JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Erik HOLMES

On the shapes of pure prime-degree number fields

Tome 37, nº 1 (2025), p. 1-48.
https://doi.org/10.5802/jtnb.1311

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **37** (2025), 1–48

On the shapes of pure prime-degree number fields

par Erik HOLMES

Résumé. Pour un nombre premier p et $\ell = \frac{p-1}{2}$, nous montrons que la *shape* (forme) d'un corps de nombres pur de degré premier appartient à l'un de deux sous-espaces de dimension ℓ de l'espace des formes, selon que p est sauvagement ramifié ou non. Lorsque ces corps sont ordonnés par leur discriminant absolu, nous démontrons que les formes sont équidistribuées, au sens régularisé, sur ces sous-espaces. Nous montrons également que la forme constitue un invariant complet au sein de la famille des corps purs de degré premier. Ce travail généralise les résultats de Harron dans [15], qui étudie les formes dans le cas des corps cubiques purs. En outre, nous traduisons ces résultats en énoncés concernant les corps de Frobenius avec un corps résolvant fixé. Plus précisément, nous montrons que cette étude est équivalente à celle des corps de nombres de groupe de Galois $F_p = C_p \rtimes C_{p-1}$ et de corps résolvant fixé $\mathbb{Q}(\zeta_p)$.

Abstract. For p prime and $\ell = \frac{p-1}{2}$, we show that the shapes of pure prime degree number fields lie on one of two ℓ-dimensional subspaces of the space of shapes, and which of the two subspaces is dictated by whether or not p ramifies wildly. When the fields are ordered by absolute discriminant we show that the shapes are equidistributed, in a regularized sense, on these subspaces. We also show that the shape is a complete invariant within the family of pure prime degree fields. This extends the results of Harron, in [15], who studied shapes in the case of pure cubic number fields. Furthermore we translate the statements of pure prime degree number fields to statements about Frobenius number fields with a fixed resolvent field. Specifically we show that this study is equivalent to the study of F_p-number fields, $F_p = C_p \rtimes C_{p-1}$, with fixed resolvent field $\mathbb{Q}(\zeta_p)$.

1. Introduction

The shape of a number field is an Archimedean invariant of the field. Roughly speaking, the shape of a rank n lattice is the equivalence class of the lattice up to scaling, rotation, and reflection. Let K be a degree n number field and consider the Minkowksi embedding: $j_{\mathbf{R}}(\alpha) = K \to K \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{R}^n$ which, when restricted to an order in K, yields rank n lattice.

Manuscrit reçu le 10 février 2023, révisé le 26 janvier 2025, accepté le 24 février 2025.
2020 *Mathematics Subject Classification.* 11R21, 11R45, 11P21, 11E12.
Mots-clefs. Number fields, lattices, equidistribution, carefree tuples.
The author was partially supported by NSERC grant RGPIN-2018-03770 and CRC tier-2 research stipend 950-231716.

Since the ring of integers of K, denoted $\mathcal{O}_K$, always has a $\mathbf{Z}$ component we define the shape of K so as to capture the "new information" of the ring. That is, we define the shape of K to be the shape of $j(\mathcal{O}_K^{\perp})$ which is, the lattice of rank $n-1$, obtained by taking the projection of $j(\mathcal{O}_K)$ onto the hyperplane orthogonal to $j(1)$. The shape of K is therefore an element of the space of shapes of lattices of rank $(n-1)$:

$$\mathcal{S}_{n-1} := \mathrm{GL}_{n-1}(\mathbf{Z})\backslash \mathrm{GL}_{n-1}(\mathbf{R})/\mathrm{GO}_{n-1}(\mathbf{R})$$

and we can study the distribution of points in this space as we vary over natural families of number fields.

1.1. Motivation. In [24] Terr studied the shape in the case of cubic number fields where he showed that the shapes were equidistributed in the space of shapes of rank 2 lattices. This proves that the shapes are, in some sense, random when we consider all cubic number fields and this "randomness" result was later extended to quartic and quintic number fields by Manjul Bhargava and Piper H, in [5]. To achieve this generalization, the authors used Bhargava's parametrization of quartic and quintic rings given in [2, 4] to show that the shape of quartic and quintic number fields are equidistributed in the space of rank 3 and 4 lattices. The authors conjecture that the same equidistribution result should hold for $n > 5$ but, without a nice parametrization of such rings, this is where this line of work with generic fields stops. The authors do, however, mention the following:

> *"It is an interesting problem to determine the distribution of lattice shapes for n-ic number fields having a given non-generic (i.e., non-S_n) associated Galois group, even heuristically."*

The distribution of non-generic fields has witnessed a number of recent studies in families of field with low degree. We will list many of these studies in the next few sections, highlighting also the study of shape as an invariant of a number field. The purpose of this paper is to generalize the results of Harron on the shapes of pure cubic fields, in [15], to all pure prime degree fields.

1.2. Our results. In this paper we study the shapes, and distribution, of pure prime degree number fields: that is, number fields obtained by adjoining a root of the *pure prime degree polynomial* $f(x) = x^p - m$, with m p-th power free. In this short section we state our results, how they compare to those in [15], and in the following sections we discuss how these results fit into the recent work in this area.

Let $\mathcal{S}_{p-1}$ denote the space of shapes of rank $(p-1)$-lattices, and $\ell = \frac{p-1}{2}$. Our first result shows that the shape of pure prime degree fields lie on one of two ℓ-dimensional subspaces of $\mathcal{S}_{p-1}$, depending on the ramification of p in the field (wild vs tame). We will, as in [15], denote those pure

prime degree fields where p is wildly (resp. tamely) ramified by Type I (resp. Type II). The following theorem shows that the shape of Type I fields are orthorhombic lattices and the shape of Type II fields are, what we refer to as ordinary lattices[1]. To state this result we interpret the space of orthorhombic lattices coming from Type I fields as lying on an orbit of the diagonal torus $\mathcal{T} \subseteq \mathrm{SL}_{p-1}(\mathbf{R})$. Letting $\mathcal{G}_{wild}(\mathbf{1})$ be the Gram matrix of the "square" lattice, represented by the $(p-1) \times (p-1)$ identity matrix, we define $\mathscr{S}_I$ to be the orbit of $\mathcal{G}_{wild}(\mathbf{1})$, under the action of the torus $\mathcal{T}$. For Type II fields things are less uniform: we define the space $\mathscr{S}_{II}$ to be an ℓ-dimensional subspace of ordinary lattices: see Remark 5.2 for more on this. Then we have the following:

Theorem A (Space of shapes)**.** *The shape of a pure prime degree field K, denoted* $\mathrm{sh}(K)$*, lies on one of two ℓ-dimensional subspaces of $\mathcal{S}_{p-1}$:*

- *If K is of Type I then* $\mathrm{sh}(K) \in \mathscr{S}_I$*; i.e. the shape of Type I fields are orthorhombic.*
- *If K is tamely ramified then* $\mathrm{sh}(K) \in \mathscr{S}_{II}$*; i.e. the shape of Type II fields are* ordinary *lattices as in* [24].

When $p = 3$ we are studying the shape of certain rank 2 lattices which are represented by points in the upper half plane modulo the action of $\mathrm{GL}_2(\mathbf{Z})$, see Figure 3.1 for a visualization of this space. Define two subspaces of $\mathcal{S}_2$ by $\mathscr{S}_I(3) = \{z \in \mathcal{S}_2 : \mathrm{Re}(z) = 0\}$ and $\mathscr{S}_{II}(3) = \{z \in \mathcal{S}_2 : \mathrm{Re}(z) = \frac{1}{3}\}$. A result of Harron then shows

Theorem a ([15], Space of shapes)**.** *The shape of a pure cubic number field lies on one of two vertical geodesics in $\mathcal{S}_2$:*

- *If K is of Type I then the shape of K lies on $\mathscr{S}_I(3)$; i.e. the shapes of Type I fields are rectangular.*
- *If K is of Type II then the shape of K lies on $\mathscr{S}_{II}(3)$; i.e. the shapes of Type II fields are parallelograms with no extra symmetry, or* ordinary *lattices.*

To compare Harron's result with the generalization we note that $\mathscr{S}_I(3)$ can be described as the orbit of $y = i$ under the action of the torus:

$$\mathcal{T} = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}.$$

Our second result concerns the invariance of shapes and shows that the shape is a complete invariant within the family of all pure, prime degree, number fields.

Theorem B (Invariance of shape)**.** *Given K and L, two pure prime degree number fields, we have that $K \cong L$ if and only if* $\mathrm{sh}(K) = \mathrm{sh}(L)$.

[1] In [24], ordinary lattices are those lying in the interior of $\mathcal{S}_2$, as opposed to rectangular (orthorhombic) lattices which lie on the border.

Remark 1.1. Harron proved this in the case of pure cubic fields however he also showed that more is true in this case: combining the results of [15] and [16], he showed that the shape is a complete invariant within the family of all complex cubic fields. Our generalization shows that the complete invariance of shape holds within the family of pure prime degree fields but this is just one step towards a potentially stronger statement which is the subject of future research.

The third statement of the paper concerns the distribution of shapes: in particular we prove that the shapes are equidistributed (in a regularized sense) along $\mathscr{S}_I$ (resp. $\mathscr{S}_{II}$) with respect to a natural measure in this context μ_I (resp. μ_{II}), which is defined in Section 5.1. For q prime, let δ_q be a q-adic density:

$$\delta_q = \left(1 + \frac{p-1}{q}\right)\left(1 - \frac{1}{q}\right)^{p-1}$$

and define constants:

$$C_I := \frac{2p-2}{2^\ell(\ell-1)!(2p-1)(p-1)^{\ell-1}p^{1+\frac{1}{p-1}}}\prod_q \delta_q$$

$$C_{II} := \frac{1}{2^\ell(\ell-1)!(2p-1)(p-1)^{\ell-1}p^{1-\frac{1}{p-1}}}\prod_q \delta_q.$$

Theorem C. *Using the constants defined above we have the following:*

$$\lim_{X\to\infty} \frac{N_I(X,W)}{C_I X^{1/p-1}\log(X)^{\ell-1}} = \mu_I(W)$$

and

$$\lim_{X\to\infty} \frac{N_{II}(X,W)}{C_{II} X^{1/p-1}\log(X)^{\ell-1}} = \mu_{II}(W)$$

where $N_I(X,W)$ (resp. $N_{II}(X,W)$) denotes the number of wildly ramified (resp. tamely ramified) pure prime degree number fields with discriminant bounded by X and shape in W.

This shows that the shapes of Type I (resp. Type II) fields are equidistributed, in a regularized sense, along $\mathscr{S}_I$ (resp. $\mathscr{S}_{II}$). Letting $p = 3$ we recover the main result of Harron's pure cubic paper:

Theorem c ([15], regularized equidistribution)**.** *Define constants:*

$$C_I = \frac{2C}{15\sqrt{3}} \text{ and } C_{II} = \frac{C}{10\sqrt{3}}$$

where

$$C = \prod_q \left(1 - \frac{3}{q^2} + \frac{2}{q^3}\right)$$

and the product is over all primes q. For $? = I$, resp. II, and real numbers $1 \leq R_1 < R_2$, let $[R_1, R_2)_?$ denote the "interval" $i[R_1, R_2)$, resp. $(1 + i[R_1, R_2))/3$ in $\mathscr{S}_?$. Then, for all R_1, R_2

$$\lim_{X\to\infty} \frac{\#\{K \text{ of type } ? : |\Delta(K)| \leq X, \mathrm{sh}(K) \in [R_1, R_2)_?\}}{C_? \sqrt{X}} = \int_{[R_1,R_2)_?} \mathrm{d}\mu_?$$

where $\Delta(K)$ is the discriminant of K, and $\mathrm{sh}(K)$ is the shape of K.

Remark 1.2. The regularized equidistribution statement in Theorem C is the higher dimensional analogue of Theorem c. The usual statement of equidistribution would have, as a denominator, the number of pure prime degree fields with absolute discriminant bound but Benli, in [1], shows that this quantity has more log terms and would therefore send the limit to 0. The reader can compare this result to those in [14, 15, 18]: in each there is at least one parameter in the space of shapes that is unrestricted and we can think of these as having infinite length. In [15] this is seen clearly as the geodesics that the shapes lie on are vertical. In this paper we sample shapes in some compact subset of the space which yields logarithmic terms containing shape conditions and not the discriminant bound. Incorporating the shape conditions into the asymptotics error term would be an interesting avenue to explore as it seems that the field asymptotic can be recovered in at least some cases: we discuss this in a bit more detail in Section 1.5.

Theorems A, B and C extend the results of [15] to all pure prime degree number fields. Our final result allows us to interpret this study in terms of Galois conditions and resolvent fields:

Theorem D. *K is a pure prime degree number field if, and only if, $\mathrm{Gal}(\widetilde{K}/\mathbf{Q}) \cong F_p = C_p \rtimes C_{p-1}$ and K has (degree $p-1$) cyclotomic resolvent field $\mathbf{Q}(\zeta_p)$.*

This result is widely known in the cubic case where the statement is that pure cubics are exactly those ($S_3 \cong F_3$) cubic fields whose quadratic resolvent is $\mathbf{Q}(\zeta_3)$: for a proof in the cubic case see Lemma 33 of [7]. We prove the generalization which not only allows us to phrase things in a manner more similar to the work being done in arithmetic statistics, but also motivates other questions which the author plans to answer in future work, see Section 7 for more on this.

In the remaining sections of the introduction we attempt to motivate our results by describing how they fit into the recent work in this area.

1.3. The strength of invariance. It is well known that the discriminant is a complete invariant of a number field of degree d if, and only if, $d = 2$. As the shape is closely related to the discriminant it is natural to ask whether the extra information it contains makes it a stronger invariant or not.

Terr, in [24], proved that cyclic cubic fields all have the same (hexagonal) shape! It seems that the extra symmetries of the field, which are inherited by the shape, can cause too much collision for the shape to be a strong invariant so what else do we know?

Remark 1.3. The study of shapes as invariants has been addressed in a few recent papers and continues to be an active area of study. We compiled a short list of some recent results in this direction.

- Guillermo Mantila-Soler and Marina Monsurrò, in [22], study the shape of cyclic number fields of prime degree and show that the shape is no more powerful an invariant than the discriminant.
- William Bolaños and Guillermo Mantila-Soler, in [8], extend the work above, [22], to study the shape of cyclic degree n number fields and show that, again, the shape of K gives you nothing more than the discriminant of the number field. As such, the shape (or trace form in their work), is far from a complete invariant of K in the case of cyclic number fields.
- In contrast to the aforementioned work, Rob Harron has shown, in [15] and [16], that the shape is a complete invariant of pure cubic fields and, more generally, of complex cubic fields (just as the discriminant is in the case of quadratic fields). This shows that, given two such number fields K_1 and K_2, $K_1 \cong K_2 \iff \mathrm{sh}(K_1) = \mathrm{sh}(K_2)$. Where we say $\mathrm{sh}(K)$ to mean the shape of the field K.
- Piper H and Rob Harron, in [14], show that if we restrict to certain families of V_4 quartics, that the shape again determines the field.

These results show that the shape can be a very powerful invariant in some cases, and a very weak invariant in others; we see that Galois fields, and specifically those with cyclic Galois group, with extra symmetries may force shapes to collide but in general much remains to completely classify the shape as an invariant. Theorem B provides, for each prime p, an infinite family of number fields for which the shape is a complete invariant.

One reason we care about this statement and the power of invariance is towards relating the study of shapes to the study of number field asymptotics. This is discussed in more detail in Section 1.5 but the quick idea is that by studying the distribution of shapes in prescribed families we can sometimes obtain the corresponding number fields asymptotics, or at least some information about the log terms in the asymptotics.

1.4. Distribution of shapes. As mentioned above Terr studied the question of non-generic distribution in the case of cyclic cubic number fields, where all fields have the same shape. This result is argued geometrically using the fact that there is only one point in the space of rank 2 lattices which admits an order 3 automorphism. Terr's results show how Galois

conditions impose strong restrictions on the shape of the field and where said shape lies: in one case (the generic, S_3, case) the shapes distribute randomly in the entire space of shapes of rank 2 lattices while the other case (the non-generic, C_3, case) yields a single point in the space of shapes. This should be somewhat intuitive based on the symmetries that the lattice inherits from the field but how this changes, when the space of shapes has higher dimension and the families that we consider are not cyclic, continues to be an intriguing question.

Remark 1.4. Here are a few of the recent studies of shape distributions.

- Rob Harron studied complex cubics, in [15] and [16], and showed that the shapes of these cubics lie, and are equidistributed, on geodesics defined by the quadratic resolvent of the cubic field. In the case of pure cubic fields the geodesics that the shapes lie on are vertical and have infinite length, whereas the non-pure complex cubics lie on geodesics of finite length. This witnesses the difference in the asymptotics of cubic fields with prescribed quadratic resolvents as is discussed in the following section.
- Piper H and Rob Harron study the shapes of Galois quartic extensions, in [14], showing that the shape of V_4 quartics are equidistributed along subspaces of the space of shapes, and that cyclic quartic fields are not. Specifically the cyclic quartic shapes distribute discretely along subspaces of the space of shapes and are therefore not equidistributed in any sense. The latter result can be compared with Terr's cyclic cubic result, though the higher dimensional space of shapes give more options for lattices with cyclic symmetry.
- Jamal Hassan, in [18], extended the V_4 result above by studying the shapes of octic multi-quadratic extensions and showing that the shapes are equidistributed along subspaces of the space of shapes.

multi-quadratic

Our current work extends the results in [15] to all pure prime degree number fields (i.e. fields of the form $K = \mathbf{Q}(\sqrt[p]{m})$). Specifically, Theorem C shows that the shapes of these fields equidistribute (in a regularized sense) along one of two subspaces of the space of (rank $p-1$) shapes and which space they lie on depends on the ramification of p in the field.

With the goal of showing that the shapes of fields in a given family are equidistributed we need to first determine the shapes as we vary over the fields in our family. Once the shapes have been determined we will create a parametrization, or bijection, between the shapes and certain integer points in some bounded subset of a real vector space. The idea is then to approximate the number of integer points in the region using Davenports

lemma and sieve methods from analytic number theory. Though some of the methods of this paper coincide with the ones used in [15] we will ultimately end up with a new proof of Harron's pure cubic results while also extending them to all pure prime degree number fields.

1.5. A Galois theoretic interpretation of pure fields and number field asymptotics. This final section provides a bit of an aside to the current project but will allow us to phrase the results in a manner that may be more familiar to anyone studying number field asymptotics. We have two major motivations in the study of shapes which stem from Malle's conjecture: the first is that it seems number field asymptotics can often be obtained from shape studies, and the second in relation to this is that the shape seems to explain log terms in certain cases. We hope to motivate both phenomena in this section.

Remark 1.5. We first talk about the shapes connection to log terms in Malle's conjecture.

- In [15, 16] Harron observed this phenomena. In these cases the shapes are 2-dimensional lattices which, after appropriate scaling/ rotation, can be viewed as points in the upper half plane. These points lie on geodesics in $\mathcal{H}$ determined by the fields trace zero form and these geodesics have finite length[2] for non-pure complex cubic fields. This difference coincides with the asymptotics of cubic fields with fixed quadratic resolvent: e.g. let $N_3(X, F_2)$ be the number of cubic fields with quadratic resolvent F_2 and absolute discriminant bounded by X. The following result was proved independently by Henri Cohen and Anna Morra, in [10], and Manjul Bhargava and Ari Shnidman, in [7]:

$$N_3\left(X, \mathbf{Q}\left(\sqrt{d}\right)\right) \sim \begin{cases} X^{1/2} & d \neq -3 \\ X^{1/2}\log(X) & d = -3 \end{cases} \tag{1.1}$$

  When $d = -3$ the quadratic field contains the cube roots of unity and the corresponding cubic field is pure. So, we see log terms in the asymptotics when the geodesics have infinite measure.
- In [14] Piper H and Rob Harron show a similar phenomena happens in the case of V_4 quartic fields. If $N_4(X, V_4)$ is the number of V_4-quartic fields with discriminant bounded by X then $N_4(X, V_4) \sim X^{1/2}\log(X)$. The authors mention that if the shape of such fields lie in a "box", of side length R, which constrains the (two) shape parameters then the number of fields with discriminant bounded by X and shape in this box grows like $X^{1/2}\log^2(R)$.

[2] with respect to the hyperbolic measure on $\mathcal{H}$

- In forthcoming work with Rob Harron and Ila Varma, [17], we study the shape of non-Galois sextic fields (i.e. those sextic fields with absolute Galois group $C_3 \wr C_2$) with a fixed quadratic subfield. Jurgen Klüners, in [20], showed that these fields witness the failure of Malle's conjecture: specifically, he shows that the conjecture predicts the correct power of X in the asymptotics but not a log term that appears when you count those sextic fields with quadratic subfield $F_2 = \mathbf{Q}(\sqrt{-3})$[3]. In fact more is true: if you count those non-Galois sextic fields which don't have this cyclotomic subfield then the count does adhere to Malle's conjecture. We investigate this family and show that the "shape" of these fields lie on one dimensional subspaces of the space of shapes. Furthermore, the subspaces on which they lie have infinite measure when the quadratic subfield is $\mathbf{Q}(\zeta_3)$, and finite measure otherwise.

In all cases we observe a relationship between the space in which the shapes lie and the asymptotics (specifically the log terms in the asymptotics) of the fields.

The works in the remark above motivated this section and that in the final section of that paper. We wanted to see if the same phenomena, as in [15], occurs in this generalization. That required a Galois interpretation, a fixed resolvent field and the asymptotics for fields with both the given Galois conditions and the fixed resolvent: Theorem D provides most of this by proving that the pure prime degree fields are exactly those degree p number fields whose Galois group[4] is isomorphic to the Frobenius group, and whose (unique) degree $(p-1)$ resolvent field is isomorphic to $\mathbf{Q}(\zeta_p)$. We define all of this precisely in the final section but for now we note that F_p is called the Frobenius group and is defined, for our purposes, as the semi direct product:

$$F_p = (\mathbf{Z}/p\mathbf{Z}) \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$$

and this provides a Galois theoretic interpretation of pure prime degree fields.

Now, for the asymptotics of such fields: Kübra Benli, in [1], proves that the number of pure prime degree fields with discriminant bounded by X grows like $X^{1/p}Q_p(\log(X))$ where $Q_p(x)$ is a polynomial of degree $p-2$. Using Theorem D this gives asymptotic results for the number of (degree p) Frobenius fields with fixed cyclotomic resolvent field. With that we can phrase our results, as was done in [14], as follows: the number of fields with discriminant bounded by X, and shape in a "hypercube" of side length R which constrains the (ℓ) shape parameters, grows like

[3]Again, this is the cyclotomic field $\mathbf{Q}(\zeta_3)$.

[4]Here we mean the Galois group of the Galois closure

$X^{1/p}\log(X)^{\ell-1}H(\log(R))$ where $H(x)$ is a homogeneous polynomial of degree ℓ. This completes a part of the generalization we are after: the remaining part, and subject of another project, is to repeat this study with Frobenius fields with different fixed resolvent fields.

Remark 1.6. It is interesting to consider whether, and under what conditions, one can recover asymptotic results (as in [21]) from results on the distribution of shapes. This process requires extra care with the error terms to account for the shape bounds, but in many of the existing results, the asymptotics can indeed be recovered. For example, in the pure cubic case, it is possible to recover not only the correct main term $(X^{1/2}\log(X))$ but also the constant of proportionality, as demonstrated in [7, 10].

We believe that recovering the correct powers of X and $\log(X)$ is achievable in this paper through a more detailed analysis of the error terms and then allowing the shape bounds to tend to a power of the discriminant. However, we do not expect that the constant of proportionality can be recovered when $p > 3$. The primary distinction seems to lie in the structure of the space of shapes: in the cubic case, the shape is governed solely by the ratio a_2/a_1, and the symmetry of these fields (swapping a_1 and a_2 yields the same field) ensures that both the distribution questions can be exhibited by counting within the same general space. In this context, Maillet's determinant is equal to 1. For $p \geq 5$, however, the measure of the space of shapes is intricately tied to Maillet's determinant, and we do not see a straightforward method to recover the constant of proportionality. One of the key objectives of [17] is to further examine these connections and make the relationship between shape distributions and field counts more explicit.

The main takeaway from this is that we can phrase our study in terms of Galois groups and resolvent fields rather than simply as pure extensions of $\mathbf{Q}$. This aligns the study of shapes and their distributions a little more closely with work in the direction of Malle's conjecture which has, in general, motivated a number of the authors projects. In general there is much to do to relate shape studies to number field asymptotics but, as is stated in [16], it would be interesting to have heuristics for the field counting functions that incorporate shape conditions.

2. The shape of a number field

The shape of a number field is defined to be the equivalence class of the lattice $j(\mathcal{O}_K^{\perp})$ up to scaling, rotation, and reflection. To define this precisely we need to know what the shape of an arbitrary lattice is, and then to specify how we obtain the lattice $j(\mathcal{O}_K^{\perp})$.

2.1. The shape of a lattice. We let Λ be a rank r lattice. The *shape* of Λ is the equivalence class of this lattice up to scaling, rotation, and reflection.

Often in the literature the space of shapes of rank r lattices is presented as the double coset space:

$$S_r = \mathrm{GL}_r(\mathbf{Z}) \backslash \mathrm{GL}_r(\mathbf{R}) / \mathrm{GO}_r(\mathbf{R})$$

where GL denotes the general linear group and GO the group of orthogonal matrices[5]. We take an alternative approach, as in [14], which will instead define the space of shapes in terms of Gram matrices. Letting $\mathcal{G}$ denote the set of positive definite real symmetric $(r \times r)$-matrices we have that the space of shapes of rank r lattices is also represented as

$$S_r = \mathrm{GL}_r(\mathbf{Z}) \backslash \mathcal{G} / \mathbf{R}^\times.$$

Given a lattice Λ in an inner product space V and with basis $\{b_1, \ldots, b_r\}$ we form the Gram matrix of λ, denoted $\mathrm{Gr}(\Lambda)$, by taking inner products of the basis:

$$\mathrm{Gr}(\Lambda) = (\langle b_i, b_j \rangle)_{1 \leq i,j \leq r}.$$

This is an element of $\mathcal{G}$ and uniquely identifies the lattice up to change of basis. For $g \in \mathrm{GL}_r(\mathbf{Z})$ and $G \in \mathcal{G}$ we define the left action of $\mathrm{GL}_r(\mathbf{Z}) \backslash \mathcal{G}$ as:

$$g \cdot G := g G g^T$$

which comes from the natural action on the set of Gram matrices. For $r \in \mathbf{R}^\times$ and $G \in \mathcal{G}$ we define the right action of $\mathcal{G}/\mathbf{R}^\times$ as:

$$G \cdot r := r^2 G$$

which, again, comes from the natural action of scaling the basis vectors of Λ and computing $\mathrm{Gr}(\Lambda)$. When we refer to the shape of a lattice we will often be referring to an explicit Gram matrix whose calculation we describe in the next section. For further details we refer the reader to [14].

2.2. The lattice $j(\mathcal{O}_K^\perp)$. Let K be a number field of degree n, $\mathcal{O}_K$ be it's ring of integers with basis $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$, and $\{\sigma_i\}_{1 \leq i \leq n}$ be the set of embeddings of K into $\mathbf{C}$. Then we have the embedding:

$$\begin{aligned} j : K &\longrightarrow \mathbf{C}^n \\ \alpha &\longmapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha)). \end{aligned}$$

The $\mathbf{R}$-span of the image of this map is an inner-product space, often denoted by $K_{\mathbf{R}} \cong \mathbf{R}^n$, and the restriction of j to $\mathcal{O}_K$ yields a rank n lattice in $K_{\mathbf{R}}$. Though there is some temptation to define the shape of K to be the shape of this lattice there are issues when investigating the distribution of shapes as we vary over some family of fields: namely, as all such lattices can be made to have the common vector $j(1)$, we lose the potential "randomness" of shape. As such, we define the shape of K to be

[5] i.e. those matrices M such that $M \cdot M^T = \lambda I$ for some $\lambda \neq 0$

the shape of the lattice obtained by projecting $j(\mathcal{O}_K)$ onto the orthogonal complement of $j(1)$: specifically we define the perp map

$$\alpha^{\perp} := n\alpha - \mathrm{tr}(\alpha)$$

and let $\mathcal{O}_K^{\perp}$ be the image of $\mathcal{O}_K$ under this map. Note that the elements of $\mathcal{O}_K^{\perp}$ are elements of trace-zero and map, under the Minkowski map, to vectors orthogonal to $j(1)$. Using this we obtain a lattice, $j(\mathcal{O}_K^{\perp})$, of rank $n-1$ and we define the shape of K to be the shape of this lattice. Given a basis of $\mathcal{O}_K$, $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$, we obtain a basis of $\mathcal{O}_K^{\perp}$, $\{\alpha_1^{\perp}, \ldots, \alpha_{n-1}^{\perp}\}$, and we obtain a representative of the shape by computing the Gram matrix:

$$\mathrm{Gr}(j(\mathcal{O}_K^{\perp})) = (\langle j(\alpha_i^{\perp}), j(\alpha_j^{\perp})\rangle).$$

3. Shapes of pure prime degree number fields

One will notice, in the studies mentioned in the introduction, that the shape of K often depends on the ramification of p in K. More specifically the subspace on which the shape of K lies is determined by whether p is wildly ramified in K or not: this is referred to as a wild versus tame dichotomy in [14, 15]. The same phenomenon occurs in this study and so, after we determine a sufficiently nice basis for $\mathcal{O}_K$, we will split this section up according to whether p is wildly ramified in K, or not: our notation for such K will be K_{wild} and K_{tame} respectively, unless it is otherwise clear from context.

We assume throughout that p is a prime number greater than 2; this will simplify the statements of Lemmas 3.1 and 3.2 but, as all quadratic fields have the same shape, we will not be losing anything with this simplification.

3.1. The integral basis of $K/\mathbf{Q}$. Let $K = \mathbf{Q}(\alpha)$ where α is the unique real root[6] of the irreducible polynomial $x^p - m$ belonging to $\mathbf{Z}[x]$ and $m = \prod_{i=1}^{p-1} a_i^i$ where the a_i are squarefree and pairwise relatively prime. Throughout this paper we will refer to K, defined in this way, as a *pure prime degree number field*. The following two lemmas, from [19], provide us with the discriminant and an integral basis for $K/\mathbf{Q}$ respectively:

Lemma 3.1 ([19])**.** *Let $K = \mathbf{Q}(\alpha)$ be a pure prime degree number field, as above, and let q run over all distinct primes dividing m. We have the following:*

(i) *When $p \mid m$, or $p \nmid m$ and $p^2 \nmid (m^p - m)$, the discriminant of K is given by:*

$$\Delta_K = (-1)^{\frac{(p-1)}{2}} p^p \prod_{q \mid m} q^{p-1}.$$

[6]This gives us that $K \subseteq \mathbf{R}$ which will simplify notation a bit in what follows.

(ii) *If* $p^2 \mid (m^{p-1}-1)$*, then the discriminant of* K *is given by:*

$$\Delta_K = (-1)^{\frac{(p-1)}{2}} p^{p-2} \prod_{q \mid m} q^{p-1}.$$

As p divides the discriminant of K we know that p is ramified in both cases: when $p^p \mid \Delta(K)$ we say p is wildly ramified in K. Otherwise, we say that p is tamely ramified in K. Using this we have that the fields in (i) are wild, and the fields in (ii) are tame. The next lemma provides an integral basis in each case:

Lemma 3.2 ([19])**.** *Let* K, α, m *be defined as above and, for* $j \in \{1, \ldots, p-1\}$*, let* $\gamma_j = \alpha^j / \prod_{i=1}^{p-1} a_i^{\lfloor \frac{ij}{p} \rfloor}$*. Then we have:*

(i) *If* $p^2 \nmid (m^{p-1}-1)$*, then the set* $\{1, \gamma_1, \gamma_2, \ldots, \gamma_{p-1}\}$ *is an integral basis of* K_{wild}*.*

(ii) *If* $p^2 \mid (m^{p-1}-1)$*, then the set* $\{\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{p-1}\}$ *is an integral basis of* K_{tame} *where* $\gamma_0 = \frac{1}{p}\sum_{i=0}^{p-1}(\epsilon\alpha)^i$ *where* ϵ *is any integer so that* $m\epsilon \equiv 1 \pmod{p^2}$*.*

To provide a familiar example and to highlight a bit of the notation to follow we remind ourselves that:

Example 3.3. When $p = 3$ and $K = \mathbf{Q}(\sqrt[3]{m})$ we write $m = a_1 a_2^2$, $\alpha = \sqrt[3]{m}$ and $\beta = \sqrt[3]{a_1^2 a_2}$. If $3^2 \mid m^2 - 1$ then $m \equiv \pm 1 \pmod 9$ and ϵ is ± 1. The integral basis of K is then given by:

$$\begin{cases} \left\{1, \alpha, \frac{\alpha^2}{a_2}\right\} = \{1, \alpha, \beta\} & \text{when } m \not\equiv \pm 1 \pmod 9 \\ \left\{\frac{1 \pm \alpha + \alpha^2}{3}, \alpha, \frac{\alpha^2}{a_2}\right\} = \left\{\frac{1 \pm \alpha + \alpha^2}{3}, \alpha, \beta\right\} & \text{when } m \equiv \pm 1 \pmod 9. \end{cases}$$

Note that the congruence condition on m is the same as the condition on ramification mentioned above. In [15] we see that the shapes of pure cubic fields lie on 2 vertical geodesics in the space of rank 2 lattices: moreover the ramification at 3 determines which vertical geodesic the shape lies on. We will see exactly what this all looks like below but those who are too excited to wait can look at Figure 3.1!

3.2. Slightly altered tame basis. We note that the integral basis of K_{tame} given in the previous section will not be particularly nice for our purposes: the shape of K is given by mapping an integral basis into $\mathbf{C}^n$ and projecting onto the orthogonal complement of the subspace spanned by $j(1)$ and it is therefore nice to write an integral basis containing 1. To that end we choose our basis to be $\{1, \nu, \gamma_2, \ldots, \gamma_{p-1}\}$ where

$$\nu = \frac{m + \alpha + \epsilon\alpha^2 + \cdots + \epsilon^{p-2}\alpha^{p-1}}{p}$$

That this element, ν, is integral comes from the fact that $\epsilon m \equiv 1 \pmod{p^2}$. Let $k \in \mathbf{Z}$ be such that $\epsilon m = 1 + kp^2$. Then we have:

$$\begin{aligned} m\gamma_0 - kp\sum_{i=1}^{p-1}\epsilon^{i-1}\alpha^i &= m\left(\frac{1+\epsilon\alpha+(\epsilon\alpha)^2+\cdots+(\epsilon\alpha)^{p-1}}{p}\right) - kp\sum_{i=1}^{p-1}\epsilon^{i-1}\alpha^i \\ &= \frac{m+\sum_{i=1}^{p-1}(\epsilon m - kp^2)\epsilon^{i-1}\alpha^i}{p} \\ &= \frac{m+\alpha+\epsilon\alpha^2+\cdots+\epsilon^{p-2}\alpha^{p-1}}{p} \\ &= \nu. \end{aligned}$$

Thus, $\nu \in \mathcal{O}_K$ and the change of basis matrix from the rational basis $\{1, \gamma_1, \gamma_2, \ldots, \gamma_{p-1}\}$ to the basis $\{1, \nu, \gamma_2, \ldots, \gamma_{p-1}\}$ is:

$$\mathcal{C}_t = \begin{pmatrix} 1 & 0 & 0 & \ldots & \ldots & 0 \\ \frac{m}{p} & \frac{1}{p} & \frac{\epsilon b_2}{p} & \ldots & \ldots & \frac{\epsilon^{p-2}b_{p-1}}{p} \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & \ldots & 0 & 1 \end{pmatrix}$$

where $b_j = \prod_{i=1}^{p-1} a_i^{\lfloor \frac{ij}{p} \rfloor}$. The determinant of this matrix is $\frac{1}{p}$ which shows that the basis $\{1, \nu, \gamma_2, \ldots, \gamma_{p-1}\}$ has the correct discriminant[7] and we can therefore conclude that it is indeed an integral basis; we use this as our basis of K_{tame} below.

3.3. The shape of K_{wild}. We let $\zeta_p = e^{2\pi i/p}$ and α be as above. We also let σ denote the real embedding of K and τ_k denote the complex embedding sending α to $\zeta_p^k\alpha$ for $k \in \{1, \ldots, \frac{(p-1)}{2}\}$. Finally we let j be the embedding of K into $\mathbf{C}^p$ given by:

$$j(a) = (\sigma(a), \tau_1(a), \ldots, \tau_{(p-1)/2}(a), \overline{\tau}_{(p-1)/2}(a), \ldots, \overline{\tau_1}(a)).$$

Note that we have changed the ordering of j from above, this does not change anything but we feel this is a slightly more pleasant way of presenting it.

Using the above embedding, j, we have the following result about the Gram matrix of the basis for pure prime degree *wild* fields:

[7]Square and compare to Lemma 3.1.

Proposition 3.4. *The Gram matrix of the basis* $\{1, \gamma_1, \gamma_2, \ldots, \gamma_{p-1}\}$ *is given by:*

$$\mathcal{G}(K_{\text{wild}}) = \begin{pmatrix} p & & & & \\ & p\gamma_1^2 & & & \\ & & p\gamma_2^2 & & \\ & & & \ddots & \\ & & & & p\gamma_{p-1}^2 \end{pmatrix}$$

Proof. To see this we first note that

$$\begin{aligned} j(1) &= (1, \ldots, 1) \\ j(\gamma_i) &= (\gamma_i, \zeta_p^i \gamma_i, \zeta_p^{2i} \gamma_i, \ldots, \zeta_p^{(p-1)i} \gamma_i) \end{aligned}$$

Taking the Hermitian inner product of all pairs of vectors we find that the (i, j) entry of the Gram matrix, $\mathcal{G}_{i,j}$, is given by:

$$\begin{aligned} \sum_{r=0}^{p-1} \zeta_p^{ir} \gamma_i \cdot \overline{\zeta_p^{jr} \gamma_j} &= \gamma_i \gamma_j \sum_{r=0}^{p-1} \zeta_p^{ir} \overline{\zeta_p^{jr}} \\ &= \gamma_i \gamma_j \sum_{r=0}^{p-1} \zeta_p^{ir} \zeta_p^{(p-j)r} \\ &= \gamma_i \gamma_j \sum_{r=0}^{p-1} \zeta_p^{(p+i-j)r} \end{aligned}$$

When $i \neq j$, $p + i - j \equiv k \pmod{p}$ for some $k \in \{1, \ldots, p-1\}$ and therefore $\sum_{r=0}^{p-1} \zeta_p^{(k)r} = \sum_{n=0}^{p-1} \zeta^n = 0$. This shows that all off diagonal entries are 0, and when $i = j$ we have $\mathcal{G}_{i,i} = \gamma_i^2 \sum_{r=0}^{p-1} \zeta_p^{(p+i-i)r} = \gamma_i^2 \sum_{r=0}^{p-1} 1 = \gamma_i^2 \cdot p$ as desired. □

The Gram matrix in Proposition 3.4 shows that the vectors are all orthogonal and therefore the vectors $j(\gamma_1), \ldots, j(\gamma_{p-1})$ span $j(\mathcal{O}_K^\perp)$. Therefore we obtain the shape of K_{wild} by simply deleting the first row and column to obtain:

Theorem 3.5. *The shape of* K_{wild} *is represented by:*

$$\begin{pmatrix} \gamma_1^2 & 0 & \ldots & 0 \\ 0 & \gamma_2^2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & \gamma_{p-1}^2 \end{pmatrix}$$

From this we see that the shape of K_{wild} is an orthorhombic lattice: i.e. $\mathcal{O}_K^\perp$ is spanned by $p-1$ pairwise orthogonal vectors of length $|\gamma_i|$. When $p = 3$ we are again in the pure cubic case and we see that, when 3 is wildly

ramified, the shape of K is rectangular (orthorhombic) and lies on the blue geodesic in S_2 shown as follows:

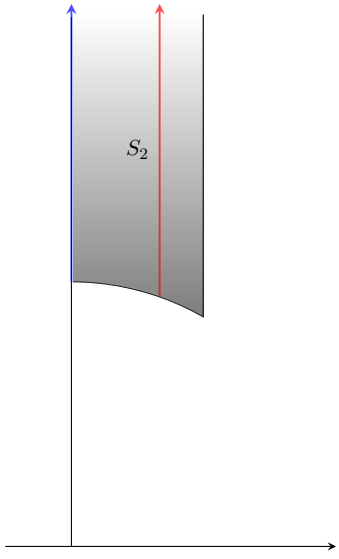


Figure 3.1. Subspaces of shapes of pure cubic fields (wild and tame) within the space of shapes of rank 2 lattices, S_2

When K is tame the shape is not orthorhombic and the distribution is along the red geodesic in S_2 with real part $\frac{1}{3}$.

Example 3.6. Using Theorem 3.5 in the cubic example above, Example 3.3, for K wildly ramified at 3, we see that the shape of K is

$$\mathrm{sh}(K) = \begin{pmatrix} \sqrt[3]{a_1^2 a_2^4} & 0 \\ 0 & \sqrt[3]{a_1^4 a_2^2} \end{pmatrix}.$$

Though this is a rectangular lattice with side lengths $\sqrt[3]{a_1 a_2^2}$ and $\sqrt[3]{a_1^2 a_2}$ it is more convenient to scale this matrix by the (1,1)-entry giving us:

$$\mathrm{sh}(K) = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt[3]{\frac{a_1}{a_2}}^2 \end{pmatrix}.$$

which represents a rectangular lattice who side lengths are 1 and, in the notation of [15], $r_K^{1/3} = \sqrt[3]{\frac{a_1}{a_2}}$. Without loss of generality we may assume $a_1 > a_2$ and we see that this lattice can be represented as a point on the blue geodesic above with height determined by r_K.

We note that it is common to scale the Gram matrix of $\mathcal{O}_K^\perp$ to obtain a unit vector, as above, and to call this the shape of K. What we do below is slightly different but will better illuminate the beautiful symmetry in these fields we study. The reader may also notice that, in Section 4, this alternative scaling, and hence alternative shape, will make the inherited measure feel very intuitive.

3.4. Shape of K_{tame}. We saw above that an integral basis of K_{tame} is given by $\{1, \nu, \gamma_2, \dots, \gamma_{p-1}\}$ where

$$\nu = \frac{m + \alpha + \epsilon\alpha^2 + \cdots + \epsilon^{p-2}\alpha^{p-1}}{p}.$$

We also saw the change of basis matrix from $\{1, \gamma_1, \gamma_2, \dots, \gamma_{p-1}\}$ to the basis above is given by:

$$\mathcal{C}_t = \begin{pmatrix} 1 & 0 & 0 & \dots & \dots & 0 \\ \frac{m}{p} & \frac{1}{p} & \frac{\epsilon b_2}{p} & \dots & \dots & \frac{\epsilon^{p-2} b_{p-1}}{p} \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}. \tag{3.1}$$

The Gram matrix of K_{tame} is therefore given by

$$\mathcal{G}(K_{\text{tame}}) = \mathcal{C}_t \mathcal{G}(K) \mathcal{C}_t^T \tag{3.2}$$

where $\mathcal{G}(K)$ is the Gram matrix of the rational basis, i.e. the Gram matrix of K_{wild} seen above.

Proposition 3.7. *The Gram matrix of the integral basis of K_{tame} given above is:*

$$\mathcal{G}(K_{\text{tame}}) = \begin{pmatrix} p & m & 0 & 0 & \dots & 0 \\ m & \nu' & \epsilon(\gamma_2)(\gamma_1)^2 & \epsilon^2(\gamma_3)(\gamma_1)^3 & \dots & \epsilon^{p-2}(\gamma_{p-1})(\gamma_1)^{p-1} \\ 0 & \epsilon(\gamma_2)(\gamma_1)^2 & p\gamma_2^2 & 0 & \dots & 0 \\ \vdots & \epsilon^2(\gamma_3)(\gamma_1)^3 & 0 & p\gamma_3^2 & \ddots & \vdots \\ & \vdots & & \ddots & \ddots & 0 \\ 0 & \epsilon^{p-2}(\gamma_{p-1})(\gamma_1)^{p-1} & \dots & & 0 & p\gamma_{p-1}^2 \end{pmatrix}$$

where $\nu' = \frac{1}{p}\left(m^2 + \gamma_1^2 + \epsilon^2\gamma_1^4 + \cdots + \epsilon^{2p-4}\gamma_1^{2p-2}\right)$.

Proof. This is shown by computing (3.2) and noting that $b_i\gamma_i^2 = b_i\gamma_i\left(\frac{\gamma_1^i}{b_i}\right) = \gamma_i\gamma_1^i$. □

Using this we obtain the shape of K_{tame} as follows:

Theorem 3.8. *The shape of K_{tame} is represented by:*

$$\begin{pmatrix} \nu' - \frac{m^2}{p} & \epsilon(\gamma_2)(\gamma_1)^2 & \epsilon^2(\gamma_3)(\gamma_1)^3 & \dots & \epsilon^{p-2}(\gamma_{p-1})(\gamma_1)^{p-1} \\ \epsilon(\gamma_2)(\gamma_1)^2 & p\gamma_2^2 & 0 & \dots & 0 \\ \epsilon^2(\gamma_3)(\gamma_1)^3 & 0 & p\gamma_3^2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \epsilon^{p-2}(\gamma_{p-1})(\gamma_1)^{p-1} & 0 & \dots & 0 & p\gamma_{p-1}^2 \end{pmatrix}$$

Proof. Note that $j(\gamma_i)$ is orthogonal to $j(1)$ for all i. In the case of $j(\nu)$ we have

$$j(\nu)^\perp = j(\nu) - \frac{\langle j(\nu), j(1)\rangle}{\langle j(1), j(1)\rangle} j(1) = j(\nu) - \frac{m}{p} j(1).$$

Therefore

$$\begin{aligned} \langle j(\nu)^\perp, j(\nu)^\perp\rangle &= \langle j(\nu), j(\nu)\rangle - 2\left\langle j(\nu), \frac{m}{p} j(1)\right\rangle + \left\langle \frac{m}{p} j(1), \frac{m}{p} j(1)\right\rangle \\ &= \langle j(\nu), j(\nu)\rangle - \frac{2m}{p}\langle j(\nu), j(1)\rangle + \frac{m^2}{p^2}\langle j(1), j(1)\rangle \\ &= \nu' - \frac{2m}{p}\cdot m + \frac{m^2}{p^2}\cdot p \\ &= \nu' - \frac{m^2}{p} \end{aligned}$$

□

In conclusion we proved that the lattice $j(\mathcal{O}_K^\perp)$, for K a pure prime degree number field, is an orthorhombic lattice if p was wildly ramified in K and a general (non-orthorhombic) lattice[8], if p was tamely ramified in K. Of course the tamely ramified fields are nearly orthogonal and the non-orthogonality comes from a single vector, the remaining sublattice is orthorhombic. Nonetheless, this again gives evidence that the type of lattice (and hence the space in which the shape lies) is determined by the ramification of p in the field K. To compare with [15] this is the type I vs type II phenomena whose shapes lie on the imaginary axis and the vertical geodesic with real part $r = \frac{1}{3}$ respectively.

4. Parametrizations

The goal of this section will be to develop a parametrization of pure prime degree number fields with specified shape conditions. We first set up a correspondence between the pure prime degree fields and tuples in $\mathbf{Z}^{p-1}$ which satisfying some specific conditions. Once we have parametrized the fields, without shape conditions, we will use this to obtain parametrizations of the shapes from these tuples.

[8]or an ordinary lattice, as in [24]

4.1. Fields. To parametrize the family of pure prime degree fields we use *strongly carefree tuples*:

Definition 4.1. *We define a tuple* $(a_1, a_2, \ldots, a_n) \in \mathbf{Z}^n$ *to be* strongly carefree *if* a_i *is squarefree for all* i *and* $(a_i, a_j) = 1$ *for all* $j \neq i$ *(i.e. the* a_i *are squarefree and pairwise relatively prime).*

Note that since $m^{1/p}$ and $(-m)^{1/p}$ generate the same pure prime degree number field we need only consider the tuples in which $a_i > 0$ for all i. For sake of uniformity we denote the set of strongly carefree (and positive) n-tuples by $\mathcal{SC}^n$ or, when the degree of K is clear, by $\mathcal{SC}$ as in [14].

The pure prime degree fields are exactly parametrized by strongly carefree $(p-1)$-tuples. For two strongly carefree tuples $(a_1, a_2, \ldots, a_{p-1})$ and $(a'_1, a'_2, \ldots, a'_{p-1})$ we obtain integers $m = a_1 a_2^2 \cdots a_{p-1}^{p-1}$ and $m' = a'_1 (a'_2)^2 \cdots (a'_{p-1})^{p-1}$. Furthermore m and m' generate the same field if $m' = \gamma^p m^i$ for $(i, p) = 1$ and $\gamma \in \mathbf{Z}$. Define an action of $g \in S_{p-1}$ on the set of strongly carefree tuples by:

$$g \cdot (a_1, a_2, \ldots, a_{p-1}) = (a_{g(1)}, a_{g(2)}, \ldots, a_{g(p-1)}).$$

We can then define the group

$$C_{p-1} = \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & p-4 & p-3 & p-2 & p-1 \\ \frac{p-1}{2} & p-1 & \frac{p-1}{2}-1 & p-2 & \ldots & 2 & \frac{p+1}{2}+1 & 1 & \frac{p+1}{2} \end{pmatrix} \right\rangle.$$

which gives us the following:

Theorem 4.2. *There is a bijection:*

$$\left\{ \begin{array}{l} \textit{Isomorphism classes of pure} \\ \textit{prime degree, } p\textit{, number fields} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} C_{p-1}\textit{-equivalence classes} \\ \textit{of } (a_1, \ldots, a_{p-1}) \in \mathcal{SC}^{p-1} \end{array} \right\}.$$

Example 4.3. When $p = 5$ we have $K = \mathbf{Q}(\sqrt[5]{m})$ with $m = a_1 a_2^2 a_3^3 a_4^4$ and $C_4 = \langle (1243) \rangle$. The elements of the rational basis, as in Lemma 3.2, are

$$\gamma_1 = (a_1 a_2^2 a_3^3 a_4^4)^{1/5} \qquad \gamma_2 = (a_1^2 a_2^4 a_3 a_4^3)^{1/5}$$
$$\gamma_3 = (a_1^3 a_2 a_3^4 a_4^3)^{1/5} \qquad \gamma_4 = (a_1^4 a_2^3 a_3^2 a_4)^{1/5}$$

and the orbit of (a_1, a_2, a_3, a_4) under $g = (1243)$ is

$$\{(a_1, a_2, a_3, a_4), (a_2, a_4, a_1, a_3), (a_4, a_3, a_2, a_1), (a_3, a_1, a_4, a_2)\}.$$

Remark 4.4. Letting $\mathcal{N}_p(X)$ be the number of pure, prime degree, fields with absolute discriminant bounded by X we could obtain an asymptotic for $\mathcal{N}_p(X)$ by counting the number of strongly carefree tuples satisfying $\prod a_i < X^{1/p}$ and $a_i \geq 1, \forall\ i$. In what follows we will want to count those fields with absolute discriminant bounded by X and shape in some "nice" set W: we denote the fields of bounded discriminant and shape in W by $\mathcal{N}_p(X, W)$. To count this we need to impose the shape conditions which will impose additional restrictions on the a_i.

4.2. Shapes. Though we will state results in the case of tame fields we will work primarily with wild fields in what follows recalling the simple conjugation between the two in (3.1). Now, the shape of K is defined to be the lattice $j(\mathcal{O}_K^{\perp})$ up to scaling, rotation, and reflections and so we will be a bit more specific in our representative of the shape of K. Specifically we will choose a representative of the shape of wild fields which has hypervolume 1 and whose diagonal entries are given in increasing order. The following normalization will show us the symmetry present in these lattices which forces the shapes to lie on an ℓ-dimensional subspace of S_{p-1}. It will also help us prove the statement of regularized equidistribution and show the shape is a complete invariant of pure prime degree number fields.

4.2.1. ***Shape parametrization.*** Let $\ell = \frac{p-1}{2}$. One may have noticed that in the Gram matrix of $j(\mathcal{O}_K)$, and hence the shape matrix, a dependence on the γ_j: namely we see that $\gamma_j = \frac{\gamma_\ell \gamma_{\ell+1}}{\gamma_{p-j}}$. The determinant of the matrix given in Theorem 3.5 is then

$$(\gamma_\ell \gamma_{\ell+1})^\ell = \prod_{i=1}^{p-1} a_i^\ell.$$

Using this we are led to a very natural normalization of the shape by $(\gamma_\ell \gamma_{\ell+1})^{-1} = \prod_i a_i^{-1}$. This yields the following representative of shape:

$$\mathrm{sh}(K_{\mathrm{wild}}) = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_\ell & & & \\ & & & \lambda_\ell^{-1} & & \\ & & & & \ddots & \\ & & & & & \lambda_1^{-1} \end{pmatrix} \tag{4.1}$$

where $\lambda_i = \frac{\gamma_i^2}{\gamma_\ell \gamma_{\ell+1}}$ for $1 \leq i \leq \ell$ and we immediately see the ℓ parameters that govern the shape of these fields.

Similarly, after normalizing by the same factor, the shape of K_{tame} given in Theorem 3.8 is:

$$\mathrm{sh}(K_{\mathrm{tame}}) = \begin{pmatrix} \nu'' & \dots & \epsilon^{\ell-1} b_\ell \lambda_\ell & \frac{\epsilon^\ell b_\ell}{\lambda_\ell} & \dots & \frac{\epsilon^{p-2} b_{p-1}}{\lambda_1} \\ & \ddots & 0 & \dots & & 0 \\ & & p\lambda_\ell & & & \vdots \\ & & & \frac{p}{\lambda_\ell} & & \\ & & & & \ddots & 0 \\ & & & & & \frac{p}{\lambda_1} \end{pmatrix} \tag{4.2}$$

where

$$\nu'' = \frac{1}{p}\left(\sum_{i=1}^{\ell}\left(\epsilon^{2(i-1)}b_i\lambda_i^2\right) + \left(\epsilon^{2(p-i-1)}b_{p-i}\frac{1}{\lambda_i^2}\right)\right).$$

In both cases we see very explicitly that the shape of K lies in an ℓ-dimensional subspace of the space of rank $p-1$ lattices, and that the parameters controlling the shape are given by $\{\lambda_i\}_{i=1}^{\ell}$.

Example 4.5. For $p=5$, $K=\mathbf{Q}\left(\sqrt[5]{a_1a_2^2a_3^3a_4^4}\right)$, and p wildly ramified in K, Theorem 3.5 tells us that:

$$\mathrm{Gr}(\mathcal{O}_K^{\perp}) = \begin{pmatrix} \left(a_1^2a_2^4a_3^6a_4^8\right)^{1/5} & 0 & 0 & 0 \\ 0 & \left(a_1^4a_2^8a_3^2a_4^6\right)^{1/5} & 0 & 0 \\ 0 & 0 & \left(a_1^6a_2^2a_3^8a_4^4\right)^{1/5} & 0 \\ 0 & 0 & 0 & \left(a_1^8a_2^6a_3^4a_4^2\right)^{1/5} \end{pmatrix}$$

The aforementioned normalization by $\prod_i a_i^{-1}$ gives us the following shape parameters:

$$\lambda_1 = \left(\frac{a_4^3a_3}{a_1^3a_2}\right)^{1/5} \qquad \lambda_2 = \left(\frac{a_4a_2^3}{a_1a_3^3}\right)^{1/5}$$

Note that as the shape of a number field is defined up to scaling, rotation, and reflection, it makes sense to scale as we have done and then perform some change of basis to obtain a shape matrix with increasing diagonal entries. After doing this we define the shape of K as:

Definition 4.6. *We choose a representative of the shape of a pure prime degree number field, denoted* $\mathrm{Sh}(K)$*, to be the matrix* $\mathrm{sh}(K)$ *above, where the diagonal elements are given in increasing order.*

Or, in terms of the shape parameters, we have that:

$$\mathrm{Sh}(K) = \{(\lambda_{\sigma_1}, \lambda_{\sigma_2}, \ldots, \lambda_{\sigma_\ell}) : 1 < \lambda_{\sigma_1} < \lambda_{\sigma_2} < \cdots < \lambda_{\sigma_\ell}\}.$$

We now describe the shape parameters explicitly in terms of the a_i and end this section by showing that the shape of a pure prime degree field, K, is a complete invariant. Note that the $\{\lambda_i\}$ and the $\{\lambda_{\sigma_i}\}$ are the same and so our description below, while not necessarily ordered as in $\mathrm{Sh}(K)$, will be enough for our purposes.

Lemma 4.7. *The shape parameters of* K*,* $\{\lambda_i^{\pm 1}\}_{i=1}^{\ell}$*, are given by:*

$$\lambda_j = \left(\prod_{i=1}^{\ell}\left(\frac{a_i}{a_{p-i}}\right)^{2ij-p-2p\left\lfloor\frac{ij}{p}\right\rfloor}\right)^{1/p}.$$

Proof. Since $\lambda_j = \frac{\gamma_j^2}{\gamma_\ell \gamma_{\ell+1}}$ we have:

$$\begin{aligned}
\lambda_j^p &= \left(\frac{\gamma_j^2}{\gamma_\ell \gamma_{\ell+1}} \right)^p \\
&= \frac{\prod_{i=1}^{\ell} a_i^{2ij - 2p\lfloor \frac{ij}{p} \rfloor} a_{p-i}^{2j(p-i) - 2p\lfloor \frac{(p-i)j}{p} \rfloor}}{\prod_{i=1}^{p-1} a_i^p} \\
&= \prod_{i=1}^{\ell} a_i^{2ij - 2p\lfloor \frac{ij}{p} \rfloor - p} a_{p-i}^{2jp - 2ji - 2p\lfloor j - \frac{ij}{p} \rfloor - p} \\
&= \prod_{i=1}^{\ell} a_i^{2ij - 2p\lfloor \frac{ij}{p} \rfloor - p} a_{p-i}^{2jp - 2ji - 2p(j - 1 - \lfloor \frac{ij}{p} \rfloor) - p} \\
&= \prod_{i=1}^{\ell} a_i^{2ij - 2p\lfloor \frac{ij}{p} \rfloor - p} a_{p-i}^{2jp - 2ji - 2pj + 2p + 2p\lfloor \frac{ij}{p} \rfloor - p} \\
&= \prod_{i=1}^{\ell} a_i^{2ij - p - 2p\lfloor \frac{ij}{p} \rfloor} a_{p-i}^{-2ji + p + 2p\lfloor \frac{ij}{p} \rfloor} \\
&= \prod_{i=1}^{\ell} \left(\frac{a_i}{a_{p-i}} \right)^{2ij - p - 2p\left\lfloor \frac{ij}{p} \right\rfloor}.
\end{aligned}$$

□

Remark 4.8. Given the shape of a pure prime degree number field we get an element in the isomorphism class of K by simply considering $\mathbf{Q}(\lambda_j)$. More precisely the shape parameters,

$$\begin{aligned}
\lambda_j &= \frac{\gamma_j^2}{\gamma_{\ell-1}\gamma_{\ell+1}} \\
&= \frac{\gamma_j^2}{\prod_{i=1}^{p-1} a_i} \\
&= \frac{\left(\frac{\alpha^{2j}}{\prod_{i=1}^{p-1} a_i^{\lfloor \frac{ij}{p} \rfloor}} \right)}{\prod_{i=1}^{p-1} a_i} \\
&= \frac{\alpha^{2j}}{\prod_{i=1}^{p-1} a_i^{1 + \lfloor \frac{ij}{p} \rfloor}}
\end{aligned}$$

lie in $K = \mathbf{Q}(\alpha^{2j}) = \mathbf{Q}(\alpha)$[9]. Lemma 4.7 shows that the shape parameters are not rational numbers and therefore that $\mathbf{Q} \subsetneq \mathbf{Q}(\lambda_j)$. As K is of prime

[9]This is because $\gcd(2j, p) = 1$

degree and therefore has no intermediate subfields and we conclude that $\mathbf{Q} \subsetneq \mathbf{Q}(\lambda_j) \subset \mathbf{Q}(\alpha^2) = \mathbf{Q}(\alpha)$ or that $\mathbf{Q}(\lambda_j) = \mathbf{Q}(\alpha)$.

From this it is clear that two non-isomorphic fields have different shapes which is enough to prove Theorem B and show that the shape is a complete invariant within the family of pure prime degree number fields. In fact, this argument shows that each shape parameter is a primitive element of the field and therefore we can recover the field using any one of these parameters. One may also ask whether this holds within the family of degree p number fields? For instance, is the fact that these shape parameters are pure numbers (i.e. those coming exactly from pure prime degree fields) enough for shape to discriminate between prime degree fields? The reader can compare this with the result of Harron in [15].

We end this section with an example:

Example 4.9. As with the example above we let $K = \mathbf{Q}\left(\sqrt[5]{a_1 a_2^2 a_3^3 a_4^4}\right)$, and assume that K is wild: then the shape parameters of K are:

$$\lambda_1 = \left(\frac{a_4^3 a_3}{a_1^3 a_2}\right)^{1/5} \qquad \lambda_2 = \left(\frac{a_4 a_2^3}{a_1 a_3^3}\right)^{1/5}.$$

It is clear that $\mathbf{Q}(\lambda_1) \subseteq \mathbf{Q}(\alpha^2)$ as $\lambda_1 = \frac{\alpha^2/a_4}{a_1 a_2 a_3 a_4}$ and that $\lambda_i \notin \mathbf{Q}$. Since there are no intermediate subfields we conclude that $\mathbf{Q}(\lambda_1) = K$ and hence the shape determines the pure quintic field.

5. Measure Theoretic Background... towards equidistribution

This section is devoted to the measures on the spaces of shapes of wild (resp. tame) pure prime degree number fields. In general for a locally compact (Hausdorff) topological group, G, there exists a unique[10] Haar measure, $\mu_G := \mu$, which is left G-invariant (i.e. $\mu(gA) = \mu(A)$ for all $A \subset G$ and $g \in G$; where $gA = \{gx \mid x \in A\} \subset G$).

5.1. Measure on spaces of shapes. Recall that, for K a pure prime degree field with wild ramification at p we have that the shape is a complete invariant of K and that the shape lies in an ℓ-dimensional subspace of the space of shapes.

For $x_i \in \mathbf{R}^\times$ we think of y_i as a ratio of monomials in x_i, as we did with λ_i and a_i/a_{p-i} in the previous section. We then define the measure on the space of shapes of each family of fields to be:

$$\mathrm{d}\mu_?(y_i) := \frac{1}{c_p} \prod_i \frac{\mathrm{d}y_i}{y_i} \tag{5.1}$$

[10] up to scaling

where $? = I$ if K is wild (resp. $? = II$ if K is tame) and the constant c_p is defined in Lemma 5.4. This notation is motivated by that in [15] and the wild (type I) vs tame (type II) phenomena we see in both of these studies.

Remark 5.1. Similar to the situation in [14, 15], we have that this measure comes from the measure on certain diagonal matrices. First, note that the set of gram matrices:

$$G_w(\{\lambda_i\}) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_d & & & & \\ & & & \lambda_d^{-1} & & & \\ & & & & \ddots & & \\ & & & & & \lambda_1^{-1} & \end{pmatrix}$$

is an orbit of the group $\mathcal{T} \subseteq \mathrm{SL}_{p-1}(\mathbf{R})$ where:

$$\mathcal{T} := \left\{ G_w(\{y_i\}) : y_i = \prod_{j=1}^{\ell} x_j^{2ij-p-2p\left\lfloor \frac{ij}{p} \right\rfloor}, x_i \in \mathbf{R}^\times \right\}^{11}.$$

The measure on this group is the one we see above which induces a measure on space of shapes of wild fields.

Remark 5.2. We saw in (3.1) that the set of Gram matrices of tame fields is obtained by conjugating the wild ones by $\mathcal{C}_t$: specifically we have $\mathcal{G}_{tame} = \mathcal{C}_t \mathcal{G}_{wild} \mathcal{C}_t^T$. If we could get rid of the dependency of $\mathcal{C}_t$ on the field and find a uniform $\mathcal{C}_t$ with this property then we would get that the set of tame Gram matrices is an orbit of the conjugated torus $\mathcal{C}_t \mathcal{T} \mathcal{C}_t^{-1}$.

Then the shape of tame fields would inherit the Haar measure from the conjugated torus $C_t \mathcal{T} C_t^{-1}$. However, we do know that the shape is parametrized by the same ℓ shape parameters, and we define the measure on these matrices to be the measure defined in (5.1).

We now follow a similar exposition to that in [14], recalling that equidistribution is a statement about the weak convergence of a sequence of measures. Note that a sequence of measures $\{\mu_N\}$ on S_I converges weakly to μ_I if for all compactly supported continuous functions, $f \in \mathcal{C}_c(S_I)$,

$$\lim_{N \to \infty} \int_{S_I} f \mathrm{d}\mu_N = \int_{S_I} f \mathrm{d}\mu_I.$$

The measures above, μ_N, are defined by:

$$\mu_N(W) = \frac{\#\{K \in \mathcal{K}_{\text{wild}} : |\Delta(K)| \leq N, \mathrm{Sh}(K) \in W\}}{CN \log^{\ell-1}(N)}.$$

[11] $G(\{\sqrt{y_i}\}) \cdot G(\{1\}) = G(\{y_i\})$

For $x_i \in \mathbf{R}^\times$ and y_i defined above, we let

$$\mathrm{Sh}_I(\{x_i\}) = \begin{pmatrix} y_1 & 0 & & \dots & & 0 \\ 0 & \ddots & & & & \\ & & y_\ell & \ddots & & \vdots \\ \vdots & & \ddots & y_\ell^{-1} & & \\ & & & & \ddots & 0 \\ 0 & \dots & & \dots & 0 & y_1^{-1} \end{pmatrix} \in S_I.$$

Now, for $R_i \in \mathbf{R}_{>0}$ we define

$$\begin{aligned} W_I(R_1, \dots, R_{\ell+1}) &= W_I(\{R_i\}) \\ &= \{\mathrm{Sh}_I(\{x_i\}) : R_1 \le y_1 < y_2 < \cdots < y_\ell < R_{\ell+1}, \text{ and } R_i < y_i\} \end{aligned}$$

and let $\chi_{I\{R_i\}}$ denote its characteristic function, we will show that it is sufficient to test these functions towards showing equidistribution. This is an immediate generalization of Lemma 3.10 in [14] and is also included in [18] so the reader can see either of these references for more details.

Lemma 5.3. *If we have that*

$$\lim_{N\to\infty} \int_{S_I} \chi_{I\{R_i\}} \mathrm{d}\mu_N = \int_{S_I} \chi_{I\{R_i\}} \mathrm{d}\mu_I$$

for all $\{R_i \in \mathbf{R}_{\ge 1} : R_i \le R_{i+1}$ *for all* $i \in \{1, \dots, \ell-1\}\}$ *then* μ_N *converges weakly to* μ_I*.*

Proof. We recall that compactly supported continuous functions on $\mathbf{R}^\ell$ can be approximated above and below by step functions of hypercubes or, in our case, by step functions of sets $W_I(\{R_i\})$. The proof of this follows from the methods in [15] and repeated applications of inclusion and exclusion to show that hypercubes in $\mathbf{R}^\ell$ can be written in terms of the sets $W_I(\{R_i\})$. For full details we refer the reader to Proposition 2.46 of [18]. □

Lemma 5.4. *For* $\{R_i\}$ *as above we have that:*

$$\mu_I(W_I(\{R_i\})) = \frac{1}{c_p \cdot \ell!} H(\{R_i\})$$

where $H(\{R_i\})$ *is a homogeneous polynomial of degree* ℓ *in* $\log(R_i)$*, and*

$$c_p = 2^{\ell-1} p^{\ell-1} h_p^-$$

where h_p^- *is the negative part of the class number of* $\mathbf{Q}(\zeta_p)$*.*

Proof. The measure of this space can be found by defining the change of variables:

$$y_i = \prod_{j=1}^{\ell} x_j^{2ij-p-2p\left\lfloor \frac{ij}{p} \right\rfloor}.$$

Then the jacobian of this change of variables is,

$$J = (y_i \mathrm{d}x_j)_{1 \leq i,j, \leq \ell},$$

whose determinant is equal to

$$c_p = 2^{\ell-1} p^{\ell-1} h_p^-.$$

From this we see that the measure of the subspace is given by:

$$\mu_I(W_I(\{R_i\})) = \frac{1}{c_p} \int_{R_\ell}^{R_{\ell+1}} \int_{R_\ell}^{y_\ell} \cdots \int_{R_1}^{y_2} \frac{1}{y_1 \cdots y_\ell} \mathrm{d}y_1 \cdots \mathrm{d}y_\ell. \qquad \square$$

We will see this measure explicitly in the case of $p = 3$ and $p = 5$, see Example 6.17 and Example 6.18, so we end this section with a calculation of the measure in each case:

Example 5.5. For $p = 3$, $\ell = 1$, and we have:

$$\mu_I(W_I(\{R_1, R_2\})) = \int_{R_1}^{R_2} \frac{\mathrm{d}x_1}{x_1} = \log\left(\frac{R_2}{R_1}\right)$$

Example 5.6. For $p = 5$, $\ell = 2$. The region we want the volume of is given by

$$\mathcal{R}_{\{R_i\}} = \{x_1, x_2 \in \mathbf{R}^\times : R_1 \leq x_1^3 x_2 \leq x_1 x_2^{-3} < R_3, \text{ and } R_2 \leq x_1 x_2^{-3}\}$$

and so we want:

$$\int_{\mathcal{R}_{\{R_i\}}} \frac{\mathrm{d}x_1 \mathrm{d}x_2}{x_1 x_2}.$$

Letting $y_1 = x_1^3 x_2$ and $y_2 = x_1 x_2^{-3}$ we have the Jacobian:

$$\begin{pmatrix} 3x_1^2 x_2 & x_1^3 \\ x_2^{-3} & -3x_1 x_2^{-4} \end{pmatrix}$$

whose determinant is $-10 \cdot \frac{x_1^3}{x_2^3}$. Dividing by $y_1 \cdot y_2$ we have $\frac{-10}{x_1 x_2}$. From this we have

$$\int_{R_2}^{R_3} \int_{R_1}^{y_2} \frac{\mathrm{d}y_1 \mathrm{d}y_2}{y_1 y_2} = 10 \int_{\mathcal{R}_{\{x_i\}}} \frac{\mathrm{d}x_1 \mathrm{d}x_2}{x_1 x_2}$$

which in turn give us:

$$\mu_I(W_I, \{R_1, R_2, R_3\}) = \frac{1}{2 \cdot 5 \cdot 2} \left(\log^2\left(\frac{R_3}{R_1}\right) - \log^2\left(\frac{R_2}{R_1}\right) \right).$$

6. Equidistribution of shapes

This section is dedicated to the proof of Theorem C where we will show that the shapes of pure prime degree fields are equidistributed (in a regularized sense) along ℓ-dimensional subspaces of the space of shapes. In Section 4 we gave a parametrization of these fields using strongly carefree tuples (with some additional congruences) in $\mathbf{Z}^{p-1} \subset \mathbf{R}^n$ so we can transfer questions about counting fields (of bounded discriminant) to questions about counting integral points in some region of $\mathbf{R}^n$. Next, we impose the shape conditions which further restricts the tuples, thereby narrowing the region. Using this we can approximate the number of fields with bounded discriminant and shape in some specified region by counting specific points in this restricted region: to achieve such an approximation we use Davenport's lemma and a strongly-carefree sieve. Recall that Davenport's lemma, [12], states that the number of integral points in a region is approximated by the volume of said region, with an error that comes from the lower dimensional shadows, see Definition 6.2. For convenience we include a slightly more general version of Davenport's lemma, as given in Proposition 2.6 of [6]:

Lemma 6.1. *Let $\mathcal{R}$ be a bounded, semialgebraic multiset in $\mathbf{R}^n$ having multiplicity at most m, which is defined by at most k polynomial inequalities each having degree at most l. Then the number of integral lattice points (counted with multiplicity) contained in $\mathcal{R}$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\overline{\mathcal{R}}), 1\}).$$

where $\mathrm{Vol}(\overline{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implied constant in the second summand depends only on n, m, l, and k.

6.1. Volumes. Let $\mathcal{R}(N, R_1, \ldots, R_{\ell+1})$ be

$$\left\{ (a_1, \ldots, a_{p-1}) \in \mathbf{R}_{>0}^{p-1} : \prod_{i=1}^{p-1} a_i < N, R_1 \leq \lambda_1^p < \cdots < \lambda_\ell^p \leq R_{\ell+1} \right. \\ \left. \text{and } \forall\, i, R_i < \lambda_i^p \right\}$$

where the λ_i are the shape parameters defined in Lemma 4.7. The first step toward counting strongly carefree tuples in this region is to compute the volume of $\mathcal{R}(N, R_1, R_2, \ldots, R_{\ell+1})$ and of its lower-dimensional shadows.

Before we compute any volumes we define a shadow of this region:

Definition 6.2. *For a prime $p \in \mathbf{Z}$ and natural number $d \in \{1, 2, \ldots, p-2\}$ we define a* d-dimensional shadow[12] *of the region $\mathcal{R}(N, R_1, \ldots, R_{\ell+1})$ to be the orthogonal projection of $\mathcal{R}$ onto any d-dimensional coordinate subspace.*

[12]This definition is motivated by Lemma 9 of [3].

We refer to these projections as the lower-dimensional shadows of $\mathcal{R}(N, \{R_i\})$ or $\mathcal{R}$ for simplicity. In order to apply Davenport's lemma we need both the volume of the main region, $\mathcal{R}$, and a bound on the measure of the lower dimensional shadows of $\mathcal{R}$. Towards this we have our first statement:

Proposition 6.3. *For any prime p, the volume of $\mathcal{R}(N, R_1, R_2, \dots, R_{\ell+1})$ is*

$$c \cdot N \log^{\ell-1}(N) \cdot H(R_1, \dots, R_{\ell+1}) + O(N \log(N)^{\ell-2})$$

where $H(R_1, \dots, R_{\ell+1})$ is the homogeneous polynomial in Lemma 5.4 and the implied constant depends only on the $\{R_i\}$.

Proof. To make the volume above a bit more pleasant to compute we define a change of variables from $\{a_i\}$ to $\{x_i\}$:

$$x_i = \begin{cases} \lambda_i^p & \text{for } i \in \{1, \dots, \ell\} \\ a_{i-\ell} \cdot a_{p-i+\ell} & \text{for } i \in \{\ell+1, \dots, p-1\} \end{cases}$$

Note that the Jacobian of this change of variables is given by

$$J = \begin{pmatrix} \frac{\partial x_1}{\partial a_1} & \cdots & \frac{\partial x_1}{\partial a_{p-1}} \\ \vdots & \ddots & \vdots \\ \frac{\partial x_{p-1}}{\partial a_1} & \cdots & \frac{\partial x_{p-1}}{\partial a_{p-1}} \end{pmatrix} \tag{6.1}$$

whose determinant is equal, by Proposition 6.10, to $(\pm 2^{p-2} p^{\ell-1} h_p^-) \cdot \prod_{i=1}^{\ell} x_i$, where h_p^- is the minus part of the class number of $\mathbf{Q}(\zeta_p)$. As above we let $c_p = 2^{\ell-1} p^{\ell-1} h_p^-$.

Now, we have explicit bounds on the first ℓ variables coming from the definition of $\mathcal{R}$, to bound the remaining ℓ variables we simply note that the product of these variables is bounded between 1 and N:

$$1 < x_{\ell+1} \cdots x_{p-1} = a_1 \cdot a_2 \cdots a_{p-1} < N.$$

This gives us the following:

$$\begin{aligned}
&\int_{\mathcal{R}(X,R_1,\dots,R_{p-1})} \mathrm{d}a_1 \dots \mathrm{d}a_{p-1} \\
&= \int_{R_\ell}^{R_{\ell+1}} \int_{R_{\ell-1}}^{x_\ell} \cdots \int_{R_1}^{x_2} \int_1^N \cdots \int_1^{\frac{N}{x_{\ell+1}\cdots x_{p-2}}} \frac{\mathrm{d}x_{p-1}\dots\mathrm{d}x_{\ell+1}\mathrm{d}x_1\dots\mathrm{d}x_\ell}{c_p \cdot x_1 \cdots x_\ell} \\
&= \frac{1}{2^\ell \cdot c_p} \int_{R_\ell}^{R_{\ell+1}} \cdots \int_{R_1}^{x_2} \int_1^N \cdots \int_1^{\frac{N}{x_{\ell+1}\cdots x_{p-3}}} \left(\frac{N}{x_{\ell+1}\cdots x_{p-2}} - 1\right) \\
&\qquad\qquad \times \frac{\mathrm{d}x_{p-2}\dots\mathrm{d}x_{\ell+1}\mathrm{d}x_1\dots\mathrm{d}x_\ell}{x_1\cdots x_\ell} \\
&= \frac{N}{2^\ell \cdot c_p} \int_{R_\ell}^{R_{\ell+1}} \cdots \int_{R_1}^{x_2} \int_1^N \cdots \int_1^{\frac{N}{x_{\ell+1}\cdots x_{p-4}}} \frac{\log\left(\frac{N}{x_{\ell+1}\cdots x_{p-3}}\right)}{x_1\cdots x_\ell \cdot x_{\ell+1}\cdots x_{p-3}} \\
&\qquad\qquad \times \mathrm{d}x_{p-3}\dots\mathrm{d}x_{\ell+1}\mathrm{d}x_1\dots\mathrm{d}x_\ell \\
&\quad - \frac{1}{2^\ell \cdot c_p} \int_{R_\ell}^{R_{\ell+1}} \cdots \int_{R_1}^{x_2} \int_1^N \cdots \int_1^{\frac{N}{x_{\ell+1}\cdots x_{p-4}}} \frac{\mathrm{d}x_{p-2}\dots\mathrm{d}x_{\ell+1}\mathrm{d}x_1\dots\mathrm{d}x_\ell}{x_1\cdots x_\ell}
\end{aligned}$$

We now drop the last line, noting that it will be absorbed into the error $O(N\log(N)^{\ell-2})$. The main term is as follows:

$$\begin{aligned}
&= \frac{N}{2\cdot 2^\ell \cdot c_p} \int_{R_\ell}^{R_{\ell+1}} \cdots \int_{R_1}^{x_2} \int_1^N \cdots \int_1^{\frac{N}{x_{\ell+1}\cdots x_{p-5}}} \frac{\log^2\left(\frac{x_1\cdots x_{p-4}}{N}\right)}{x_1\cdots x_{p-4}} \\
&\qquad\qquad \times \mathrm{d}x_{p-4}\dots\mathrm{d}x_{\ell+1}\mathrm{d}x_1\dots\mathrm{d}x_\ell \\
&= \frac{N}{3!\cdot 2^\ell \cdot c_p} \int_{R_\ell}^{R_{\ell+1}} \cdots \int_{R_1}^{x_2} \int_1^N \cdots \int_1^{\frac{N}{x_{\ell+1}\cdots x_{p-6}}} \frac{\log^3\left(\frac{N}{x_1\cdots x_{p-5}}\right)}{x_1\cdots x_{p-5}} \\
&\qquad\qquad \times \mathrm{d}x_{p-5}\dots\mathrm{d}x_{\ell+1}\mathrm{d}x_1\dots\mathrm{d}x_\ell \\
&\vdots \\
&= \frac{N\log(N)^{\ell-1}}{(\ell-1)!\cdot 2^\ell \cdot c_p} \int_{R_\ell}^{R_{\ell+1}} \int_{R_{\ell-1}}^{x_\ell} \cdots \int_{R_1}^{x_2} \frac{1}{x_1\cdots x_\ell} \mathrm{d}x_1\dots\mathrm{d}x_\ell
\end{aligned}$$

Where the latter integral–together with c_p^{-1}–is the measure, $\mu_?$, whose evaluation is a homogeneous polynomial of degree ℓ in $\{\log(R_i)\}$, see Lemma 5.4. □

Now that we know the volume of the region $\mathcal{R}(N,\{R_i\})$ we need a bound on the volume of the lower dimensional shadows:

Proposition 6.4. *The maximum measure of the lower dimensional shadows of $\mathcal{R}(N,\{R_i\})$ is $\mathcal{O}(N\log^{\ell-2}(N))$.*

First we note that the bounds on the shape parameters can be used to bound the ratios:

$$r_i := \frac{a_i}{a_{p-i}}.$$

Specifically, for all $i \in \{1, \dots, \ell\}$, we have that $1 \leq R_1 < \lambda_i < R_{\ell+1}$ and we can use this to bound each ratio by something of the form:

$$R_1^{\delta_i} < r_i^{u_i} < R_{\ell+1}^{\epsilon_i}$$

where $u_i \in \{-1, 1\}$ and δ_i, ϵ_i are non-zero rational numbers.

Remark 6.5. It is not hard to see that the bounds on the shape parameters impose bounds on these ratios: if, for all $i \in \{1, \dots, \ell\}$, we let $v_i = \log\left(\frac{a_i}{a_{p-i}}\right)$ then we are making a statement about the linear independence of the shape parameters, after applying the logarithm. More explicitly we have a linear map from the $\{v_i\}$ to $\{\log(\lambda_j)\}$ which is represented by the matrix:

$$C_\ell = \left(\left(2ij - p - 2p\left\lfloor \frac{ij}{p} \right\rfloor\right)\right)_{1 \leq i,j \leq \ell}$$

the invertibility of which is a consequence of Proposition 6.10. This shows that from the bounds on the shape parameters we obtain bounds on the ratios, r_i.

Remark 6.6. Each d-dimensional shadow of $\mathcal{R}(N, R_1, \dots, R_{\ell+1})$ is contained in the shadow of the slice of $\mathcal{R}(N, R_1, \dots, R_{\ell+1})$ where the coordinates perpendicular to the shadow are equal to 1. Also when any $a_j = 1$ we obtain constant bounds for a_{p-j} from above. This will allow us to ensure that the region defined below depends on an even number of variables: if the dimension of the shadow is odd then, without loss of generality, we know that at least one variable, a_j, appears without a_{p-j}. As we only care about the hypervolume of the shadows up to a constant, the constant bound on a_j can then be used to exclude this from the region we define above. Doing this for all such a_j we are left to worry only about the pairs (a_i, a_{p-i}) in the shadow.

Example 6.7. When $p = 5$ we have $r_1 = \frac{a_1}{a_4}$ and $r_2 = \frac{a_2}{a_3}$ and, without loss of generality, we have something of the form:

$$R_1 \leq r_1 r_2^3 < r_1^3 r_2^{-1} \leq R_3.$$

In this case we have that

$$R_1^3 < r_1^9 r_2^{-3} \leq R_3^3$$

which we can multiply with the inequality above to gives us that:

$$R_1^4 \leq r_1^{10} < R_3^4$$

or $R_1^{2/5} \leq r_1 < R_3^{2/5}$. Isolating the other ratio we see that:

$$R_1^3 R_3^{-1} \leq r_2^{10} \leq R_1^{-1} R_3^3 \tag{6.2}$$

$$\left(\frac{R_1^3}{R_3}\right)^{1/10} \leq r_2 \leq \left(\frac{R_3^3}{R_1}\right)^{1/10}. \tag{6.3}$$

Now, consider the shadow given by $a_1 a_2 a_3$. Following the strategy from above we know that a_1 is bounded by constants and so to bound this shadow we only need to consider the region defined by:

$$\mathcal{R}_2(N) = \left\{ (a_2, a_3) \in \mathbf{R}^2 \,\middle|\, 1 < a_2 a_3 < N, b_1 < \frac{a_2}{a_3} < B_1 \right\}$$

where b_1 and B_1 are the bounds given in (6.3). Using the change of variables:

$$x_1 = \frac{a_2}{a_3} \qquad\qquad x_2 = \frac{a_2 a_3}{x_1} = a_3^2$$

we have the Jacobian matrix

$$\begin{pmatrix} \frac{1}{a_3} & \frac{-a_2}{a_3^2} \\ 0 & 2a_3 \end{pmatrix}$$

which has determinant 2 and we obtain the following bounds on these new variables:

$$1 < x_1 x_2 < N \qquad\qquad b_1 < x_1 < B_1.$$

Now, the volume of the shadow is approximated by:

$$\begin{aligned} \mathrm{Vol}(R_2(N)) &= \int_{b_1}^{B_1} \int_0^{N/x_1} \frac{1}{2} \mathrm{d}x_1 \mathrm{d}x_2 \\ &= \int_{b_1}^{B_1} \frac{N}{2x_1} \mathrm{d}x_1 \\ &= \frac{N \log\left(\frac{B_1}{b_1}\right)}{2} \\ &= \mathcal{O}(N) \end{aligned}$$

The same can be done with any other shadows which shows that the maximum volume of any lower-dimensional shadow of $\mathcal{R}(N, R_1, R_2, R_3)$ is bounded by $\mathcal{O}(N)$.

Let d be even, $i \in \{1, \ldots, \frac{d}{2}\}$, and define the region

$$\begin{aligned} &\mathcal{R}_d(N, \{b_i, B_i\}) \\ &\qquad := \left\{ (a_1, \ldots, a_d) \in \mathbf{R}^d \,\middle|\, 1 < a_1 \cdots a_d < N, b_i < \frac{a_i}{a_{d+1-i}} < B_i \right\}. \end{aligned}$$

We will show that it is sufficient to consider the volume of such a region when computing the volume of the lower-dimensional shadows. First, we show that:

Lemma 6.8. *The hypervolume of the region $\mathcal{R}_d(N)$ is $\mathcal{O}(N\log^{(d-3)/2}(N))$ and the implied constant depends only on the collection of $\{(b_i, B_i)\}$.*

Proof. The proof will follow the same strategy as Proposition 6.3. We define the following change of variables:

$$\begin{aligned} x_1 &= \frac{a_1}{a_d} \\ x_2 &= \frac{a_2}{a_{d-1}} \\ &\vdots \\ x_{d/2} &= \frac{a_{d/2}}{a_{d/2+1}} \\ x_{d/2+1} &= a_1 \\ x_{d/2+2} &= a_2 \\ &\vdots \\ x_{d-1} &= a_{d/2-1} \\ x_d &= \frac{a_1 \cdot a_2 \cdots a_d}{x_1 \cdot x_2 \cdots x_{d-1}} \end{aligned}$$

The Jacobian determinant of this change of variables is constant and equal to ± 2, this follows by permuting the columns in Lemma 6.13. Then, for $i \in \{1, 3, \ldots, d-1\}$ we have the following bounds: $b_{(i+1)/2} < x_i < B_{(i+1)/2}$. We obtain bounds on the remaining variables using the fact that $1 < x_1 \cdots x_d < N$ and this gives us:

$$\begin{aligned} &\mathrm{Vol}(\mathcal{R}_d(N, \{b_i, B_i\})) \\ &= \int_{b_1}^{B_1} \cdots \int_{b_{d/2}}^{B_{d/2}} \int_{1/\prod_{i=1}^{d/2} x_i}^{N/\prod_{i=1}^{d/2} x_i} \cdots \int_{1/\prod_{i=1}^{d-1} x_i}^{N/\prod_{i=1}^{d-1} x_i} \frac{1}{2} \mathrm{d}x_d \cdots \mathrm{d}x_2 \mathrm{d}x_1 \\ &= \frac{1}{2} \int_{b_1}^{B_1} \cdots \int_{b_{d-1}}^{B_{d-1}} \int_{1/\prod_{i=1}^{d/2} x_i}^{N/\prod_{i=1}^{d/2} x_i} \cdots \int_{1/\prod_{i=1}^{d-2} x_i}^{N/\prod_{i=1}^{d-2} x_i} \frac{N-1}{x_1 \cdots x_{d-1}} \mathrm{d}x_{d-1} \cdots \mathrm{d}x_1 \\ &= \frac{(N-1)\log^{d/2-1}(N)}{2} \int_{b_1}^{B_1} \cdots \int_{b_{d-1}}^{B_{d-1}} \frac{1}{x_1 x_2 \cdots x_{d/2}} \mathrm{d}x_{d/2} \cdots \mathrm{d}x_1 \\ &= \frac{(N-1)\log^{d/2-1}(N)}{2} \prod_{i=1}^{d/2} \log\left(\frac{B_i}{b_i}\right) \\ &= \mathcal{O}(N\log^{d/2-1}(N)). \end{aligned}$$

□

This gives the hypervolume of the region $\mathcal{R}_d(N, \{b_i, B_i\})$ and we use this to prove Proposition 6.4.

Proof of Proposition 6.4. For the region $\mathcal{R}(N, R_1, \dots, R_{\ell+1})$, take any d dimensional shadow. If a_j is in the shadow but a_{p-j} is not then we have constant bounds on a_j and we can drop the dimension of the shadow in consideration by 1: we do this for all a_j until the only variables in the shadow are the pairs (a_j, a_{p-j}). We note that this will only change the error by a constant which will not affect our result. Once this is complete we are considering a region $\mathcal{R}_{d'}(N)$ where d' is even and we have:

$$\mathrm{Vol}(\mathcal{R}_d) = \mathcal{O}(\mathrm{Vol}(\mathcal{R}_{d'})) = \mathcal{O}(N \log^{d'/2-1}(N)).$$

Now, this approximation will increase–by $\log(N)$–each time we add a pair of variables(a_j, a_{p-j}) to the shadow. As the largest, even, d that we could consider is $d = p - 3$ this shows that the maximum volume of any lower dimensional shadow is:

$$\mathcal{O}\Big(N \log(N)^{\frac{p-3}{2}-1}\Big) = \mathcal{O}(N \log(N)^{\ell-2}). \qquad \square$$

Combining Propositions 6.3 and 6.4 we have the following:

Theorem 6.9. *For any prime p, the volume of $\mathcal{R}(N, R_1, R_2, \dots, R_{\ell+1})$ is*

$$\frac{1}{2^\ell(\ell-1)!(c_p \cdot \ell!)} N \log^{\ell-1}(N) \cdot H(R_1, \dots, R_{\ell+1}) + O(N \log(N)^{\ell-2})$$

where $H(R_1, \dots, R_{\ell+1})$ is the homogeneous polynomial in Lemma 5.4 and the implied constant depends only on the $\{R_i\}$.

6.2. Adventure into the land of Jacobian determinants. In this section we prove results about the Jacobian determinants used in the proofs of Proposition 6.3 and Lemma 6.8.

6.2.1. *Jacobian determinant in Proposition 6.3.* Here we prove that the Jacobian determinant, (6.1), is non-zero. We define the change of variables again:

$$x_i = \begin{cases} \lambda_i^p & \text{for } i \in \{1, \dots, \ell\} \\ a_{i-\ell} & \text{for } i \in \{\ell+1, \dots, p-1\} \end{cases}$$

where λ_i are given in Lemma 4.7.

Proposition 6.10. *The Jacobian determinant of this change of variables from $(a_1, a_2, \dots, a_{p-1})$ to $(x_1, x_2, \dots, x_{p-1})$ is equal to:*

$$(\pm 2^{p-2} p^{\ell-1} h_p^-) \cdot \prod_{i=1}^{\ell} x_i.$$

We will prove this proposition by showing that the determinant is equal to a constant times $\prod_{i=1}^{\ell} x_i$ and then, using a result of Carlitz and Olson on Maillet's determinant, [9], we will show that the constant is equal to:

$$\pm 2^{\ell} \cdot \det\left(\left(2ij - p - 2p\left\lfloor \frac{ij}{p} \right\rfloor\right)_{1\leq i,j\leq \ell}\right).$$

Before this we provide a short example, again with $p = 5$:

Example 6.11. We saw, in Example 4.5, that the shape parameters of $K = \mathbf{Q}(\sqrt[5]{m})$ are:

$$\lambda_1 = \left(\frac{a_4^3 a_3}{a_1^3 a_2}\right)^{1/5} \qquad \lambda_2 = \left(\frac{a_4 a_2^3}{a_1 a_3^3}\right)^{1/5}$$

We will, without loss of generality, assume that $\lambda_1 < \lambda_2$ and so $x_1 = \lambda_1^p$ and $x_2 = \lambda_2^p$. Then $x_3 = a_1 a_4$ and

$$x_4 = a_2 a_3$$

The Jacobian of this change of variables is given by:

$$\mathrm{Jac}\left(\frac{\partial x_i}{\partial a_j}\right) = \begin{pmatrix} \frac{-3a_4^3 a_3}{a_1^4 a_2} & \frac{-a_4^3 a_3}{a_1^3 a_2^2} & \frac{a_4^3}{a_1^3 a_2} & \frac{3a_4^2 a_3}{a_1^3 a_2} \\ \frac{-a_4 a_2^3}{a_1^2 a_3^3} & \frac{3a_4 a_2^2}{a_1 a_3^3} & \frac{-3a_4 a_2^3}{a_1 a_3^4} & \frac{a_2^3}{a_1 a_3^3} \\ a_4 & 0 & 0 & a_1 \\ 0 & a_3 & a_2 & 0 \end{pmatrix}$$

And, finally, the determinant is $\left|\mathrm{Jac}\left(\frac{\partial x_i}{\partial a_j}\right)\right| = -40 \cdot \frac{a_4^4 a_2^2}{a_1^4 a_3^2} = 2^3 \cdot 5 \cdot x_1 x_2$.

For sake of the arguments below, we define the coefficient matrix, C_p, of $\mathrm{Jac}\left(\frac{\partial x_i}{\partial a_j}\right)$ to be the matrix obtained by extracting the coefficients of the Jacobian:

$$C_5 = \begin{pmatrix} -3 & -1 & 1 & 3 \\ -1 & 3 & -3 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Note that the top ℓ rows are antisymmetric, meaning the (i,j) entry is minus the $(i, p-j)$ entry. Therefore, adding the j^{th} column to the $(p-j)^{th}$ column, for $j \in \{1, \ldots, \ell\}$, yields the matrix

$$C_5' = \begin{pmatrix} -3 & -1 & 0 & 0 \\ -1 & 3 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 2 & 0 \end{pmatrix}.$$

Then we have that:

$$\begin{aligned}|\det(C_5)| &= |\det(C_5')| \\ &= 2^2 \cdot \det\begin{pmatrix}-3 & -1\\ -1 & 3\end{pmatrix} \\ &= 2^2 \cdot 10 \\ &= 2^2 \cdot c_5 \\ &= \frac{\det\left(\mathrm{Jac}\left(\frac{\partial x_i}{\partial a_j}\right)\right)}{x_1 x_2}\end{aligned}$$

This argument will pass through in general to show that the Jacobian determinant is equal to

$$\det\left(\mathrm{Jac}\left(\frac{\partial x_i}{\partial a_j}\right)\right) = \frac{2^\ell}{x_1 \cdots x_\ell} \cdot \det\left(\left(2ij - p - 2p\left\lfloor \frac{ij}{p}\right\rfloor\right)_{1\le i,j\le \ell}\right). \tag{6.4}$$

Remark 6.12. We believe that when p is replaced by any odd integer n, and one defines a change of variables in a similar way, that the resulting determinant should be non-zero. One difference is that the statement in (6.4) is not true when n is odd and composite. In this case the formula for the determinant of the Jacobian becomes:

$$\begin{aligned}&\det\left(\mathrm{Jac}\left(\frac{\partial x_i}{\partial a_j}\right)\right) \\ &\qquad = 2^\ell \cdot \det\left(\left(2ij - nj - n\left\lfloor \frac{ij}{n}\right\rfloor + n\left\lfloor \frac{(n-i)j}{n}\right\rfloor\right)\right)_{1\le i,j\le \ell}.\end{aligned} \tag{6.5}$$

The result of Carlitz and Olson, [9], is enough to prove our desired claim though there is also a generalized statement for arbitrary odd integers due to Wang, [25], which may be helpful in the general case.

Proof of Proposition 6.10. Note that the change of variables depends on the ordering of the λ_i^p. In general we cannot assume any particular ordering but this does not change the absolute value of the determinant as switching λ_i and λ_j only changes the determinant by a factor of -1. Similarly, switching $x_i = \lambda_i$ with $x_i = \lambda_i^{-1}$ multiplies the determinant by -1. As such, we need only prove this for a particular choice of $\{\lambda_i\}$. We first show that the determinant is a constant times $x_1 \cdots x_\ell$ which will allow us to focus on a more simple matrix, namely the coefficient matrix $\mathcal{C}_p$ which we define below.

The Jacobian determinant of the change of variables is given by:

$$\sum_{\sigma \in S_{p-1}} (\mathrm{sgn}(\sigma)) \cdot \prod_{i=1}^{p-1} J_{i,\sigma(i)}$$

where the product is over elements of the form $J_{i,\sigma(i)} = \frac{\partial x_i}{\partial a_{\sigma(i)}}$. But we also have that x_i is a ratio of the a_j as given in Lemma 4.7 and hence we have the following relationship:

$$J_{i,\sigma(i)} = \frac{\partial x_i}{\partial a_{\sigma(i)}} = c_{\sigma(i)} \frac{x_i}{a_{\sigma(i)}}$$

where $c_{\sigma(i)}$ is a constant, equal to the exponent of $a_{\sigma(i)}$ in x_j. Looking again at the product above we have:

$$\begin{aligned}
\prod_{i=1}^{p-1} J_{i,\sigma(i)} &= \prod_{i=1}^{p-1} \frac{\partial x_i}{\partial a_{\sigma(i)}} \\
&= \prod_{i=1}^{p-1} \frac{c_{\sigma(i)} x_i}{a_{\sigma(i)}} \\
&= \prod_{i=1}^{p-1} c_{\sigma(i)} \frac{x_1 \cdots x_{p-1}}{a_{\sigma(i)}} \\
&= \frac{x_1 \cdots x_{p-1}}{a_1 \cdots a_{p-1}} \prod_{i=1}^{p-1} c_{\sigma(i)} \\
&= x_1 \cdots x_\ell \cdot c_\sigma,
\end{aligned}$$

where the last equality comes from $x_{\ell+1} \cdots x_{p-1} = a_1 \cdots a_{p-1}$. This shows that each term in the sum above is a constant times $x_1 \cdots x_\ell$, and we need only determine the constant:

$$\sum_{\sigma \in S_{p-1}} (\operatorname{sgn}(\sigma) \cdot c_\sigma)$$

The problem then reduces to determining the determinant of the matrix of coefficients, C_p. This matrix is given as follows:

$$C_p(i,j) = \begin{cases} \left(2ij - p - 2p \left\lfloor \frac{ij}{p} \right\rfloor\right) & \text{if } 1 \le i \le \ell \text{ and } 1 \le j \le p-1 \\ 1 & \text{if } \ell + 1 \le i \le p-1 \\ & \quad \text{and } j = i - \ell \text{ or } j = p - i + \ell \\ 0 & \text{otherwise.} \end{cases}$$

Now the matrix C_p is anti-symmetric about the columns when $1 \le i \le \ell$, so $C_p(i,j) = -C_p(i, p-j)$. Adding the $(p-i)^{th}$ column to the i^{th} column yields

$$C_p' = \left(\begin{array}{c|c} C_p(i,j)_{1 \le i,j \le \ell} & 0 \\ \hline I_\ell & N \end{array} \right)$$

where I_ℓ is the $\ell \times \ell$ identity matrix and N is given by:

$$N(i,j) = \begin{cases} 2 & \text{if } i+j = \ell+1 \\ 0 & \text{otherwise} \end{cases}$$

The matrix N has determinant 2^ℓ which shows that

$$\begin{aligned} |\det(C_p)| = |\det(C'_p)| &= 2^\ell \cdot |\det(C_p(i,j)_{1\le i,j\le \ell})| \\ &= 2^\ell \cdot \left| \det\left(\left(2ij - p - 2p \left\lfloor \frac{ij}{p} \right\rfloor \right) \right)_{1\le i,j\le \ell} \right| \end{aligned}$$

What remains is to show that $\det\Big(\Big(2ij-p-2p\Big\lfloor\frac{ij}{p}\Big\rfloor\Big)\Big)_{1\le i,j\le\ell}$ is non-zero. In [9] the authors show that Maillet's determinant is non-zero and equal to $\pm p^{(p-3)/2} h_p^-$. Note that Maillet's determinant, which we denote D_p, is the determinant of the matrix $(R(rs'))$ where $R(r)$ is the least positive residue of r, and s' is such that $ss' \equiv 1 \pmod p$. One step in proving this involves showing that the determinant:

$$D'_p = \det\left(R(rs') - \frac{p}{2} \right) = \frac{-1}{2} D_p.$$

However, since $R(rs') - \frac{p}{2} = rs' - \frac{1}{2} - p\left\lfloor \frac{rs'}{p} \right\rfloor$, we only need to multiply this matrix D'_p by 2 to obtain the matrix above (and apply some number of column swaps which will only change the determinant by a sign). This shows that the determinant of the change of variable matrix is equal to:

$$\begin{aligned} &\pm 2^\ell \cdot \det\left(\left(2ij - p - 2p \left\lfloor \frac{ij}{p} \right\rfloor \right) \right)_{1\le i,j\le \ell} \\ &= \pm 2^\ell \cdot 2^\ell \cdot D'_p \\ &= \pm 2^{p-1} \cdot \frac{1}{2} D_p \\ &= \pm 2^{p-2} p^{\ell-1} h_p^- \end{aligned}$$

as desired. □

6.2.2. ***Jacobian determinant in Lemma 6.8.*** Let d be an even integer and define the following change of variables:

$$x_i = \begin{cases} \frac{a_i}{a_{i+1}} & \text{if } i \text{ is odd} \\ a_{i-1} & \text{if } i \text{ is even and } i \neq d \\ \frac{N}{\prod_{j=1}^{d-1} x_i} & \text{if } i = d \end{cases}.$$

We note that this differs a bit from the change of variables seen in Lemma 6.8 but, as was mentioned in its proof, we can go between these by simply permuting the columns of the matrix we obtain.

Lemma 6.13. *The Jacobian determinant of this change of variables from* $(a_1, a_2, \ldots, a_d)$ *to* $(x_1, x_2, \ldots, x_d)$ *is constant and equal to* 2.

Proof. We stated above that the determinant is constant, by the same argument as seen in the proof of Lemma Proposition 6.10, and therefore that we only need to worry about the coefficients in the Jacobian matrix. The coefficient matrix can be defined recursively as follows:

$$C_2 = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$$

and

$$C_d = \left(\begin{array}{cc|ccc} 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & C_{d-2} & \\ 0 & 0 & & & \\ -1 & 2 & & & \end{array}\right)$$

Since the determinant of $C_2 = 2$, and $\det(C_d) = \det\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \det(C_{d-2}) = \det(C_{d-2})$ we have that $\det C_d = 2$ for all d. □

6.3. Point count. To count integer points in the region, $\mathcal{R}(N, \{R_i\})$ we define its intersection with $\mathcal{L} = \mathbf{Z}^{p-1}$ as

$$\mathcal{R}_{\mathcal{L}}(N, \{R_i\}) := R(N, R_1, \ldots, R_{\ell+1}) \cap \mathcal{L}$$

and using Davenports lemma we obtain the following corollary:

Corollary 6.14. *For* p, $N, R_i \in \mathbf{R}$, *and* $R_1 < R_2 < \cdots < R_{\ell+1}$ *as above we have:*

$$\#\mathcal{R}_{\mathcal{L}}(N, R_1, \ldots, R_{\ell+1}) = \frac{N \log(N)^{\ell-1}}{2^{\ell}(\ell-1)! \cdot c_p \cdot \ell!} H(R_1, \ldots, R_\ell) + O\left(N \log(N)^{\ell-2}\right)$$

where the implied constant in the error term depends on the $\{R_i\}$.

What we really need to count are the integer points in this region which satisfy the infinitely many congruence conditions coming from our strongly carefree condition.

6.3.1. *Point Count/Sieve.* As stated above, we have translated our problem of counting number fields of bounded discriminant and shape restrictions to counting certain strongly carefree tuples in some specific regions. Since we have already computed the volume of the region, and estimated the number of lattice points in said region, we must now apply a strongly carefree sieve.

For this section we will try to avoid using p entirely, and will consider the general case of n-tuples. The strongly carefree condition will impose infinitely many congruence conditions and will correspond to the tuples $(a_1, \ldots, a_n)$ such that (for all primes q) $a_i \not\equiv 0 \pmod{q^2}$ and if $a_i \equiv 0 \pmod{q}$ then there is no other $a_j \equiv 0 \pmod{q}$ for $j \neq i$. These are the squarefree, and relatively prime conditions respectively and this set will be denoted, as above, by $\mathcal{SC}_n$.

We begin by defining the following set:

$$\mathcal{C}_{n,q}^{cf} := \left\{ (a_1, \ldots, a_n) \in \left(\mathbf{Z}/q^2\mathbf{Z}\right)^n_{\neq 0} : \text{ at least two of the } a_i \text{ are } 0 \pmod{q} \right\}$$

This, being part of a cover of the complement of the set that we desire, will play an important role in the application of the elementary sieve and has a particularly nice expression (for a fixed prime q):

$$\#\mathcal{C}_{n,q}^{cf} = \sum_{i=2}^{n} \binom{n}{i} (q-1)^i (q^2-q)^{n-i} \tag{6.6}$$

This is obtained by simply choosing i entries to be $0 \pmod{q}$; noting that for each of the i entries there are $(q-1)$ such values. The other entries only need to avoid multiples of q and whence there are $(q(q-1))$ possibilities for the $n-i$ remaining entries[13]. Letting $\mathcal{C}_{n,q}^{s} := \{(a_1, a_2, \ldots, a_n) \in \mathbf{Z}^n : a_i \equiv 0 \pmod{q^2} \text{ for some } i \in \{1, \ldots, n\}\}$, we define the set:

$$\mathcal{C}_{n,q}^{scf} = \mathcal{C}_{n,q}^{s} \cup \mathcal{C}_{n,q}^{cf}$$

noting that this will gather all tuples (in $\mathbf{Z}/q^2\mathbf{Z}$) which are not squarefree, and not relatively prime with respect to q. We denote the complement of this set in $\mathbf{Z}/q^2\mathbf{Z}$ by$\mathcal{SC}_{n,q}$ and, finally, we note that:

$$\#\mathcal{SC}_{n,q} = (q-1)^n (q^n + nq^{n-1}) \tag{6.7}$$

6.3.2. *q-adic density.* For all $Y \geq 2$ we define the following:

$$n(Y) := \prod_{q \leq Y} q^2$$

and $\mathcal{C}_{n,Y}$ denote the set of congruence conditions, $\mathcal{C}_{q,n}^{scf}$, modulo $n(Y)$ for $1 < q \leq Y$. Letting

$$\mathcal{L}_n(Y) := \{(a_1, a_2, \ldots, a_n) \in \mathbf{Z}^n : (a_1, a_2, \ldots, a_n) \notin \mathcal{C}_{n,Y}\}$$

[13] note we have avoided any entries that are $0 \pmod{q^2}$

we obtain the following q-adic density of $\mathcal{L}_n(Y)$:

$$\begin{aligned}\delta_q(\mathcal{L}_n(Y)) &= \frac{\#\mathcal{SC}_{n,q}}{q^{2n}} \\ &= \frac{(q-1)^n(q+n)q^{n-1}}{q^{2n}} \\ &= \frac{(q-1)^n(q+n)}{q^{n+1}} = \left(1+\frac{n}{q}\right)\left(1-\frac{1}{q}\right)^n \\ &= \frac{q^{n+1}-n^2q^{n-1}+(q+n)\left(\sum_{i=2}^n \binom{n}{i}q^{n-i}(-1)^i\right)}{q^{n+1}} \\ &= 1-\frac{n^2}{q^2}+(q+n)\sum_{i=2}^n \binom{n}{i}q^{-i-1}(-1)^i\end{aligned}$$

Remark 6.15. For what comes next the condition at p needs further consideration. Namely, from the strongly carefree tuples, we need to split the tame fields from the wild ones. Recall that this is a condition on m, and therefore on the tuples, modulo p^2: the pure field is tame iff $m^{p-1} \equiv 1 \pmod{p^2}$. Now, it is clear that this condition is independent of being strongly carefree at p so we need only consider the tuples for which this congruence holds. To that end, and the tuple size being clear, we let

$$\mathcal{SC}_p^{II} = \{(a_1, \ldots, a_{p-1}) \in \mathcal{SC}_p : m^{p-1} \equiv 1 \pmod{p^2}\}$$

and, as the remaining tuples will yield wild fields, we have $\mathcal{SC}_p^I = \mathcal{SC}_p \backslash \mathcal{SC}_p^{II}$. We can think of this as finding an inverse of $\prod_{i=2}^{p-1}(a_i^i)^{p-1}$ modulo p^2. To ensure this product is invertible we need only avoid multiples of p in these $p-2$ coordinates and for any such choice there are $(p-1)$ elements of $\mathbf{Z}/p^2\mathbf{Z}$ such that $\left(\prod_{i=1}^{p-1} a_i^i\right)^{p-1} \equiv 1 \pmod{p^2}$. We therefore obtain the proportion of tame fields:

$$\frac{\#\mathcal{SC}_p^{II}}{\#\mathcal{SC}_p} = \frac{p^{p-2}(p-1)^{p-1}}{(p-1)^{p-1}(p+(p-1))p^{p-2}} = \frac{1}{2p-1}$$

and that of the wild ones:

$$\frac{\#\mathcal{SC}_p^I}{\#\mathcal{SC}_p} = \frac{\#\mathcal{SC}_p - \#\mathcal{SC}_p^{II}}{\#\mathcal{SC}_p} = \frac{2p-2}{2p-1}.$$

6.3.3. ***Application to pure prime degree fields.*** Using the notation above and a standard argument, as in [14], we have the following corollary which will lead us to the main result of this paper.

Corollary 6.16. *For p a fixed prime and $1 < R_1 < R_2 < \cdots < R_{\ell+1}$*

$$\mathcal{R}_{\mathcal{L}_{p-1}(Y)}(N, \{R_i\}) = \frac{\prod_{q \le Y} \delta_q(\mathcal{L}_{p-1}(Y))}{2^\ell (\ell-1)! \cdot \ell! \cdot c_p} N \log(N)^{\ell-1} H(R_1, \ldots, R_{\ell+1}) + O\left(N \log(N)^{\ell-2}\right),$$

where the implied constant in the error term depends on the $\{R_i\}$.

What remains is to show that we may take the limit of Y. This uses one of the basic sieve techniques which appears in many related works, see [13, 14, 18], and whose notation we try to emulate here. Since p is a fixed prime the length of the n-tuple is now $p-1$ so we exclude this from $\mathcal{L}_n(Y)$ and simply write $\mathcal{L}(Y)$. Letting $\mathcal{L}_\infty$ be the set with congruence conditions applied at all primes, we have a naive upper bound

$$\begin{aligned}\limsup_{N\to\infty} \frac{\#\mathcal{R}_{\mathcal{L}_\infty}(N, R_1, \ldots, R_{\ell+1})}{N \log(N)^{\ell-1}} &\le \lim_{Y\to\infty} \lim_{N\to\infty} \frac{\#\mathcal{R}_{\mathcal{L}(Y)}(N, R_1, \ldots, R_{\ell+1})}{N \log(N)^{\ell-1}} \\ &\le c_p^? \prod_{q \le Y} \delta_q(\mathcal{L}(Y)) H(R_1, \ldots, R_{\ell+1})\end{aligned}$$

We now set $\mathcal{W}_q := \{(a_1, \ldots, a_{p-1}) \in \mathbf{Z}^{p-1} : (a_1, \ldots, a_{p-1}) \in \mathcal{C}_q^{scf}\}$, and write:

$$\begin{aligned}&\mathcal{R}_{\mathcal{L}(Y)}(N, R_1, \ldots, R_{\ell+1}) \\ &\qquad \subseteq \mathcal{R}_{\mathcal{L}_\infty}(N, R_1, \ldots, R_{\ell+1}) \cup \bigcup_{q>Y} \mathcal{R}_{\mathcal{W}_q}(N, R_1, \ldots, R_{\ell+1})\end{aligned}$$

This allows us to bound the quantity below as follows:

$$\begin{aligned}&\frac{\#\mathcal{R}_{\mathcal{L}_\infty}(N, R_1, \ldots, R_{\ell+1})}{N \log(N)^{\ell-1}} \\ &\qquad \ge \frac{\mathcal{R}_{\mathcal{L}(Y)}(N, R_1, \ldots, R_{\ell+1})}{N \log(N)^{\ell-1}} - O\left(\sum_{q>Y} \frac{\mathcal{R}_{\mathcal{W}_q}(N, R_1, \ldots, R_{\ell+1})}{N \log(N)^{\ell-1}}\right).\end{aligned} \tag{6.8}$$

By the previous section, we know that

$$\frac{\mathcal{R}_{\mathcal{W}_q}(N, R_1, \ldots, R_{\ell+1})}{N \log(N)^{\ell-1}} = O(q^{-2})$$

which is enough to show that in the limit, as $Y \to \infty$, the big O term on the RHS of (6.8) tends to 0. Taking the lim inf of (6.8), in conjunction with the lim sup above, we have the desired result:

$$\mathcal{R}_{\mathcal{L}_\infty}(N, R_1, \ldots, R_{\ell+1}) = \frac{\prod_q \delta_q(\mathcal{L}_\infty)}{2^\ell (\ell-1)! \cdot \ell! \cdot c_p} N \log(N)^{\ell-1} H(R_1, \ldots, R_{\ell+1}) + o\left(N \log(N)^{\ell-1}\right)$$

In what follows we write δ_q for the q-adic density $\delta_q(\mathcal{L}_\infty)$.

The only thing remaining is to apply this to the case at hand: namely, to count the number of fields whose discriminant is bounded by N and whose shape lies in $\{R_i\}$. The total number of such fields is given by:

$$\begin{aligned}
&\mathcal{N}_p(N,\{R_i\}) \\
&= \frac{1}{2^\ell(\ell-1)!\cdot\ell!\cdot c_p}\prod_q \delta_q N\log(N)^{\ell-1}H(R_1,\dots,R_{\ell+1}) + o\left(N\log(N)^{\ell-1}\right) \\
&= \frac{1}{(\ell-1)!\cdot\ell!\cdot 2^{p-2}p^{\ell-1}h_p^-}\prod_q \delta_q N\log(N)^{\ell-1}H(R_1,\dots,R_{\ell+1}) \\
&\qquad\qquad + o\left(N\log(N)^{\ell-1}\right).
\end{aligned}$$

For wild (type I) fields we have that

$$\Delta(K) = -p^p\prod_{i=1}^{p-1}a_i^{p-1} \implies N = \frac{1}{p}\cdot\left(\frac{X}{p}\right)^{1/(p-1)}$$

and for tame (type II) fields we have

$$\Delta(K) = -p^{p-2}\prod_{i=1}^{p-1}a_i^{p-1} \implies N = \left(\frac{X}{p^{p-2}}\right)^{1/(p-1)}.$$

Using this we can determine the asymptotics for the number of pure prime degree fields of type I (resp. type II) with absolute discriminant bounded by X and shape in $\{R_i\}$:

$$\begin{aligned}
&\mathcal{N}_p^I(X,\{R_i\}) \\
&\qquad = C_i\prod_q \delta_q X^{1/(p-1)}\log(X)^{\ell-1}H(\{R_i\}) + o(X^{1/(p-1)}\log(X)^{\ell-1})
\end{aligned}$$

$$\begin{aligned}
&\mathcal{N}_p^{II}(X,\{R_i\}) \\
&\qquad = C_{ii}\prod_q \delta_q X^{1/(p-1)}\log(X)^{\ell-1}H(\{R_i\}) + o(X^{1/(p-1)}\log(X)^{\ell-1})
\end{aligned}$$

where the constants above are:

$$\begin{aligned}
C_i &= \frac{2p-2}{(\ell-1)!\ell!(2p-1)2^{p-2}p^{\ell+\frac{1}{p-1}}h_p^-(p-1)^{\ell-1}} \\
C_{ii} &= \frac{1}{(\ell-1)!\ell!(2p-1)2^{p-2}p^{\ell-\frac{1}{p-1}}h_p^-(p-1)^{\ell-1}}
\end{aligned}$$

This, together with Lemma 5.3, proves Theorem C: the (regularized) equidistribution of shapes in the family of pure prime degree number fields.

6.4. Examples. We end this section with two examples: first we recover the result of Harron, in [15], and second we state the result in the case of pure quintic fields.

Example 6.17. When $p = 3$ the minus part of the class number is 1, $c_3 = 1$, and we have:

$$\begin{aligned}\mathcal{N}_3^I(X, \{R_1, R_2\}) &= \frac{4}{5 \cdot 2 \cdot 3 \cdot 3^{\frac{1}{2}}} \prod_q \delta_q X^{1/2} H(R_1, R_2) + o(X^{1/2}) \\ &= \frac{2}{15\sqrt{3}} \prod_q \left(1 - \frac{3}{q^2} + \frac{2}{q^3}\right) X^{1/2} \log\left(\frac{R_2}{R_1}\right) + o(X^{1/2}) \\ \mathcal{N}_3^{II}(X, \{R_1, R_2\}) &= \frac{1}{5 \cdot 2 \cdot 3^{\frac{1}{2}}} \prod_q \delta_q X^{1/2} H(R_1, R_2) + o(X^{1/2}) \\ &= \frac{1}{10\sqrt{3}} \prod_q \left(1 - \frac{3}{q^2} + \frac{2}{q^3}\right) X^{1/2} \log\left(\frac{R_2}{R_1}\right) + o(X^{1/2})\end{aligned}$$

Example 6.18. For $p = 5$ the minus part of the class number is again 1, $c_5 = 20$, $\delta_q = \left(1 - \frac{10}{p^2} + \frac{20}{p^3} - \frac{15}{p^4} + \frac{4}{p^5}\right)$ and so

$$\begin{aligned}&\mathcal{N}_5^I(X, \{R_1, R_2, R_3\}) \\ &\quad = \frac{1}{1800\sqrt[4]{5}} \prod_q \delta_q X^{1/4} \log(X) \cdot \left(\log^2\left(\frac{R_3}{R_1}\right) - \log^2\left(\frac{R_2}{R_1}\right)\right) \\ &\qquad\qquad + o(X^{1/4} \log(X))\end{aligned}$$

and

$$\begin{aligned}&\mathcal{N}_5^{II}(X, \{R_1, R_2, R_3\}) \\ &\quad = \frac{1}{2880\sqrt[4]{5^3}} \prod_q \delta_q X^{1/4} \log(X) \cdot \left(\log^2\left(\frac{R_3}{R_1}\right) - \log^2\left(\frac{R_2}{R_1}\right)\right) \\ &\qquad\qquad + o(X^{1/4} \log(X))\end{aligned}$$

7. Pure and F_p fields

In this last section we prove our final theorem, that the pure prime degree number fields are exactly those F_p number fields, with degree $(p-1)$-resolvent equal to $\mathbf{Q}(\zeta_p)$. We begin by discussing the group theoretic prerequisites, defining the group F_p, and defining what exactly we mean by the resolvent field. Once we have the relevant tools and definitions in hand we prove the aforementioned claim which allows us to phrase the above study in the flavor of Malle.

7.1. Group Theory. We first define Frobenius groups in general (following the nice narrative laid out by Terrance Tao, in [23]), and state some well known facts about these groups. We will then define the specific Frobenius group, F_p, to which we refer and state some facts that will be of use for us below.

Definition 7.1. *We call G a Frobenius group if there exists a subgroup H of G such that: $(H \cap gHg^{-1}) = \{1\}$ for all $g \in G \setminus H$. This yields the following decomposition:*

$$G = \bigcup_{gH \in G \setminus H} (gHg^{-1} \setminus \{1\}) \cup J$$

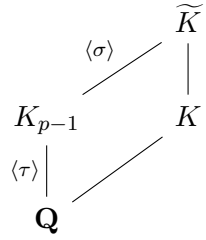
We note that H and J are often referred to as the *Frobenius complement* and *Frobenius kernel*, respectively. The following theorem will then provide the motivation for our definition of F_p that we use throughout:

Theorem 7.2 (Frobenius (1901))**.** *Let G be a Frobenius group with complement H and kernel J. Then $K \lhd G$ and $G = J \rtimes H$.*

This theorem shows us that, in general, Frobenius groups can be realized as a semi direct product of the complement and the kernel and hence we define the Frobenius group, F_p, as follows:

$$F_p := \mathbb{F}_p \rtimes \mathbb{F}_p^{\times} = \langle \sigma, \tau \mid \sigma^p = \tau^{p-1} = 1, \tau\sigma\tau^{-1} = \sigma^g \rangle$$

where g is a primitive root modulo p. As C_p is a normal Sylow p subgroup of F_p, we define the *degree $(p-1)$-resolvent* of $\widetilde{K}$, which we will refer to simply as the resolvent (the degree being clear), to be the unique fixed field of C_p in $\widetilde{K}$. We denote the resolvent of $\widetilde{K}$ by K_{p-1} and we have the following field diagram:

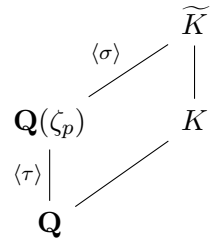


7.2. Pure prime degree fields and F_p fields. With the necessary background covered we now turn our attention to the proof of Theorem D.

Proof.

($\Rightarrow$). If K is pure then $K \cong \mathbf{Q}(\alpha)$ where α is the real root of $f_\alpha(x) = x^p - m$ where $m \in \mathbf{Q}$, $m \neq \pm 1$ and m is p-power free. It is clear that the other roots are $\zeta_p^i \alpha$ for $i \in \{1, \ldots, p-1\}$ hence $\mathbf{Q}(\zeta_p) \subseteq \widetilde{K}$ and so it is the resolvent as desired.

($\Leftarrow$). Consider K, $[K : \mathbf{Q}] = p$, with $\mathrm{Gal}(\widetilde{K}/\mathbf{Q}) \cong F_p \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times$ and resolvent field equal to $\mathbf{Q}(\zeta_p)$. This gives us the following tower:



where $(\mathbf{Z}/p\mathbf{Z})^\times = \langle\tau\rangle$ and $\mathbf{Z}/p\mathbf{Z} = \langle\sigma\rangle$. We will show that $K = \mathbf{Q}\left(\sqrt[p]{m'}\right)$ for some $m' \in \mathbf{Q}$.

Fixing g to be a generator of $(\mathbf{Z}/p\mathbf{Z})^\times$; we have that

$$F_p = \langle \tau, \sigma \mid \tau^{p-1} = \sigma^p = 1 \text{ and } \tau\sigma = \sigma^g\tau \rangle$$

and using this we see that $\tau(\zeta_p) = \zeta_p^g$, $\sigma(\alpha) = \zeta_p\alpha$, $\sigma(\zeta_p) = \zeta_p$. We know by Kummer Theory that $K_p = \mathbf{Q}(\zeta_p)(\sqrt[p]{m})$ for some $m \in \mathbf{Q}(\zeta_p)$, so letting $\alpha = \sqrt[p]{m}$ we can consider the element

$$\theta = \prod_{i=1}^{p-1} \tau^i(\alpha)$$

It is clear that θ is fixed by τ and, as there are no intermediate extensions of $K/\mathbf{Q}$, that $\theta \in K$ or $\theta \in \mathbf{Q}$. Showing that σ acts non-trivially on θ will show that $\theta \in K \setminus \mathbf{Q}$ and hence $K = \mathbf{Q}(\theta)$. The condition that $\tau\sigma = \sigma^g\tau$ is equivalent to $\sigma\tau = \tau\sigma^{g^{-1}}$, where $g^{-1} \in \mathbf{Z}$ is such that $g^{-1}g \equiv 1 \pmod p$, and using this we see that:

$$\sigma\tau^i = \tau^i\sigma^{g^{-i}}$$

Using that σ acts on α via multiplication by ζ_p, and acts trivially on ζ_p, we have that:

$$\begin{aligned}
\sigma\tau^i(\alpha) &= \tau^i\sigma^{g^{-i}}(\alpha) \\
&= \tau^i(\zeta_p^{g^{-i}}\alpha) \\
&= \zeta^{g^i\cdot g^{-i}}\tau^i(\alpha) \\
&= \zeta\tau^i(\alpha)
\end{aligned}$$

and this implies that:

$$\begin{aligned}\sigma(\theta) &= \sigma\left(\prod_{i=1}^{p-1}\tau^i(\alpha)\right)\\ &= \prod_{i=1}^{p-1}\sigma\tau^i(\alpha)\\ &= \prod_{i=1}^{p-1}\zeta\tau^i(\alpha)\\ &= \zeta^{p-1}\theta.\\ &\neq \theta\end{aligned}$$

Thus, letting $m' = \prod_{i=1}^{p-1}\tau^i(m) \in \mathbf{Q}$ we have that $(m') = \theta^p$ and so $K = \mathbf{Q}(\sqrt[p]{m'})$ as desired. □

Remark 7.3. We note that this result is widely stated as fact in the case of cubic number fields where we have the more familiar notion of resolvent field, however we were unable to find a general statement of this result.

7.3. Conclusion. Theorem D allows us to phrase this study in terms of Galois conditions and resolvent fields, rather than pure prime degree number fields. Our desire to reframe the study in this way is partially motivated by the work of Cohen and Thorne who count, for example, D_p extensions with a fixed quadratic resolvent [11]. In turn, it is motivated by Malle's conjecture and all the work that is being done towards counting number fields with prescribed Galois group. Using this, we are able to state all the results of this paper as results about shapes and (regularized) equidistribution of F_p number fields with resolvent field $\mathbf{Q}(\zeta_p)$. Furthermore, the work in this paper can then be used to show that the number of F_p number fields with fixed resolvent $\mathbf{Q}(\zeta_p)$, and discriminant bounded by X, grows like:

$$X^{\frac{1}{p-1}}\log^{p-2}(X)$$

Of course the number of such fields seems quite minimal given that they arise as pure extensions but this begs the question, which the author hopes to answer in future work:

Question. *How does this study compare to those F_p number fields, K, with resolvent $K_{p-1} \neq \mathbf{Q}(\zeta_p)$?*

This is motivated by the result mentioned in (1.1) regarding the asymptotics of cubic number fields with a fixed quadratic resolvent, $K_2 = \mathbf{Q}(\sqrt{d})$. Of course when $d = -3$ we have that $K_2 = \mathbf{Q}(\zeta_3)$ and so what one might expect is that the asymptotic for Frobenius fields with resolvent $K_{p-1} \neq \mathbf{Q}(\zeta_p)$ has fewer log terms.

Acknowledgments

The author would like to thank Rob Harron and Ila Varma for their guidance and support in all aspects of this project. He would also like to thank Kübra Benli, Piper H and Arul Shankar for helpful conversations and Pavel Guerzhoy, Michelle Manes, Khoa Nguyen, Ari Shnidman and Christelle Vincent for their feedback on earlier versions of this work. Special thanks go to Henri Cohen, who answered a question of the author on mathoverflow regarding a determinant formula that appears in the proof of Proposition 6.10, and to Vlad Matei who referred the author to the work of Carlitz and Olson, in [9]. Finally, he would like to thank the referee for a very thorough reading and for many helpful comments, questions, and suggestions.

References

[1] K. Benli, "On the number of pure fields of prime degree", *Colloq. Math.* **153** (2018), no. 1, p. 39-50.
[2] M. Bhargava, "Higher composition laws III: The parametrization of quartic rings", *Ann. Math. (2)* **159** (2004), no. 3, p. 1329-1360.
[3] ———, "The density of discriminants of quartic rings and fields", *Ann. Math. (2)* **162** (2005), no. 2, p. 1031-1063.
[4] ———, "Higher composition laws IV: The parametrization of quintic rings", *Ann. Math. (2)* **167** (2008), no. 1, p. 53-94.
[5] M. Bhargava & P. Harron, "The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields", *Compos. Math.* **152** (2016), no. 6, p. 1111-1120.
[6] M. Bhargava & A. Shankar, "Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves", *Ann. Math. (2)* **181** (2015), no. 1, p. 191-242.
[7] M. Bhargava & A. Shnidman, "On the number of cubic orders of bounded discriminant having automorphism group C_3, and related problems", *Algebra Number Theory* **8** (2014), no. 1, p. 53-88.
[8] W. Bolanõs & G. Mantilla-Soler, "The trace form over cyclic number fields", *Can. J. Math.* **73** (2021), no. 4, p. 947-969.
[9] L. Carlitz & F. R. Olson, "Maillet's determinant", *Proc. Am. Math. Soc.* **6** (1955), p. 265-269.
[10] H. Cohen & A. Morra, "Counting cubic extensions with given quadratic resolvent", *J. Algebra* **325** (2011), no. 1, p. 461-478.
[11] H. Cohen & F. Thorne, "On D_ℓ-extensions of odd prime degree ℓ", *Proc. Lond. Math. Soc.* **121** (2020), no. 5, p. 1171-1206.
[12] H. Davenport, "On a principle of Lipschitz", *J. Lond. Math. Soc.* **26** (1951), p. 179-183.
[13] H. Davenport & H. Heilbronn, "On the density of discriminants of cubic fields. II", *Proc. R. Soc. Lond., Ser. A* **322** (1971), no. 1551, p. 405-420.
[14] P. H & R. Harron, "The shapes of galois quartic fields", *Trans. Am. Math. Soc.* **373** (2020), no. 10, p. 7109-7152.
[15] R. Harron, "The shapes of pure cubic fields", *Proc. Am. Math. Soc.* **145** (2017), no. 2, p. 509-524.
[16] ———, "Equidistribution of shapes of complex cubic fields of fixed quadratic resolvent", *Algebra Number Theory* **15** (2021), no. 5, p. 1095-1125.
[17] R. Harron, E. Holmes & I. Varma, "Shapes of sextic fields and log-terms in Malle's conjecture", in preparation, 2025.

[18] J. Hassan, "On shapes of multiquadratic extensions", PhD Thesis, University of Hawai'i, Manoa, USA, 2019.
[19] A. Jakhar & N. Sangwa, "Integral Basis Of Pure Prime Degree Number Fields", *Indian J. Pure Appl. Math.* **50** (2019), p. 309-314.
[20] J. Klüners, "A counter example to Malle's conjecture on the asymptotics of discriminants", *C. R. Math.* **340** (2005), no. 6, p. 411-414.
[21] G. Malle, "On the distribution of Galois groups", *J. Number Theory* **92** (2002), no. 2, p. 315-322.
[22] G. Mantilla-Soler & M. Monsurrò, "The Shape of $\mathbb{Z}/\ell\mathbb{Z}$-number fields", *Ramanujan J.* **39** (2016), no. 3, p. 451-463.
[23] T. Tao, "The theorems of Frobenius and Suzuki on finite groups", retrieved from `https://terrytao.wordpress.com/2013/04/12`.
[24] D. C. Terr, "The distribution of shapes of cubic orders", PhD Thesis, University of California, Berkeley, USA, 1997.
[25] K. Wang, "On Maillet determinant", *J. Number Theory* **18** (1984), no. 3, p. 306-312.

Erik Holmes
40 St. George Street, Room 6290,
Toronto, ON M5S 2E4, Canada
E-mail: `eholmes@math.toronto.edu`
URL: `http://www.erikholmesmath.com`