', *Duke Math. J.* **153**(1) (2010), 173–210.

[5] M. Bhargava, 'Higher composition laws III: the parametrization of quartic rings', *Ann. of Math. (2)* **159**(3) (2004), 1329–1360.

[6] M. Bhargava, 'Higher composition laws IV: the parametrization of quintic rings', *Ann. of Math. (2)* **167**(1) (2008), 53–94.

[7] M. Bhargava, 'The density of discriminants of quartic rings and fields', *Ann. of Math. (2)* **162**(2) (2005), 1031–1063.

[8] M. Bhargava, 'The density of discriminants of quintic rings and fields', *Ann. of Math. (2)* **172**(3) (2010), 1559–1591.

[9] M. Bhargava, ‘Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants’, *Int. Math. Res. Not. IMRN* (2007), no. 17, Art. ID rnm052, 20 pp.

[10] M. Bhargava, A. Shankar and J. Tsimerman, ‘On the Davenport-Heilbronn theorems and second order terms’, *Invent. Math.* **193**(2) (2013), 439–499.

[11] M. Bhargava, A. Shankar and X. Wang, ‘Squarefree values of polynomial discriminants I’, Preprint, 2016, arXiv:1611.09806.

[12] M. Bhargava, A. Shankar and X. Wang, ‘Geometry-of-numbers methods over global fields I: prehomogeneous vector spaces’, Preprint, 2015, arXiv:1512.03035.

[13] B. J. Birch and J. R. Merriman, ‘Finiteness theorems for binary forms with given discriminant’, *Proc. Lond. Math. Soc. (3)* **24** (1972), 385–394.

[14] A. R. Booker and A. Strömbergsson, ‘Numerical computations with the trace formula and the Selberg eigenvalue conjecture’, *J. Reine Angew. Math.* **607** (2007), 113–161.

[15] D. Buchsbaum and D. Eisenbud, ‘Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3’, *Amer. J. Math.* **99**(3) (1977), 447–485.

[16] F. Calegari, ‘The Artin conjecture for some S_5-extensions’, *Math. Ann.* **356**(1) (2013), 191–207.

[17] J. W. S. Cassels, *Rational Quadratic Forms*, London Mathematical Society Monographs, 13 (Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London–New York, 1978), pp. xvi+413.

[18] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, (Academic Press, London–New York, 1967).

[19] P. J. Cho and H. H. Kim, ‘Low lying zeros of Artin L-functions’, *Math. Z.* **279**(3–4) (2015), 669–688.

[20] P. J. Cho and H. H. Kim, ‘n-level densities of Artin L-functions’, *Int. Math. Res. Not. IMRN* (17) (2015), 7861–7883.

[21] H. Cohen, F. Diaz y Diaz and M. Olivier, ‘Enumerating Quartic Dihedral Extensions of $\mathbb{Q}$’, *Compos. Math.* **133**(1) (2002), 65–93.

[22] J. B. Conrey and K. Soundararajan, ‘Real zeros of quadratic Dirichlet L-functions’, *Invent. Math.* **150**(1) (2002), 1–44.

[23] C. W. Curtis, *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer*, History of Mathematics, 15 (American Mathematical Society, Providence, RI, 1999).

[24] H. Davenport and H. Heilbronn, ‘On the density of discriminants of cubic fields II’, *Proc. R. Soc. Lond. Ser. A* **322**(1551) (1971), 405–420.

[25] C. David, J. Fearnley and H. Kisilevsky, ‘On the vanishing of twisted L-functions of elliptic curves’, *Experiment. Math.* **13**(2) (2004), 185–198.

[26] R. Dedekind, ‘Konstruktion von Quaternionkörpern’, in *Gesammelte mathematische Werke, Bd. 2* (Vieweg & Sohn, Braunschweig, 1931), 376–384.

[27] P. Deligne, *SGA* $4\frac{1}{2}$*—Cohomologie étale*, Lecture Notes in Mathematics, 569 (Springer, New York, 1977).

[28] B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Translations of Mathematical Monographs, 10 (American Mathematical Society, Providence, RI, 1964).

[29] A.-W. Deng, ‘Rational points on weighted projective spaces’, Preprint, 1998, arXiv:9812082.

[30] R. Dietmann, ‘On the distribution of Galois groups’, *Mathematika* **58**(1) (2012), 35–44.

[31] J. Ellenberg, L. B. Pierce and M. M. Wood, ‘On ℓ-torsion in class groups of number fields’, *Algebra Number Theory* **11**(8) (2017), 1739–1778.

[32] A. Entin, E. Roditty-Gershon and Z. Rudnick, ‘Low-lying zeros of quadratic Dirichlet L-functions, hyper-elliptic curves and random matrix theory’, *Geom. Funct. Anal.* **23**(4) (2013), 1230–1261.

[33] D. Fiorilli, J. Parks and A. Södergren, ‘Low-lying zeros of elliptic curve L-functions: beyond the ratios conjecture’, *Math. Proc. Cambridge Philos. Soc.* **160**(2) (2016), 315–351.

[34] É. Fouvry, F. Luca, F. Pappalardi and I. E. Shparlinski, ‘Counting dihedral and quaternionic extensions’, *Trans. Amer. Math. Soc.* **363**(6) (2011), 3233–3253.

[35] G. Frobenius and I. Schur, ‘Über die reellen Darstellungen der endlichen Gruppen’, *Sitzungsber, Preuss, Akad. d* (1906), 186–208.

[36] A. Fröhlich, ‘Artin root numbers and normal integral bases for quaternion fields’, *Invent. Math.* **17**(2) (1972), 143–166.

[37] A. Fröhlich and J. Queyrut, ‘On the functional equation of the Artin L-function for characters of real representations’, *Invent. Math.* **20** (1973), 125–138.

[38] W. T. Gan, B. Gross and G. Savin, ‘Fourier coefficients of modular forms on G_2’, *Duke Math. J.* **115**(1) (2002), 105–169.

[39] H. Heilbronn, ‘On the 2-classgroup of cubic fields’, in *Studies in Pure Mathematics (Presented to Richard Rado)* (Academic Press, London, 1971), 117–119.

[40] H. Iwaniec, ‘Conversations on the exceptional character’, in *Analytic Number Theory*, Lecture Notes in Mathematics, 1891 (Springer, Berlin, 2006), 97–132.

[41] C. U. Jensen and N. Yui, ‘Quaternion extensions’, in *Algebraic Geometry and Commutative Algebra, Vol. I* (Kinokuniya, Tokyo, 1988), 155–182.

[42] N. M. Katz, ‘Sato–Tate in the higher dimensional case: elaboration of 9.5.4 in Serre’s $N_X(p)$ book’, *Enseign. Math.* **59**(3–4) (2013), 359–377.

[43] N. M. Katz and P. Sarnak, ‘Zeroes of zeta functions and symmetry’, *Bull. Amer. Math. Soc. (N.S.)* **36**(1) (1999), 1–26.

[44] K. S. Kedlaya, ‘Mass formulas for local Galois representations’, *Int. Math. Res. Not. IMRN* (17) (2007), Art. ID rnm021, 26 pp.

[45] I. Kiming, ‘Explicit classification of some 2-extensions of a field of characteristic different from 2’, *Canad. J. Math.* **42**(5) (1990), 825–855.

[46] J. Klüners, ‘Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe’, Habilitationsschrift, Universität Kassel, 2005.

[47] E. Kowalski, ‘Families of cusp forms’, in *Actes de la Conférence ‘Théorie des Nombres et Applications’*, Publ. Math. Besançon Algèbre Théorie Nr. (Presses Univ. Franche-Comté, Besançon, 2013), 5–40.

[48] J. C. Lagarias and B. L. Weiss, ‘Splitting behavior of S_n-polynomials’, *Res. Number Theory* **1** (2015), Art. 7, 30 pp.

[49] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, Mathematics Lecture Note Series (Benjamin/Cummings Publishing Co., Inc., Advanced Book Program, Reading, MA, 1980).

[50] R. J. Lemke Oliver and F. Thorne, ‘The number of ramified primes in number fields of small degree’, *Proc. Amer. Math. Soc.* **145**(8) (2017), 3201–3210.

[51] F. Levi, ‘Kubische Zahlkörper und binäre kubische Formenklassen’, *Ber. Sächs. Akad. Wiss. Leipzig, Math.-Naturwiss* **66** (1914), 26–37.

[52] I. G. Macdonald, *Symmetric Functions and Orthogonal Polynomials*, University Lecture Series, 12 (American Mathematical Society, Providence, RI, 1998).

[53] M. Munsch, ‘Character sums over squarefree and squarefull numbers’, *Arch. Math. (Basel)* **102**(6) (2014), 555–563.

[54] J. Nakagawa, ‘Binary forms and orders of algebraic number fields’, *Invent. Math.* **97**(2) (1989), 219–235.

[55] J. Neukirch, *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften, 280 (Springer, Berlin, 1986).

[56] R. Perlis, 'On the equation $\zeta_K(s) = \zeta_{K'}(s)$', *J. Number Theory* **9**(3) (1977), 342–360.

[57] E. Peyre, 'Hauteurs et mesures de Tamagawa sur les variétés de Fano', *Duke Math. J.* **79**(1) (1995), 101–218.

[58] H. Reichardt, 'Über Normalkörper mit Quaternionengruppe', *Math. Z.* **41**(1) (1936), 218–221.

[59] M. Rubinstein, 'Low-lying zeros of L-functions and random matrix theory', *Duke Math. J.* **109**(1) (2001), 147–181.

[60] Z. Rudnick and P. Sarnak, 'Zeros of principal L-functions and random matrix theory', *Duke Math. J.* **81**(2) (1996), 269–322.

[61] P. Sarnak, S. W. Shin and N. Templier, 'Families of L-functions and their symmetry', in *Proceedings of Simons Symposia, Families of Automorphic Forms and the Trace Formula* (Springer Verlag, 2016), 531–578.

[62] M. Sato and T. Kimura, 'A classification of irreducible prehomogeneous vector spaces and their relative invariants', *Nagoya Math. J.* **65** (1977), 1–155.

[63] J.-P. Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, 11 (CRC Press, Boca Raton, FL, 2012).

[64] A. Shankar and J. Tsimerman, 'Counting S_5-fields with a power saving error term', *Forum Math. Sigma* **2** (2014), e13 (8 pages).

[65] S. W. Shin and N. Templier, 'Sato–Tate theorem for families and low-lying zeros of automorphic L-functions', *Invent. Math.* **203**(1) (2016), 1–177.

[66] C. L. Siegel, 'The average measure of quadratic forms with given determinant and signature', *Ann. of Math. (2)* **45** (1944), 667–685.

[67] K. Soundararajan, 'Nonvanishing of quadratic Dirichlet L-functions at $s = \frac{1}{2}$', *Ann. of Math. (2)* **152**(2) (2000), 447–488.

[68] T. Taniguchi and F. Thorne, 'Secondary terms in counting functions for cubic fields', *Duke Math. J.* **162**(13) (2013), 2451–2508.

[69] J. Tate, 'Number theoretic background', in *Automorphic Forms, Representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proceedings of Symposia in Pure Mathematics, XXXIII (American Mathematical Society, Providence, RI, 1979), 3–26.

[70] O. Taussky, 'Pairs of sums of three squares of integers whose product has the same property', in *General Inequalities 2 (Proc. Second Internat. Conf., Oberwolfach, 1978)* (Birkhäuser, Basel–Boston, MA, 1980), 29–36.

[71] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, 800 (Springer, Berlin, 1980).

[72] K. H. Wilson, 'Three perspectives on n points in $\mathbb{P}^{n-2}$', PhD Thesis, Princeton University, 2012.

[73] E. Witt, 'Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordung p^f', *J. Reine Angew. Math.* **174** (1936), 237–245.

[74] M. M. Wood, 'Moduli spaces for rings and ideals', PhD Thesis, Princeton University, June 2009.

[75] M. M. Wood, 'Mass formulas for local Galois representations to wreath products and cross products', *Algebra Number Theory* **4** (2008), 391–405.

[76] M. M. Wood, 'Rings and ideals parameterized by binary n-ic forms', *J. Lond. Math. Soc. (2)* **83**(1) (2011), 208–231.

[77] M. M. Wood, 'How to determine the splitting type of a prime, unpublished note', available at http://www.math.wisc.edu/∼mmwood/Splitting.pdf.

[78] D. J. Wright and A. Yukie, 'Prehomogeneous vector spaces and field extensions', *Invent. Math.* **110**(2) (1992), 283–314.

[79] A. Yang, 'Distribution problems associated to zeta functions and invariant theory', PhD Thesis, Princeton University, 2009.