Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces

Manjul Bhargava, Arul Shankar, and Xiaoheng Wang

June 26, 2017

Abstract

We develop geometry-of-numbers methods to count orbits in prehomogeneous vector spaces having bounded invariants over any global field. As our primary example, we apply these techniques to determine the density of discriminants of field extensions of degree at most 5 over any base global field F.

1 Introduction

sec:intro

In recent years, there have been a number of problems in arithmetic statistics that have been solved by developing suitable geometry-of-numbers techniques to count integral orbits of a representation of an algebraic group on a vector space defined over $\mathbb{Z}$. These methods have been applied, e.g., to determine the densities of discriminants of number field extensions of $\mathbb{Q}$ of small degree, to establish new cases of the Cohen–Lenstra–Martinet heuristics for class groups, to bound the average rank of elliptic curves over $\mathbb{Q}$, and to show that most hyperelliptic curves over $\mathbb{Q}$ have few rational points (see, e.g., [6, 7], [9]–[24], [36], [39], [42], [46] for these and further examples). The representations that have so far been the most useful for the purpose fall into two categories, namely, prehomogeneous representations having one relative invariant, and coregular representations having at least two relative invariants, with the former parametrizing primarily field extensions and related objects, and the latter parametrizing primarily algebraic curves together with additional data.

In this series of two articles, our purpose is to generalize the aforementioned counting methods from the geometry of numbers so that they may be applied over an arbitrary global number or function field. In this first article, we concentrate on the case of counting integral orbits in a prehomogeneous vector space. Our primary application is the determination of the density of discriminants of field extensions of degree less than or equal to 5 of any given global field.

Let F denote a global number or function field. A fundamental problem in arithmetic statistics is to determine the densities of discriminants of field extensions of F having a fixed degree-n over F. The case of $n = 2$ when $F = \mathbb{Q}$ (and the case of $n = 1$ for all F!) are trivial. When $n = 3$, even the case $F = \mathbb{Q}$ is highly nontrivial and is a celebrated result of Davenport–Heilbronn [30]. Surprisingly, even the case $n = 2$ is nontrivial for more general F and is a result of Datskovsky–Wright [28], who also settle the case of $n = 3$ for general global fields F having characteristic not 2 or 3. The cases $n = 4$ and 5 for $F = \mathbb{Q}$ were carried out in [6, 7].

Let L be any field extension of F of finite degree. The norm of the relative discriminant of L over F is given by the local product

$$N(\mathrm{Disc}(L/F)) := \prod_{\mathfrak{p}\notin M_\infty}\prod_{w|\mathfrak{p}} |\mathrm{Disc}(L_w/F_\mathfrak{p})|_\mathfrak{p}^{-1}, \qquad (1)$$ eqnormdisc

where M_∞ denotes the set of archimedean places of F, $|\cdot|_\mathfrak{p}$ denotes the normalized absolute value at $\mathfrak{p}$, and $F_\mathfrak{p}$ and L_w respectively denote the completion of F at $\mathfrak{p}$ and the completion of L at w. When F is a function field, M_∞ is empty.

Our main theorem determines the number of isomorphism classes of field extensions L of F of degree at most 5 having bounded relative discriminant:

thmainfield **Theorem 1.** *For any $n = 2, 3, 4$ or 5, we let $N_n(F, X)$ denote the number of isomorphism classes of degree-n field extensions L of F weighted by $(\#\mathrm{Aut}(L/F))^{-1}$, whose normal closure over F has full Galois group S_n, such that the norm of the relative discriminant of L over F is at most X if F is a number field, and is equal to X if F is a function field. Let $q(n, k)$ denote the number of partitions of n into at most k parts.*

(a) *If F is a number field with r_1 real embeddings and $2r_2$ complex embeddings, then*

$$\lim_{X\to\infty} \frac{N_n(F,X)}{X} = \frac{1}{2}\operatorname*{Res}_{s=1}\zeta_F(s)\left(\frac{\#S_n[2]}{n!}\right)^{r_1}\left(\frac{1}{n!}\right)^{r_2}\prod_{\mathfrak{p}\notin M_\infty}\left(\sum_{k=0}^{n}\frac{q(k,n-k)-q(k-1,n-k+1)}{\mathbf{N}\,\mathfrak{p}^k}\right). \tag{2}$$ eq: numberfieldcount

(b) *If F is a function field with field of constants $\mathbb{F}_q$, then*

$$\lim_{m\to\infty} \frac{N_n(F,q^{2m})}{q^{2m}} = (\log q)\operatorname*{Res}_{s=1}\zeta_F(s)\prod_{\mathfrak{p}}\left(\sum_{k=0}^{n}\frac{q(k,n-k)-q(k-1,n-k+1)}{\mathbf{N}\,\mathfrak{p}^k}\right). \tag{3}$$ eq: functionfieldcount

Here $S_n[2]$ denotes the number of elements of order dividing 2 in the symmetric group on n letters. We remark that the weight $(\#\mathrm{Aut}(L/F))^{-1}$ is equal to 1 for $n \geq 3$ and is $1/2$ for $n = 2$. The inclusion of these weights yields a statement of Theorem 1 that is uniform in n. We note that Theorem 1 is new even for $n = 2$ when F has characteristic 2 or 3. We note that Theorem 1(a) proves [5, Conjecture A] for $n \leq 5$. We conjecture that both parts of Theorem 1 hold for all n.

For any global field K, one may define its *absolute discriminant* D_K as follows. If K is a number field, then D_K is the absolute value of the discriminant of K viewed as an extension of $\mathbb{Q}$. If K is the function field of a smooth projective and geometrically connected curve $\mathcal{C}$ over $\mathbb{F}_q$, then $D_K = q^{2g-2}$ where g is the genus of $\mathcal{C}$. The norm of the relative discriminant of L over F is related to the absolute discriminants of L and F by the following formula ([34]):

$$D_L/D_F^{[L:F]} = N(\mathrm{Disc}(L/F)).$$

Therefore, the version of Theorem 1 where we instead order degree-n extensions of F by absolute discriminant is a trivial consequence of Theorem 1.

We will actually prove much more general versions of Theorem 1. First, we count field extensions of F of degree n satisfying any collection of local conditions at finitely many places. In fact, we will even allow for certain collections of local conditions at infinitely many places. For each place $\mathfrak{p}$ of F, let $\Sigma_\mathfrak{p}$ be a set of isomorphism classes of étale algebras of degree n over $F_\mathfrak{p}$. We say that the collection $(\Sigma_\mathfrak{p})$ is *acceptable* if, for all but finitely many $\mathfrak{p}$, the set $\Sigma_\mathfrak{p}$ contains all étale algebras of degree n over $F_\mathfrak{p}$ that are unramified or have splitting type $(1^2\tau)$ where τ is an unramified splitting type of dimension $n-2$. Note when the characteristic of F is not 2, one of these two splitting possibilities will happen if the discriminant is squarefree. We have the following asyptotic for the total number of isomorphism classes of extensions L over F of degree n of bounded relative discriminant whose local specification lies in $(\Sigma_\mathfrak{p})$, i.e., $L \otimes F_\mathfrak{p} \in \Sigma_\mathfrak{p}$ for all $\mathfrak{p}$.

thmainfield2 **Theorem 2.** *Let $n = 2, 3, 4$, or 5. Let $\Sigma = (\Sigma_\mathfrak{p})$ be an acceptable collection of local specifications for degree-n extensions of F. Let $N_{n,\Sigma}(F, X)$ denote the number of degree-n field extensions L with local specifications in Σ, weighted by $(\#\mathrm{Aut}(L/F))^{-1}$, whose normal closure over F has full Galois group S_n, such that the norm of the relative discriminant of L over F is at most X if F is a number field, and is equal to X if F is a function field. Then*

$$\lim_{X\to\infty}\frac{N_{n,\Sigma}(F,X)}{X} = c\operatorname*{Res}_{s=1}\zeta_F(s)\prod_{\mathfrak{p}} m_\mathfrak{p}(\Sigma_\mathfrak{p}), \tag{4}$$ eq: combinedcount

where the constant c is $\frac{1}{2}$ if F is a number field and $\log q$ if F is a function field, and where

$$m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = \begin{cases} \dfrac{N\mathfrak{p}-1}{N\mathfrak{p}} \displaystyle\sum_{K\in\Sigma_{\mathfrak{p}}} \frac{|\mathrm{Disc}(K/F_{\mathfrak{p}})|_{\mathfrak{p}}}{\#\mathrm{Aut}(K/F_{\mathfrak{p}})} & \text{if } \mathfrak{p}\notin M_\infty, \\ \displaystyle\sum_{K\in\Sigma_{\mathfrak{p}}} \frac{1}{\#\mathrm{Aut}(K/F_{\mathfrak{p}})} & \text{if } \mathfrak{p}\in M_\infty. \end{cases}$$

When F is a function field, X only runs through the possible norms of relative discriminants in the above limit.

If, for every $\mathfrak{p}$, the set $\Sigma_{\mathfrak{p}}$ consists of all étale extensions of degree n of $F_{\mathfrak{p}}$, then the local masses $m_{\mathfrak{p}} = m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})$ have been computed in [5], and Theorem 2 reduces to Theorem 1. Thus Theorem 2 gives an interpretation of the constants appearing in the asymptotics in Theorem 1 in terms of local masses. Theorem 2 also yields the density of discriminants of degree-n extensions having squarefree discriminant.

Theorem 2 can be used to prove a complement to the Chebotarev density theorem. If F is a global field, and L is an S_n-extension of F unramified at a finite prime $\mathfrak{p}$ of F, then the Artin symbol at p for the Galois closure of L over F is defined as a conjugacy class in S_n. The Chebotarev density theorem asserts that for fixed L and varying $\mathfrak{p}$, the value of the corresponding Artin symbol is equidistributed amongst the conjugacy classes of S_n, where each class is weighted by its size. We prove the analogous result for fixed $\mathfrak{p}$ and varying L.

Theorem 3. *Let F be a global field and let $\mathfrak{p}$ be a finite prime of F. For $n = 2$, 3, 4, or 5, let $\Sigma = (\Sigma_{\mathfrak{p}})$ be an acceptable collection of local specifications for degree-n extensions of F such that $\Sigma_{\mathfrak{p}}$ consists of all unramified degree-n étale extensions of $F_{\mathfrak{p}}$. Then, as L varies over degree-n field extensions with local specifications in Σ whose Galois closure over F have Galois group S_n, the corresponding Artin symbol at $\mathfrak{p}$ is equidistributed across the conjugacy classes of S_n, where each conjugacy class is weighted by its size.*

We prove a further generalization of Theorem 2. Let Σ denote again any acceptable collection of local specifications of degree-n extensions of F, and let S be any nonempty finite set of places of F containing M_∞. Define the relative S-discriminant $\mathrm{Disc}_S(L/F)$ of an extension L of F in the usual way. Then the norm of $\mathrm{Disc}_S(L/F)$ is given by

$$N(\mathrm{Disc}_S(L/F)) := \prod_{\mathfrak{p}\notin S}\prod_{w|\mathfrak{p}} |\mathrm{Disc}(L_w/F_{\mathfrak{p}})|_{\mathfrak{p}}^{-1}. \tag{5}$$
eqnormdiscS

We prove:

thmainfieldS **Theorem 4.** *Let $n = 2$, 3, 4, or 5. Let $\Sigma = (\Sigma_{\mathfrak{p}})$ be an acceptable collection of local specifications for degree-n extensions of F. Let S be a nonempty finite set of places of F containing M_∞. Let $N_{n,\Sigma,S}(F,X)$ denote the number of degree-n field extensions L with local specifications in Σ, weighted by $(\#\mathrm{Aut}(L/F))^{-1}$, whose normal closure over F has full Galois group S_n, such that the norm of the relative S-discriminant of L over F is at most X if F is a number field, and is equal to X if F is a function field. Then*

$$\lim_{X\to\infty}\frac{N_{n,\Sigma,S}(F,X)}{X} = c\,\mathrm{Res}_{s=1}\,\zeta_{F,S}(s)\prod_{\mathfrak{p}} m_{\mathfrak{p},S}(\Sigma_{\mathfrak{p}}), \tag{6}$$
eq: combinedcount2

where $\zeta_{F,S}(s) = \prod_{\mathfrak{p}\notin S}(1-(N\mathfrak{p})^{-s})^{-1}$ is the partial zeta function and the constant c is $\frac{1}{2}$ if F is a number field and $\log q$ if F is a function field, and where

$$m_{\mathfrak{p},S}(\Sigma_{\mathfrak{p}}) = \begin{cases} \dfrac{N\mathfrak{p}-1}{N\mathfrak{p}} \displaystyle\sum_{K\in\Sigma_{\mathfrak{p}}} \frac{|\mathrm{Disc}(K/F_{\mathfrak{p}})|_{\mathfrak{p}}}{\#\mathrm{Aut}(K/F_{\mathfrak{p}})} & \text{if } \mathfrak{p}\notin S, \\ \displaystyle\sum_{K\in\Sigma_{\mathfrak{p}}} \frac{1}{\#\mathrm{Aut}(K/F_{\mathfrak{p}})} & \text{if } \mathfrak{p}\in S. \end{cases} \tag{7}$$
eq: localmassold

When F is a function field, X only runs through the possible norms of relative S-discriminants in the above limit.

We will use Theorem 4 to prove Theorem 2 (and hence Theorem 1). When F is a number field and $S = M_\infty$, Theorem 4 reduces to Theorem 2. When F is the function field of a smooth projective and geometrically connected curve $\mathcal{C}$ over $\mathbb{F}_q$, we set S to be any nonempty finite set of closed points and use Theorem 4 to count the number of degree-n extensions L, or equivalently, degree-n covers $\mathcal{C}'$ of $\mathcal{C}$, having a fixed genus and prescribed splitting/ramification behavior at the chosen points; we then sum over all the possible splitting/ramification behaviors at these points to obtain Theorem 2. Theorem 4, with S taken to be the union of M_∞ and all the places above 2, also allows a new, clean proof of Theorems 1 and 2 via geometry of numbers when F is a number field and $n = 2$.

Let $\mathcal{O}_S$ denote the ring of S-integers in F. In the case of function fields, $\mathcal{O}_S$ is the ring of regular functions on the affine curve obtained by removing the closed points in S. For any degree-n extension L of F, the integral closure $\mathcal{O}_{L,S}$ of $\mathcal{O}_S$ in L is a projective module over $\mathcal{O}_S$ of rank n. The structure theory of projective modules over a Dedekind domain [37, Theorem 1.6] says that $\mathcal{O}_{L,S} \simeq \mathcal{O}_S^{n-1} \times I$ as $\mathcal{O}_S$-modules for some fractional ideal I of $\mathcal{O}_S$. The ideal class of I is called the *S-Steinitz class* of L. As a byproduct of the proofs of Theorems 1 and 4, we obtain the following equidistribution result.

thm: equidistribution **Theorem 5.** *Let F be a global field. Let S be a nonempty finite set places of F containing M_∞. For any $n = 2$, 3, 4 or 5, let $\Sigma = (\Sigma_\mathfrak{p})$ be an acceptable collection of local specifications for degree-n extensions of F. Then the S-Steinitz classes of degree-n field extensions of F with local specifications in Σ, whose normal closure has full Galois group S_n, are equidistributed in the class group of $\mathcal{O}_S$.*

The result above was proven in the cases $n = 2$ or 3 and $S = M_\infty$ for the full family of degree-n field extensions of F by Kable and Wright [35].

The cases $n = 3$ and $n = 4$ of Theorems 1 and 2 yield results on the average sizes of the 3-torsion subgroups of the relative class groups of quadratic extensions of F and the 2-torsion subgroups of the relative class groups of cubic extensions of F. For a finite extension L/F, recall that the relative class group $\mathrm{Cl}(L/F)$ is the kernel of the relative norm map $N_{L/F} : \mathrm{Cl}(L) \to \mathrm{Cl}(F)$ from the class group of L to the class group of F. Instead taking the kernel of the relative norm map between the narrow class groups of L and F yields the relative narrow class group $\mathrm{Cl}^+(L/F)$. For a prime p, we let $h_p(L/F)$ and $h_p^+(L/F)$ denote the sizes of the p-torsion subgroups of $\mathrm{Cl}(L/F)$ and $\mathrm{Cl}^+(L/F)$, respectively. To state these theorems, we need to introduce some additional notation. Let F be a global field, and let $\Sigma = (\Sigma_\mathfrak{p})$ be an acceptable set of local specifications for degree-n extensions of F. We say that Σ is *archimedeally pure* if for every $\mathfrak{p} \in M_\infty$, the set $\Sigma_\mathfrak{p}$ consists of a single element. For $n = 2$ and $n = 3$, we define the quantities $\alpha_n(\Sigma)$ as follows:

$$\alpha_2(\Sigma) := \#\{\mathfrak{p} : F_\mathfrak{p} = \mathbb{R};\ \Sigma_\mathfrak{p} = \{\mathbb{R}^2\}\}; \quad \alpha_3(\Sigma) := \#\{\mathfrak{p} : F_\mathfrak{p} = \mathbb{R};\ \Sigma_\mathfrak{p} = \{\mathbb{R}^3\}\}. \tag{8}$$ eqalphapure

If F is a function field, then $\alpha_n(\Sigma) = 0$. We have the following result:

thclassgps **Theorem 6.** *Let $n = 2$ or 3, and let F be a fixed global field. If F is a number field, we denote the number of real completions of F by r_1 and the number of conjugate pairs of complex completions of F by r_2. If F is a function field, we set $r_1 = r_2 = 0$. Let Σ be an acceptable archimedially pure collection of local specifications for degree-n extensions of F. Let $S_{n,\Sigma}(F,X)$ denote the set of degree-n field extensions L with local specifications in Σ, whose normal closure over F has full Galois group S_n, such that the norm of the relative discriminant of L over F is at most X if F is a number field, and is equal to X if F is a function field. Then*

(a) *If $n = 2$, then*

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{L\in S_{2,\Sigma}(F,X)} h_3(L/F)}{\displaystyle\sum_{L\in S_{2,\Sigma}(F,X)} 1} = 1 + 3^{-r_2-\alpha_2(\Sigma)} .$$

(b) *If $n=3$, then*

$$\lim_{X\to\infty}\frac{\displaystyle\sum_{L\in S_{3,\Sigma}(F,X)} h_2(L/F)}{\displaystyle\sum_{L\in S_{3,\Sigma}(F,X)} 1} \;=\; 1+2^{-r_1-2r_2-\alpha_3(\Sigma)};$$

$$\lim_{X\to\infty}\frac{\displaystyle\sum_{L\in S_{3,\Sigma}(F,X)} h_2^+(L/F)}{\displaystyle\sum_{L\in S_{3,\Sigma}(F,X)} 1} \;=\; 1+2^{-r_1-2r_2+\alpha_3(\Sigma)}.$$

When $F=\mathbb{Q}$, Part (a) of the above theorem is a result of Davenport–Heilbronn [30] and Part (b) is proved in [6]. For general global fields F having characteristic not 2 or 3, Part (a), for the full family of quadratic fields, is due to Datskovsky–Wright [28].

Finally, we explore the average number of certain unramified *nonabelian* extensions of quadratic extensions of a global field F. More precisely, given finite groups $G\subset G'$ and a quadratic extension L of F, we say that K is a (G,G')-extension of L if K is Galois over L with Galois group G, and the Galois closure of K over F has Galois group G'. The average number of (G,G')-extensions of quadratic fields over $\mathbb{Q}$, for $(G,G')=(A_n,S_n)$, $(G,G')=(S_n,S_n\times C_2)$ for $n=3,4,5$, were determined in [8]. Here, we prove the analogous results for acceptable families of quadratic extensions of global fields F.

thurna **Theorem 7.** *Let F be a fixed global field. If F is a number field, we denote the number of real completions of F by r_1 and the number of conjugate pairs of complex completions of F by r_2. If F is a function field, we set $r_1=r_2=0$. Let Σ be an acceptable archimedially pure collection of local specifications for quadratic extensions of F. For $n=3$, 4, or 5, let $E_\Sigma(G,G')$ denote the average number of unramified (G,G')-extensions of quadratic extensions L of F having local specifications in Σ, where these fields L are ordered by the norm of their relative discriminant over F. Then*

$$\text{(a)}\quad E_\Sigma(A_n,S_n) \;=\; \frac{1}{2}\cdot\Big(\frac{2}{n!}\Big)^{r_2+\alpha_2(\Sigma)}\cdot\Big(\frac{1}{(n-2)!}\Big)^{r_1-\alpha_2(\Sigma)};$$

$$\text{(b)}\quad E_\Sigma(S_n,S_n\times C_2) \;=\; \infty.$$

Note that the average values in Theorems 6 and 7 do *not* change with local conditions imposed at finite places. The reason we have restricted to archimedially pure local specifications is that the averages *do* depend on local specifications at infinite places.

Our proofs of these results extend the geometry-of-numbers techniques developed in [30, 6, 7] so that they may be applied over arbitrary global fields. More precisely, we consider prehomogeneous representations V_n of split (over $\mathbb{Z}$) reductive groups G_n for $2\le n\le 5$ such that the $G_n(F)$-orbits of $V_n(F)$ of nonzero discriminant parametrize degree-n étale extensions of F, with the exception in the case $n=2$ and F has characteristic 2 where the group G_2 is non-reductive. These representations first arose in a unified context in the work of Sato–Kimura [40], and the connection with field extensions was first studied systematically in the work of Wright–Yukie [52]. The integral orbits of these representations were classified in [31, 2, 3], and the rational orbits were then counted using this classification of integral orbits via suitable geometry-of-numbers arguments, in [30, 6, 7]. In this paper, it is these latter parametrization and counting methods that we aim to extend to general base fields.

One key difference in working over an arbitarary global field F rather than $\mathbb{Q}$ is that not all $\mathcal{O}_S$-modules are free. In these cases, it is no longer sufficient to consider just the S-integral orbits $G_n(\mathcal{O}_S)\backslash V_n(\mathcal{O}_S)$ to parametrize degree-n extensions of $\mathcal{O}_S$. The parametrization of ring extensions of degrees up to 4 over an arbitirary base is due to Wood [50] [49], and this parametrization could be used to prove our main theorems in these cases. However, we use a different approach and instead consider, for each ideal class β of $\mathcal{O}_S$, orbits $\Gamma_\beta\backslash\mathcal{L}_\beta^{\max}$, where Γ_β is a subgroup of $G_n(F)$ commensurable with $G_n(\mathcal{O}_S)$ and $\mathcal{L}_\beta^{\max}$ is a Γ_β-invariant subset of an additive subgroup $\mathcal{L}_\beta$ of $V_n(F)$ commensurable with $V_n(\mathcal{O}_S)$. The subset $\mathcal{L}_\beta^{\max}$ of $\mathcal{L}_\beta$ is defined by congruence conditions at every prime $\mathfrak{p}$ of $\mathcal{O}_S$. These

Γ_β-orbits in $\mathcal{L}_\beta^{\max}$ are then shown to correspond to S_n-extensions whose S-Steinitz class is β. Our approach works uniformly for all degrees $n \leq 5$.

To count the number of Γ_β-orbits in $\mathcal{L}_\beta$, we view $\mathcal{L}_\beta$ as a lattice in $V_n(F_S)$ where $F_S = \prod_{\mathfrak{p}\in S} F_\mathfrak{p}$. We construct a fundamental domain R for the action of Γ_β on $V_n(F_S)$, so that the set of $\mathcal{L}_\beta$-points in this fundamental domain will be in bijection with the set of Γ_β-orbits in $\mathcal{L}_\beta$. We then wish to obtain asymptotics for the number of these orbits of bounded size by computing the volume of the subset of the fundamental domain of bounded size. This is much easier when the relevant subset of the fundamental domain is bounded, which is true only in the case $n = 2$. When $n = 3, 4, 5$, the fundamental domains contain cusps that go off to infinity and we show that the number of points in these cusps corresponding to S_n-extensions of F is negligible. When $n = 3$, it turns out no points in the cusp region correspond to S_n-extensions. When $n = 4$, there are two cuspidal regions that contain points corresponding to S_n-extensions, and when $n = 5$, there are hundreds of such cusps! We will reduce this cusp analysis to the verification of certain combinatorial conditions on the characters of the maximal torus of the derived subgroup of G_n that we prove hold over a general global field if and only if they hold over $\mathbb{Q}$ (using the fact that G_n is split over $\mathbb{Q}$). Since these conditions have been checked over $\mathbb{Q}$ in [30, 6, 7], it follows that these conditions hold over arbitrary global fields.

To obtain the number of Γ_β-orbits in $\mathcal{L}_\beta^{\max}$ from the number of Γ_β-orbits in $\mathcal{L}_\beta$, we impose congruence conditions at every prime ideal $\mathfrak{p}$ of $\mathcal{O}_S$ by multiplying together density functions at each $\mathfrak{p}$. Since an infinite number of conditions are imposed, a uniformity estimate on the error term is required. For $n = 2$, this is elementary. For $n = 3, 4, 5$, such a uniformity estimate over $\mathbb{Q}$ has been established in [8] and, as we will see, only some mild modifications are required to generalize this estimate to arbitrary global fields.

Finally, we must compute the volumes of some subsets of $V_n(F_S)$ and $V_n(F_\mathfrak{p})$ for $\mathfrak{p} \notin S$. We use a Jacobian change of variable formula to transfer these volume computations to G_n. Once we multiply all the local volumes together and sum over the S-Steinitz classes, we find that we obtain essentially the Tamagawa number of G_n, which in all our cases turns out to be 1. This completes the proof of Theorem 4, and thus also of Theorems 1 and 2.

This article is organized as follows. In Section 2, we set up some notations, recall the formula for the local masses $m_\mathfrak{p}$, and the definition of the Tamagawa number of a reductive group over a global field. In Section 3, we give the representations (G_n, V_n) for $n = 2, 3, 4, 5$ and describe the parametrization of S_n-extensions via rational orbits and S-integral orbits. In Section 4, we count the number of S-integral orbits and carry out the cusp analysis as described above. In Section 5, we impose the necessary congruence conditions and prove the corresponding uniformity estimates needed to sieve. In Section 6, we specialize to the congruence conditions required for counting field extensions. In Section 7, we perform the corresponding local volume computations in terms of the Tamagawa number of the group and the local masses. In Section 8, we combine together the results of the previous sections to prove our main theorems with the restriction that the characteristic of F is not 2 if $n = 2$. In Section 9, we introduce a new representation that parametrizes quadratic extensions that works in any characteristic and prove our main theorems in the case $n = 2$ with no restriction on the characteristic of F.

We note that our methods may be applied to many other counting problems as well. For example, they may be used to study the 3-torsion in the S-class groups of orders in quadratic extensions of any base field, as well as the 2-torsion in the S-class groups of orders in cubic extensions, thus proving new cases of the Cohen–Lenstra–Martinet heuristics for class groups. Finally, the counting methods can eventually be extended to representations over F having more than one invariant, leading, e.g., to a proof of the boundedness of the average rank of elliptic curves over an arbitrary global field F and related results for average Selmer group sizes and curves of higher genus. These directions and the corresponding requisite extensions of the methods will be discussed in the second article of this series.

2 Preliminaries

sec:prelim

2.1 Notations

sec:notation

Throughout this paper, F is a fixed global field. That is, F is either a number field or the field of rational functions of a smooth projective and geometrically connected algebraic curve $\mathcal{C}$ over $\mathbb{F}_q$.

For every place $\mathfrak{p}$ of F, denote by $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$. When $\mathfrak{p}$ is nonarchimedean, denote by $\mathcal{O}_\mathfrak{p}$ and $k(\mathfrak{p})$ the ring of integers and the residue field at $\mathfrak{p}$ respectively. Let $N\mathfrak{p} = |k(\mathfrak{p})|$ denote the norm of $\mathfrak{p}$. For any $a \in F_\mathfrak{p}$, define its $\mathfrak{p}$-adic norm by $|a|_\mathfrak{p} = (N\mathfrak{p})^{-\mathfrak{p}(a)}$ where $\mathfrak{p}(a)$ denotes the $\mathfrak{p}$-adic valuation of a. Since every fractional ideal I of $\mathcal{O}_\mathfrak{p}$ is generated by an element $a \in F_\mathfrak{p}$ unique up to $\mathcal{O}_\mathfrak{p}^\times$, we define $|I|_\mathfrak{p}$ to be $|a|_\mathfrak{p}$. Note that this is the inverse of the ideal norm. When F is a number field and $\mathfrak{p}$ is archimedean, we denote by $|\cdot|_\infty$ the usual absolute value on $\mathbb{R}$ and define $|a|_\mathfrak{p} = |N_{F_\mathfrak{p}/\mathbb{R}}(a)|_\infty$ for any $a \in F_\mathfrak{p}$. Then for any $a \in F^\times$, we have the product formula $\prod_\mathfrak{p} |a|_\mathfrak{p} = 1$.

Let $\mathbb{A}$ denote the ring of adeles of F. For any adele $a = (a_\mathfrak{p})$, we write $|a|$ for the product $\prod_\mathfrak{p} |a_\mathfrak{p}|_\mathfrak{p}$. For any finite set S of places containing M_∞, let $\mathbb{A}_S$ denote the ring of S-adeles of F, that is, $\mathbb{A}_S$ is the restricted direct product of $F_\mathfrak{p}$ for $\mathfrak{p} \notin S$. Denote by F_S the product $\prod_{\mathfrak{p}\in S} F_\mathfrak{p}$. We embed $\mathbb{A}_S$ and F_S in $\mathbb{A}$ by setting all other coordinates to 1, and continue to write $|\cdot|$ for the restrictions of $|\cdot|$ on $\mathbb{A}$. On F_S, $|\cdot|$ is also called the *S-norm*. For any S-adele $a = (a_\mathfrak{p})$, we write (a) for the fractional ideal of $\mathcal{O}_S$ such that $(a) \otimes \mathcal{O}_\mathfrak{p} = a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ for every $\mathfrak{p} \notin S$. For any fractional ideal I of $\mathcal{O}_S$, let $|I|$ denote the product of $|I \otimes \mathcal{O}_\mathfrak{p}|_\mathfrak{p}$ as $\mathfrak{p}$ runs through places not in S. Then $|(a)| = |a|$ for any $a \in \mathbb{A}_S$.

2.2 The local masses $m_\mathfrak{p}$

For any $\mathfrak{p} \notin S$, the local masses $m_\mathfrak{p}(\Sigma_\mathfrak{p})$, in the case that Σ is the set of all degree-n separable extensions of F that are totally ramified at $\mathfrak{p}$, was computed in [41, Theorem 1]. When $F_\mathfrak{p} = \mathbb{Q}_p$ and Σ consists of all degree-n extensions with no local restrictions, the corresponding full mass $m_\mathfrak{p} = m_\mathfrak{p}(\Sigma_\mathfrak{p})$ was computed in [5, Theorem 1.1]. The methods apply to general nonarchimedean local fields $F_\mathfrak{p}$ to give

$$\frac{N\mathfrak{p}}{N\mathfrak{p}-1} m_\mathfrak{p} = \sum_{\substack{[K:F_\mathfrak{p}]=n \\ K\text{étale}}} \frac{|\mathrm{Disc}(K/F_\mathfrak{p})|_\mathfrak{p}}{\#\mathrm{Aut}(K/F_\mathfrak{p})} = \sum_{k=0}^{n-1} \frac{q(k, n-k)}{(N\mathfrak{p})^k}. \tag{9}$$ eq:localmassfinite

When $F_\mathfrak{p} = \mathbb{R}$, we have ([5, Proposition 2.4])

$$m_\mathfrak{p} = \sum_{\substack{[K:\mathbb{R}]=n \\ K\text{étale}}} \frac{1}{\#\mathrm{Aut}(K/\mathbb{R})} = \frac{\#S_n[2]}{n!}. \tag{10}$$ eq:localmassR

When $F_\mathfrak{p} = \mathbb{C}$, a degree-$n$ étale extension of $\mathbb{C}$ can only be $\mathbb{C}^n$ and so we have

$$m_\mathfrak{p} = \sum_{\substack{[K:\mathbb{C}]=n \\ K\text{étale}}} \frac{1}{\#\mathrm{Aut}(K/\mathbb{C})} = \frac{1}{n!}. \tag{11}$$ eq:localmassC

2.3 Tamagawa number of a reductive group over F

sec:tam

In this section, we first recall the definition of the Tamagawa number of a reductive group G over a global field F where the (global) character group has rank 1. See [38, Chapitre I, §5] for the definition in more general cases.

Let ω_G denote a top degree left-invariant differential form on G defined over F. For every place $\mathfrak{p}$, write $\omega_{G,\mathfrak{p}}$ for the associated Haar measure on $G(F_\mathfrak{p})$. Let S be a nonempty finite set containing all the archimedean places. Then the Tamagawa measure τ_G of $G(\mathbb{A})$ is defined by

$$\tau_G = \frac{D_F^{-\frac{\dim G}{2}}}{\operatorname{Res}_{s=1} \zeta_S(s)} \prod_{\mathfrak{p}\notin S} \frac{N\mathfrak{p}}{N\mathfrak{p}-1} \omega_{G,\mathfrak{p}} \prod_{\mathfrak{p}\in S} \omega_{G,\mathfrak{p}}.$$

We note that this measure is independent of the choice of S. Let χ denote a basis element for the character group. Let $G(\mathbb{A})^1$ denote the subgroup of $G(\mathbb{A})$ consisting of elements g such that $|\chi(g)| = 1$. The Tamagawa number of G is defined to be the volume of $G(F)\backslash G(\mathbb{A})^1$ with respect to a Haar measure τ_G^1 on $G(\mathbb{A})^1$ defined as follows.

When F is a number field, there is an embedding of $\mathbb{R}^+$ in $G(\mathbb{A})$ sending each $\lambda \in \mathbb{R}^+$ to the adele $\iota(\lambda)$ so that $|\chi(\iota(\lambda))| = \lambda$ and that via this embedding, one may write $G(\mathbb{A})$ as a Cartesian product $G(\mathbb{A}) \simeq G(\mathbb{A})^1 \times \mathbb{R}^+$. Then τ_G^1 is the Haar measure of $G(\mathbb{A})^1$ such that

$$\tau_G = \tau_G^1 \times d^\times \lambda$$

where $d^\times\lambda = d\lambda/\lambda$ is the usual multiplicative measure on $\mathbb{R}^+$.

When F is a function field with field of constants $\mathbb{F}_q$, $G(\mathbb{A})^1$ is an open subgroup of $G(\mathbb{A})$ and τ_G^1 is the Haar measure on $G(\mathbb{A})^1$ defined by

$$\tau_G^1 = \frac{\tau_{G|G(\mathbb{A})^1}}{\log q}.$$

It is known that the Tamagawa number of a reductive group over F whose derived group is a product of SL_k's is 1 ([38, Chapitre III, Théorème 5.3]).

3 Parametrization of quadratic, cubic, quartic, and quintic extensions of a fixed global field

sec:param

Let F be a fixed global field. Our goal in this section is to parametrize quadratic, cubic, quartic, and quintic extensions of F in terms of certain orbits of prehomogeneous representations. The representation we give here for $n = 2$ does not parametrize quadratic extensions in the case when F has characteristic 2; however, in Section 9, we will describe a different (though slightly more complicated and non-reductive) representation that will apply in all characteristics. We have chosen to keep the representation listed here for simplicity of exposition in the cases when the characteristic of F is not 2. For $n = 2$, 3, 4, and 5, we define the prehomogeneous representations (G_n, V_n) as in Table 1.

n	G_n	V_n	Action
2	$\mathbb{G}_m$	$\mathbb{G}_a$	$g \cdot v := g^2 v$
3	GL_2	$\mathrm{Sym}^3(2)$	$g \cdot f(x,y) := \det(g)^{-1} f((x,y)\cdot g)$
4	$\mathrm{GL}_2 \times \mathrm{GL}_3 /\{(\lambda^2, \lambda^{-1})\}$	$2 \otimes \mathrm{Sym}^2(3)$	$(g_2, g_3)\cdot(A,B) := (g_3 A g_3^t, g_3 B g_3^t) g_2^t$
5	$\mathrm{GL}_4 \times \mathrm{GL}_5 /\{(\lambda^2, \lambda^{-1})\}$	$4 \otimes \wedge^2(5)$	$(g_4, g_5)\cdot(A,B,C,D) := (g_5 A g_5^t, g_5 B g_5^t, g_5 C g_5^t, g_5 D g_5^t) g_4^t$

Table 1: Prehomogeneous representations parametrizing degree-n extensions tablereps

In Table 1, $\lambda \in \mathrm{GL}_k$ denotes the element in the center of GL_k with λ's on the diagonal. In the cases $n = 4$ and 5, the actions listed are the actions of $\mathrm{GL}_2 \times \mathrm{GL}_3$ and $\mathrm{GL}_4 \times \mathrm{GL}_5$, respectively, on V_n. It is easy to check that the subgroup $\{(\lambda^2, \lambda^{-1})\}$ of G_n acts trivially, and thus the action descends to an action of G_n of V_n. Each of these groups G_n are reductive, and their (global) character groups $\mathrm{Hom}(G_n, \mathbb{G}_m)$ all have rank 1. Let χ be a generator of $\mathrm{Hom}(G_n, \mathbb{G}_m)$. Then χ is unique up to inversion and for $n = 2$, 3, 4, and 5, we may take χ to respectively be

$$\begin{array}{rcl} \chi(g) & = & g, \\ \chi(g) & = & \det(g), \\ \chi(g_2, g_3) & = & \det(g_2)^3 \det(g_3)^4, \\ \chi(g_4, g_5) & = & \det(g_4)^5 \det(g_5)^8. \end{array} \qquad (12)$$

eqchi

The representations (G_n, V_n) are *prehomogeneous*, that is, the action of $G_n(\mathbb{C})$ on $V_n(\mathbb{C})$ consists of a single open orbit (in the Zariski topology); see [40]. It follows that for each n, the ring of relative invariants for the representation V_n of G_n is generated by a single element which we refer to as the *discriminant* and denote by $\Delta = \Delta_n$. The condition of being a relative invariant means that $\Delta_n(g \cdot v) = \chi(g)^k \Delta_n(v)$ for $g \in G_n(\mathbb{C})$ and $v \in V_n(\mathbb{C})$ for k independent of g and v. It is easy to check that $k = 2$ in all our cases. We note that the constant c in Theorems 1, 2 and 4 when F is a number field arises as $1/k$.

For any $v \in \mathbb{G}_a$, we have $\Delta_2(v) = v$. For any binary cubic form $ax^3 + bx^2y + cxy^2 + dy^3 \in \mathrm{Sym}^3(2)$, we have

$$\Delta_3(ax^3 + bx^2y + cxy^2 + dy^3) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

For any pair ternary quadratic forms viewed formally as 3×3 symmetric matrices

$$(A, B) = \left(\begin{pmatrix} a_{11} & \frac{1}{2}a_{12} & \frac{1}{2}a_{13} \\ \frac{1}{2}a_{12} & a_{22} & \frac{1}{2}a_{23} \\ \frac{1}{2}a_{13} & \frac{1}{2}a_{23} & a_{33} \end{pmatrix}, \begin{pmatrix} b_{11} & \frac{1}{2}b_{12} & \frac{1}{2}b_{13} \\ \frac{1}{2}b_{12} & b_{22} & \frac{1}{2}b_{23} \\ \frac{1}{2}b_{13} & \frac{1}{2}b_{23} & b_{33} \end{pmatrix} \right),$$

we have

$$\Delta_4(A, B) = \Delta_3(4 \det(Ax - By)).$$

The polynomial Δ_5 is homogeneous in the coordinates of 5×5 alternating matrices A, B, C, D of total degree 40.

The reason why the representations in Table 1 are particularly interesting is due to the following parametrization theorem.

thfieldparamR **Theorem 8.** *Suppose R is a ring. Then there is a map θ_R from the set of $G_n(R)$-orbits on $V_n(R)$ to the set of rings of rank n over R. Suppose that 2 is invertible in R when $n = 2$. Then θ has the following properties:*

(a) *When R is a PID, θ_R is a surjection and is a bijection when restricted to the preimages of maximal rank n rings over R. Furthermore if $v \in V_n(R)$ with $\theta_R(v)$ maximal, then*

$$\mathrm{Aut}(\theta_R(v)/R) \cong \mathrm{Stab}_{G_n(R)}(v),$$

where $\mathrm{Aut}(\theta_R(v)/R)$ denotes the group of automorphisms of $\theta_R(v)$ fixing R, and where for simplicity we write $\theta_R(v)$ for $\theta_R(G_n(R)v)$.

(b) *When R is a Dedekind domain, we have for any $v \in V_n(R)$,*

$$\mathrm{Disc}(\theta_R(v)/R) = (\Delta_n(v)).$$

We say a rank n ring over R is maximal if it is not strictly contained in any other rank n ring over R. In particular, since every étale ring of rank n over a field is maximal, we have the following particular case of Theorem 8 for the parametrization of degree-n fields, which was the main theorem of Wright–Yukie [52]:

cor: fieldparam **Theorem 9.** *Let K be a field. There is a bijection θ_K between the set of $G_n(K)$-orbits on $V_n(K)$ having nonzero discriminant and the set of étale degree-n extensions of K. For any $v \in V_n(K)$, we have*

$$\mathrm{Aut}(\theta_K(v)/K) \cong \mathrm{Stab}_{G_n(K)}(v).$$

Proof of Theorem 8. The set of $G_n(\mathbb{Z})$-orbits of a vector $v \in V_n(\mathbb{Z})$ have been determined in [31, 2, 3, 4] by explicitly writing down multiplication tables for a corresponding ring of rank n over $\mathbb{Z}$ and for its resolvent ring. The same multiplication tables define in general rings of rank n over R and its resolvent ring, for any $v \in V_n(R)$, and agree with the construction of Wright–Yukie [52] in Theorem 9 when R

is a field. Forgetting about the resolvent ring gives our map θ_R. When R is a PID, maximal rank n rings over R have unique resolvent rings ([31, §15], [3, Corollary 5], and [4, Corollary 3]). Hence θ_R, when restricted to the preimages of maximal rings, is a bijection.

The stabilizer statement follows also from the construction of the multiplication table. The case $n = 2$ is immediate. We now consider the case $n = 3$, 4, or 5. Suppose R is a PID. Let v be an element of $V_n(R)$ with $R' = \theta_R(v)$ maximal and hence has a unique resolvent ring S. Since R is a PID, the quotients R'/R and S/R are free. An automorphism of R' over R induces an automorphism of R'/R and an automorphism of S/R which under the identification of these quotients as free R-modules gives an element of $G_n(R)$ stabilizing v. Conversely, an element g of $G_n(R)$ induces an automorphism of R', as a free R-module, which is a ring homomorphism if g stabilizes v.

For the discriminant statement when $n > 2$, from the multiplication table we see that for any Dedekind domain R and any $v \in V_n(R)$, $\mathrm{Disc}(\theta_R(v)/R)$ is the ideal of R generated by a polynomial $\widetilde{\Delta}_n(v)$ in the coordinates of v. Moreover, for any $g \in G_n(R)$, one has $\widetilde{\Delta}_n(g.v) = \chi(g)^2\widetilde{\Delta}_n(v)$. Hence $\widetilde{\Delta}_n$ is a constant multiple of Δ_n. Computing both at a particular v shows that this constant is a unit. The discriminant statement when $n = 2$ is clear. □

We would like to describe a degree-n extension L of F integrally. By Corollary 9, there exists an element $v \in V_n(F)$ unique up to the action of $G_n(F)$ such that $\theta_F(v) = L$. Let S be a fixed nonempty finite set of places containing M_∞. Suppose further that S contains all the places above 2 if $n = 2$. For any place $\mathfrak{p} \notin S$, let $\mathcal{O}_{L,\mathfrak{p}}$ denote the integral closure of $\mathcal{O}_\mathfrak{p}$ in L and let $v_\mathfrak{p}$ be an element of $V_n(\mathcal{O}_\mathfrak{p})$ unique up to the action of $G_n(\mathcal{O}_\mathfrak{p})$ such that $\theta_{\mathcal{O}_\mathfrak{p}}(v_\mathfrak{p}) = \mathcal{O}_{L,\mathfrak{p}}$.

We would like patch these $v_\mathfrak{p}$ together into a global integral element. Since $\theta_{F_\mathfrak{p}}(v) = \theta_{F_\mathfrak{p}}(v_\mathfrak{p}) = L_\mathfrak{p}$, there exists $g_\mathfrak{p} \in G_n(F_\mathfrak{p})$ such that $v_\mathfrak{p} = g_\mathfrak{p} v$. The adele $(g_\mathfrak{p}) \in G_n(\mathbb{A}_S)$ is well-defined up to translation by $\prod_{\mathfrak{p}\notin S} G_n(\mathcal{O}_\mathfrak{p})$ on the left and by $G_n(F)$ on the right and so it defines an element in the corresponding double coset space cl_S. We fix a representative $\beta \in G_n(\mathbb{A}_S)$ for each double coset and write cl_S again for this set of representatives. Then we have the decomposition

$$G_n(\mathbb{A}_S) = \coprod_{\beta\in\mathrm{cl}_S} \Big(\prod_{\mathfrak{p}\notin S} G_n(\mathcal{O}_\mathfrak{p})\Big)\beta G_n(F). \tag{13}$$ eqstrongapproximation0

The set cl_S is finite due to the works of Borel [25] and Borel–Prasad [26]. There then exists a unique $\beta \in \mathrm{cl}_S$ and some $g \in G_n(F)$ such that $(g_\mathfrak{p}) \in \prod_{\mathfrak{p}\notin S} G_n(\mathcal{O}_\mathfrak{p})\beta g$. The element $v' = g.v$ corresponds also to the field L and lies in

$$\mathcal{L}_\beta := V_n(F) \cap \beta^{-1} \prod_{\mathfrak{p}\notin S} V_n(\mathcal{O}_\mathfrak{p}) \prod_{\mathfrak{p}\in S} V_n(F_\mathfrak{p}). \tag{14}$$ eq:Lbeta

Moreover, as fractional ideals of $\mathcal{O}_S$, we have

$$\mathrm{Disc}_S(L) = \prod_{\mathfrak{p}\notin S} \mathrm{Disc}(L_\mathfrak{p}/F_\mathfrak{p}) = \prod_{\mathfrak{p}\notin S} (\Delta_n(v_\mathfrak{p})) = (\chi(\beta)^2\Delta_n(v')).$$

Note that $\mathcal{L}_\beta$ is an additive subgroup of $V_n(F)$ commensurable with $V_n(\mathcal{O}_S)$.

We have now associated to a degree-n extension L over F an element $v' \in V_n(F)$ that is $\mathcal{O}_S$-integral up to finite denominators and such that $\mathrm{Disc}_S(L)$ and $\Delta_n(v')$ are equal up to a fixed bounded factor. How unique is such a v'?

For nonarchimedean places $\mathfrak{p}$, we say that an element $v \in V_n(\mathcal{O}_\mathfrak{p})$ is *maximal at* $\mathfrak{p}$ if $\theta_{\mathcal{O}_\mathfrak{p}}(v)$ is maximal. We say that an element $v \in \mathcal{L}_\beta$ is *S-maximal* if $\beta \cdot v$, when viewed as an element of $V_n(\mathcal{O}_\mathfrak{p})$ is maximal at $\mathfrak{p}$ for all $\mathfrak{p} \notin S$. Denote the set of S-maximal elements of $\mathcal{L}_\beta$ by $\mathcal{L}_\beta^{\max}$. Then it is clear that $v' \in \mathcal{L}_\beta^{\max}$.

prop:unique **Proposition 10.** *If $v_1, v_2 \in V_n(\mathcal{O}_\mathfrak{p})$ are maximal, then any $g \in G_n(F_\mathfrak{p})$ such that $g \cdot v_1 = v_2$ is an element of $G_n(\mathcal{O}_\mathfrak{p})$. In particular, If $v \in V_n(\mathcal{O}_\mathfrak{p})$ is maximal, then* $\mathrm{Stab}_{G_n(\mathcal{O}_\mathfrak{p})}(v) = \mathrm{Stab}_{G_n(F_\mathfrak{p})}(v)$.

Proof. Since v_1, v_2 are maximal and correspond to the same field, they also correspond to the same ring. By Theorem 8, $\theta_{\mathcal{O}_\mathfrak{p}}$ is a bijection when parameterizating maximal rings. Hence there exists

$g_0 \in G_n(\mathcal{O}_\mathfrak{p})$ such that $g_0 \cdot v_1 = v_2$. Then $g_0^{-1}g$ is in $\mathrm{Stab}_{G_n(F_\mathfrak{p})}(v_1)$ and we see that the two assertions in the proposition are in fact equivalent. We prove the stabilizer statement instead. By Theorem 8, we have

$$\mathrm{Stab}_{G_n(\mathcal{O}_\mathfrak{p})}(v) \cong \mathrm{Aut}(\theta_{\mathcal{O}_\mathfrak{p}}(v)/\mathcal{O}_\mathfrak{p}) = \mathrm{Aut}(\theta_{F_\mathfrak{p}}(v)/F_\mathfrak{p}) \cong \mathrm{Stab}_{G_n(F_\mathfrak{p})}(v),$$

as desired. □

As a consequence, if v_1 and v_2 are two elements in $\mathcal{L}_\beta^{\max}$ that are equivalent via some element g of $G_n(F)$, then g must be an element of Γ_β, where

$$\Gamma_\beta := G_n(F) \cap \beta^{-1}\Big(\prod_{\mathfrak{p}\notin S} G_n(\mathcal{O}_\mathfrak{p}) \prod_{\mathfrak{p}\in S} G_n(F_\mathfrak{p})\Big)\beta. \tag{15}$$

Therefore, we conclude that v' is unique up to the action of Γ_β.

We summarize the above discussion in the following theorem.

thmainparam **Theorem 11.** *We have a bijection*

$$\{\textit{degree-}n\textit{ extensions of } F \textit{ having nonzero discriminant}\} \longleftrightarrow \bigcup_{\beta\in \mathrm{cl}_S} (\Gamma_\beta \backslash \mathcal{L}_\beta^{\max}).$$

Furthermore, if L is a degree-n extension corresponding to $v' \in \mathcal{L}_\beta$ for some $\beta \in \mathrm{cl}_S$ under this bijection, then

$$\mathrm{Disc}_S(L) = (\chi(\beta))^2(\Delta_n(v')).$$

As a consequence, the S-Steinitz class of L is the $\mathcal{O}_S$-ideal class of $(\chi(\beta))$.

Proof. Only the last statement on the S-Steinitz class needs to be justified. When $n = 2$, this is clear. When $n > 2$, it follows immediately from a result of Artin [1] (see also [35, Proposition 3.3]): let $\delta_{L/F} \in F^\times$ be the discriminant of the trace form with respect to some F-basis of L; then there is a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_S$ such that $\mathrm{Disc}_S(L) = (\delta_{L/F})\mathfrak{a}^2$ and moreover, the ideal class of $\mathfrak{a}$ is the S-Steinitz class of L. □

4 Counting S-integral orbits over global fields

sec:count

Let F be a fixed global field.

We say that an element $v \in V_n(F)$ is *generic* if the degree-n extension L of F corresponding to v is a field extension of F, and the Galois group of the normal closure of L over F is S_n. For a subset U of $V_n(F)$, we denote the set of generic elements in U by U^{gen} .

For the rest of this section, we fix a nonempty finite set S of places of F containing M_∞. Since the purpose of this section is to count the number of S-integral orbits instead of counting field extensions, we make no assumption on the characteristic of F or S when $n = 2$. For any positive real number X and any subset U of $V_n(F)$, we denote by U_X the set of elements of U whose discriminants have S-norm less than X when F is a number field and S-norm equal to X when F is a function field. If H is a subgroup of $G_n(F)$ that preserves U, then we let $N(U, H; X)$ denote the number of generic H-orbits on U_X, where each orbit $H \cdot v$ is counted with weight $1/\#\,\mathrm{Stab}_H(v)$.

By Theorem 11, it suffices to count the number of S-integral orbits such that the S-norm of the Δ_n-invariant is bounded. Since we need to impose congruence conditions later, we consider the more general case of a sublattice $\mathcal{L}$ of $V_n(F)$ that is commensurable with $V_n(\mathcal{O}_S)$ and a subgroup Γ of $G_n(F)$ preserving $\mathcal{L}$ that is commensurable with $G_n(\mathcal{O}_S)$. Our goal in this section is to determine asymptotics for $N(\mathcal{L}, \Gamma, X)$. We do this by constructing a fundamental domain for the action of Γ on $V_n(F_S)$ and counting the number of $\mathcal{L}$-points via suitable geometry-of-numbers arguments.

4.1 Reduction Theory

sec:fund

Let S denote a set of places of F containing M_∞, and let $F_S = \prod_{\mathfrak{p}\in S} F_{\mathfrak{p}}$. In this section, we construct a fundamental domain for the action of Γ on $V_n(F_S)$ by constructing a fundamental domain $\mathcal{F}$ for the action of Γ on $G_n(F_S)$ via left multiplication, a fundamental domain R for the action of $G_n(F_S)$ on $V_n(F_S)$, and then taking $\mathcal{F}\cdot R$ as a multiset (so it is in bijection with $\mathcal{F}\times R$).

The set R can be taken as a finite discrete set. By Theorem 8, the set of $G_n(F_S)$-orbits on $V_n(F_S)$ is in bijection with the set of all S-*specifications*. Here an S-specification is a collection $(L_{\mathfrak{p}})_{\mathfrak{p}\in S}$ of degree-n étale extensions $L_{\mathfrak{p}}$ of $F_{\mathfrak{p}}$ for each $\mathfrak{p}\in S$. For each such S-specification σ, we let $V_n(F_S)^{(\sigma)}$ denote the set of elements $(v_{\mathfrak{p}})_{\mathfrak{p}\in S}\in V_n(F_S)$ such that the extension corresponding to $v_{\mathfrak{p}}$ is $L_{\mathfrak{p}}$ for every $\mathfrak{p}\in S$. We also fix some v_σ in each $V_n(F_S)^{(\sigma)}$. Then we may take R to be the collection of the v_σ's. In what follows, we will fix an S-specification σ and consider only $V_n(F_S)^{(\sigma)}$. We define $\mathrm{Aut}(\sigma)$ by

$$\mathrm{Aut}(\sigma) := \prod_{\mathfrak{p}\in S}\mathrm{Aut}(L_{\mathfrak{p}}).$$

Then the stabilizer in $G_n(F_S)$ of every element in $V_n(F_S)^{(\sigma)}$ is isomorphic to $\mathrm{Aut}(\sigma)$ by Theorem 8. We have the following theorem whose proof is identical to that of [15, §2.1].

thmfunddomain

Theorem 12. *Let $\mathcal{F}$ denote a fundamental domain for the action of Γ on $G_n(F_S)$. For any fixed $v_\sigma\in V_n(F_S)^{(\sigma)}$, the multiset $\mathcal{F}\cdot v_\sigma$ is an $\#\mathrm{Aut}(\sigma)$-fold cover of a fundamental domain for the action of Γ on $V_n(F_S)^{(\sigma)}$. More precisely, for $v\in V_n(F_S)$, we have*

$$\#\{g\in\mathcal{F} : g\cdot v_\sigma = v\} = \#\mathrm{Aut}(\sigma)/\#\,\mathrm{Stab}_\Gamma(v).$$

Fix any positive real number X. Recall the basis χ for the group of characters of G_n defined in (12) and define $G_n(\mathbb{A})^1$ to be the subset of $G_n(\mathbb{A})$ consisting of adeles g such that adele norm $|\chi(g)|$ is 1. Similarly define $G_n(F_S)^1$ via its natural embedding in $G_n(\mathbb{A})$. Let $G_n(F_S)^{(\sigma)}_X$ denote the subset of $G_n(F_S)$ consisting of S-adeles g such that the adele norm $|\chi(g)|^2$ is at most (resp., equal to) $X/|\Delta_n(v_\sigma)|$ when F is a number field (resp., when F is a function field). For any $g\in G_n(\mathcal{O}_S)$, we have $|\chi(g)|_{\mathfrak{p}} = 1$ for every $\mathfrak{p}\notin S$ while the product $\prod_{\mathfrak{p}}|\chi(g)|_{\mathfrak{p}} = 1$ by the product formula. Hence the group homomorphism $\chi_S : G_n(F_S)\to\mathbb{R}^+$ defined by $\chi_S(g) = \prod_{\mathfrak{p}\in S}|\chi(g)|_{\mathfrak{p}}$ is trivial on $G_n(\mathcal{O}_S)$. Since Γ is commensurable to $G_n(\mathcal{O}_S)$, we see that $\chi_S(g)$ is a root of unity for any $g\in\Gamma$. Hence Γ is contained in the kernel of χ_S and preserves $G_n(F_S)^{(\sigma)}_X$. Let $\mathcal{F}(X)$ denote a fundamental domain for the action of Γ on $G_n(F_S)^{(\sigma)}_X$, then $\mathcal{F}(X)\cdot v_\sigma$ is an $\#\mathrm{Aut}(\sigma)$-fold cover of a fundamental domain for the action of Γ on $V_n(F_S)^{(\sigma)}_X$.

To construct $\mathcal{F}(X)$, we recall the reduction theory developed by Springer [45]. Let P be a minimal parabolic subgroup of G_n. Let T be a maximal split torus of G_n contained in P, and let N be the unipotent radical of P. Finally, let Δ denote a set of simple roots. That is, Δ is a basis for the set of positive roots defined by P.

We use the following coordinates for T and Δ:

$$\begin{aligned}
&n=2; \quad T = 1;\\
&n=3; \quad T = \left\{\begin{pmatrix} s_1^{-1} & \\ & s_1\end{pmatrix}\right\}, && \Delta = \{s_1^2\};\\
&n=4; \quad T = \left\{\begin{pmatrix} s_1^{-1} & \\ & s_1\end{pmatrix}, \begin{pmatrix} s_2^{-2}s_3^{-1} & & \\ & s_2 s_3^{-1} & \\ & & s_2 s_3^2\end{pmatrix}\right\}, && \Delta = \{s_1^2, s_2^3, s_3^3\};\\
&n=5; \quad T = \left\{\begin{pmatrix} s_1^{-3}s_2^{-2}s_3^{-1} & & & \\ & s_1^1 s_2^{-2}s_3^{-1} & & \\ & & s_1^1 s_2^2 s_3^{-1} & \\ & & & s_1^1 s_2^2 s_3^3\end{pmatrix}, \begin{pmatrix} s_4^{-4}s_5^{-3}s_6^{-2}s_7^{-1} & & & & \\ & s_4^1 s_5^{-3}s_6^{-2}s_7^{-1} & & & \\ & & s_4^1 s_5^2 s_6^{-2}s_7^{-1} & & \\ & & & s_4^1 s_5^2 s_6^3 s_7^{-1} & \\ & & & & s_4^1 s_5^2 s_6^3 s_7^4\end{pmatrix}\right\}, && \Delta = \{s_1^4, s_2^4, s_3^4, s_4^5, s_5^5, s_6^5, s_7^5\};
\end{aligned} \tag{16}$$

Set S_∞ to be M_∞ when F is a number field and to be any (fixed) nonempty subset of S when F is a function field. For any positive constants c and c', define:

$$\begin{aligned} T(c) &= \{t = (t_\mathfrak{p})_{\mathfrak{p}\in S_\infty} \in T(F_{S_\infty}) : |\alpha(t)| \geq c, \forall \alpha \in \Delta\}, \\ T(c,c') &= \{t \in T(c) : ||\frac{\log |t_v|_v}{\log |t_{v'}|_{v'}}||_\infty \leq c', \forall v, v' \in S_\infty\}, \end{aligned}$$

where we identify T with $\mathbb{G}_m^r$, view $\log |t_v|_v / \log |t_{v'}|_{v'}$ as an element of $\mathbb{R}^r$ and where $||\cdot||_\infty$ denotes the supremum norm on $\mathbb{R}^r$. Then by [45, Remark 2.2] there exist positive real numbers c, c', a compact subset $N' \subset N(F_{S_\infty})$, and a compact subgroup K' of $G_n(F_S)$ such that

$$G_n(F_S)^1 = G_n(\mathcal{O}_S)N'T(c,c')K'. \qquad (17)$$

eq:Spred

We remark that in [45], the set $T(c)$ is defined by $|\alpha(t)| \leq c$. Since we want a fundamental domain for the left action of $G_n(\mathcal{O})$ on $G_n(F_S)$, we need to apply inverses to the results of [45]. The extra parameter c' comes from computing $T(\mathcal{O}_S)\backslash T(c)$ using the fact that the image of $\mathcal{O}_S^\times$ in $\mathbb{R}^{|S_\infty|}$ under the map $t \mapsto (\log |t_v|_v)$ is a lattice of rank $|S_\infty| - 1$ in the hyperplane $H : x_1 + \cdots + x_{|S_\infty|} = 0$ with compact quotient.

The subset $N'T(c,c')K'$ is called a *Siegel domain* $\mathfrak{D}_0$. Since Γ is commensurable with $G_n(\mathcal{O}_S)$, there exists a finite set of elements $g_1, \ldots, g_k \in G_n(F)$ such that the union $\cup_{i=1}^k g_i\mathfrak{D}_0$ of translates of $\mathfrak{D}_0$ contains a fundamental domain Ω for the action of Γ on $G_n(F_S)^1$. To obtain $\mathcal{F}(X)$ or $\mathcal{F}$, we use the center of G_n to apply a scaling as follows. We write $g(\lambda)$ for the element of the center of G_n that scales every coordinate of V_n by λ. When F is a number field, there is an embedding ι of $\mathbb{R}^+$ into $G_n(F_S)$ sending $\lambda \in \mathbb{R}^+$ to the adele $\iota(\lambda)$ that is $g(\lambda^\kappa)$ at every infinite place and is 1 at every finite place in S where κ is a positive real constant chosen so that the S-norm $|\chi(\iota(\lambda))|$ is λ. Let Λ_X be the image of this embedding of the interval $(0, (X/|\Delta_n(v_\sigma)|)^{1/2}]$. Then we may take $\mathcal{F}(X)$ to be $\Lambda_X\Omega$. We let Λ denote the entire image of ι and set $\mathcal{F} = \Lambda\Omega$.

When F is a function field of characteristic p, one could let Λ_X be an arbitrary (fixed) element of $G_n(F_S)_X^{(\sigma)}$ and take $\Lambda_X\Omega$ to be $\mathcal{F}(X)$. We will use this construction when we later compute the various volumes to obtain the main term of the estimate. However in order for the shape of the fundamental domain to remain the same as X grows, for the purpose of a controllable error term, we make the following modification. We fix an embedding of $\mathbb{F}_p(u)$ into F. Precomposing it with the map $\mathbb{Z} \to \mathbb{F}_p(u)$ sending m to u^m, and postcomposing it with the embedding of F into F_S that is the natural embedding at all the places of S_∞ and is the constant 1 at all other places, give an embedding $\mathbb{Z} \to F_S$. Next we postcompose it with the embedding of F_S into $G_n(F_S)$ sending λ to $g(\lambda)$ as described above. Denote by ι the resulting embedding $\mathbb{Z} \to G_n(F_S)$. Let Λ denote the image of ι. A finite union of right translates of the set $\Lambda\Omega$ then forms a fundamental domain $\mathcal{F}$ for the action of Γ on $G_n(F_S)$. Note that one may combine these right translates with the compact subgroup K'. We set $\mathcal{F}(X)$ to be the intersection of $\mathcal{F}$ with $G_n(F_S)_X^{(\sigma)}$. Of course, we only consider X when this set is nonempty, for otherwise there are no orbits such that the S-norm of the Δ_n invariant is X.

We summarize the above construction in the following theorem.

thm:fundG **Theorem 13.** *There exists a subset $\mathfrak{D}$ of $G_n(F_S)$ of the form $\Lambda N'T(c,c')K''$ where Λ is a subset of the center of $G_n(F_S)$, where N' and $T(c,c')$ are as above, and where K'' is a finite union of right translates of a compact subgroup K' of $G_n(F_S)$, such that a fundamental domain for the left action of Γ on $G_n(F_S)$ is contained in a finite union of translates $g_i\mathfrak{D}$, with $g_i \in G_n(\mathcal{O}_S)$, for $i = 1, \ldots, k$.*

For each $i = 1, \ldots, k$, let $\mathcal{F}_i$ denote $\mathcal{F} \cap g_i\mathfrak{D}$. Then $\mathcal{F}$ is the disjoint union of $\mathcal{F}_1, \ldots, \mathcal{F}_k$.

4.2 Averaging

Theorem 12 implies that we have

$$N(\mathcal{L}^{(\sigma)}, \Gamma; X) = \frac{1}{\#\mathrm{Aut}(\sigma)}\#\{\mathcal{F}(X) \cdot v_\sigma \cap \mathcal{L}^{\mathrm{gen}}\}.$$

When F is a number field, we define $G_0 \subset G_n(F_S)$ to be some fixed product of nonempty open bounded semialgebraic sets $G_0' \subset G_n(F_{M_\infty})$ and nonempty open compact sets $G_0'' \subset G_n(F_{S\setminus M_\infty})$. When F is a function field, we set G_0 to be some fixed nonempty open compact subset of $G_n(F_S)$. Suppose further that $|\chi(g)| > 1$ for every $g \in G_0$.

We have the following equalities used in [7]:

$$\begin{aligned} N(\mathcal{L}^{(\sigma)}, \Gamma; X) &= \frac{1}{\mathrm{Vol}(G_0)\#\mathrm{Aut}(\sigma)} \int_{g\in G_0} \#\{(\mathcal{F}g \cdot v_\sigma)_X \cap \mathcal{L}^{\mathrm{gen}}\} dg \\ &= \frac{1}{\mathrm{Vol}(G_0)\#\mathrm{Aut}(\sigma)} \int_{g\in \mathcal{F}} \#\{(gG_0 \cdot v_\sigma)_X \cap \mathcal{L}^{\mathrm{gen}}\} dg \qquad (18) \\ &= \frac{1}{\mathrm{Vol}(G_0)\#\mathrm{Aut}(\sigma)} \sum_{i=1}^{k} \int_{g\in \mathcal{F}_i} \#\{(gG_0 \cdot v_\sigma)_X \cap \mathcal{L}^{\mathrm{gen}}\} dg, \end{aligned}$$ eqavg

where dg is any Haar-measure on $G_n(F_S)$ and the volume of G_0 is taken with respect to dg.

The action of g_i^{-1} on $V_n(F)$ takes $\mathcal{L}$ to a different lattice and preserves generic elements and the S-norms of their discriminants. Then we have

$$\int_{g\in \mathcal{F}_i} \#\{(gG_0 \cdot v_\sigma)_X \cap \mathcal{L}^{\mathrm{gen}}\} dg = \int_{g\in g_i^{-1}\mathcal{F}_i} \#\{(gG_0 \cdot v_\sigma)_X \cap g_i^{-1}\mathcal{L}^{\mathrm{gen}}\} dg. \tag{19}$$ eqdivide

Since $g_i^{-1}\mathcal{L}$ is also a lattice in $V_n(F_S)$, the S-norms of nonzero coefficients of elements in $g_i^{-1}\mathcal{L}$ are uniformly bounded from below by a positive constant $c_i > 0$.

Let Var denote the set of coefficients of V. For $\alpha \in \mathrm{Var}$, let $w(\alpha)$ denote the quantity by which an element of ΛT scales α. Then $w(\alpha)$ is a monomial in λ and the s_i. It is easy to see that the exponent of λ appearing in the weight of each $\alpha \in \mathrm{Var}$ is the same. We define a partial order $\leq$ on Var, where we set $\alpha \leq \beta$ if the weight $w(\beta\alpha^{-1})$, when viewed as a character of T is positive; that is, it is a product of nonnegative powers of the s_i. In all our cases, Var contains an element α_0 with $\alpha_0 \leq \alpha$ for all $\alpha \in \mathrm{Var}$. For V_3 we have $\alpha_0 = a$, the coefficient of x^3, for V_4 we have $\alpha_0 = a_{11}$, and for V_5 we have $\alpha = a_{12}$. Since our representations are not trivial, we see that the powers of every s_i in $w(\alpha_0)$ is negative. Let $\mathcal{F}'_{i,X}$ denote the set of elements $g \in \mathcal{F}_i$ such that $(g_i^{-1}gG_0 \cdot v_\sigma)_X$ contains elements whose α_0-coefficients have S-norm at least c_i. It follows that if $g \in \mathcal{F}_i \setminus \mathcal{F}'_{i,X}$, then every element of $(g_i^{-1}gG_0 \cdot v_\sigma)_X \cap g_i^{-1}\mathcal{L}$ has α_0-coefficient equal to 0.

We call the set $g_i^{-1}\mathcal{F}'_{i,X}G_0 \cdot v_\sigma$ "the main body" and the set $g_i^{-1}(\mathcal{F}_i \setminus \mathcal{F}'_{i,X})G_0 \cdot v_\sigma$ "the cuspidal region". In the §4.5 and §4.3, we prove respectively that the number of non-generic elements in the main body is negligible and that the number of generic elements in the cuspidal region is negligible.

4.3 The number of generic elements in the cusp is negligible

sec: cuspgensmall

Let L be some fixed lattice in $V_n(F_S)$ that is commensurable with $V_n(\mathcal{O}_S)$. We will apply the result of this section when $L = g_i^{-1}\mathcal{L}$. The S-norms of the nonzero coefficients of elements in $gG_0 \cdot v_\sigma \cap L$ for $g \in \mathfrak{D}$ are uniformly bounded from below, say by some constant $c_0 > 0$. Write $\mathfrak{D}_X = \mathfrak{D} \cap G_n(F_S)^{(\sigma)}_X$. and let $\mathfrak{D}'_X$ denote the set of elements $g \in \mathfrak{D}_X$ such that $gG_0 \cdot v_\sigma$ contains elements whose α_0-coefficients have S-norm at least c_0. Since $|\chi(g)|$, for any $g \in G_0$, is bounded below and above by an absolute constant, it suffices to prove the following theorem.

Theorem 14. *We have*

$$\int_{g\in \mathfrak{D}_X \setminus \mathfrak{D}'_X} \#\{gG_0 \cdot v_\sigma \cap L^{\mathrm{gen}}\} dg = O(X^{1-\epsilon_n}) \tag{20}$$ eqcuspcutoff

where $\epsilon_n = 1$ when $n = 2$ or 3 and $\epsilon_n = 1/d_n$ when $n = 4$ or 5; here d_n is the dimension of V_n.

Proof. When $n=2$ or $n=3$, the theorem is immediate because every $v \in gG_0 \cdot v_\sigma \cap L$, with $g \in \mathfrak{D}_X \backslash \mathfrak{D}'_X$, satisfies $\alpha_0(v)=0$, which implies that v is not generic. When $n=4$ or $n=5$, we proceed as in [7].

For a subset $U \subset \mathrm{Var}$, let $L(U)$ denote the set of elements of L such that: for every $\alpha \in U$, $\alpha(v)=0$ for every $v \in L(U)$; and for every $\alpha \notin U$, there exists $v \in L(U)$ such that $\alpha(v) \neq 0$. There are characters δ_n of the torus (not involving the center) such that the measure $\delta_n(s) d^\times \lambda dn d^\times s dk$ is a (left-invariant) Haar measure on $G_n(F_S)$, where dk is the measure on K'' obtained from translating the Haar-measure on K', dn is a Haar-measure on $N(F_{S_\infty})$ and $d^\times s$ denotes $\prod ds_i/s_i$. When F is a number field, we have the embedding ι of $\mathbb{R}^+$ into the center of $G_n(F_S)$ and $d^\times\lambda$ is the push forward of the measure $d\lambda/\lambda$ on $\mathbb{R}^+$. When F is a function field, then $d^\times\lambda$ is 1 (i.e., it does not appear in the Haar measure). The characters $\delta_n(s)$ are given by:

$$
\begin{aligned}
\delta_2(s) &= 1,\\
\delta_3(s) &= s_1^{-2},\\
\delta_4(s) &= s_1^{-2}s_2^{-6}s_3^{-6},\\
\delta_5(s) &= s_1^{-8}s_2^{-12}s_3^{-8}s_4^{-20}s_5^{-30}s_6^{-30}s_7^{-20}.
\end{aligned}
$$

Write Λ'_X for Λ_X when F is a number field and for $\iota(m)$ when F is a function field where m is the integer such that $X/|\Delta_n(v_\sigma)|$ lies between $|\iota(m)|$ and $|\iota(m+1)|$. By definition of T and N, we see that there exists a compact subset $N'' \subset N(F_{S_\infty})$ such that for any $t \in T(c)$ and any $n \in N'$, $t^{-1}nt \in N''$. Hence any element of $\mathfrak{D}_X$ has the form gk where $g \in \Lambda'_X T(c,c')$ and k belongs to the compact set $N''K'$. It suffices to prove the estimate

$$\int_{g \in \Lambda'_X T(c,c')} \#\{gkG_0 \cdot v_\sigma \cap L(U)^{\mathrm{gen}}\} |\delta_n(s)| d^\times s d^\times \lambda \ll X^{1-1/d_n}, \tag{21}$$ eqcutcusp

for any $k \in N''K'$ for all sets $U \subset \mathrm{Var}$ containing α_0, where the implied constant does not depend on k. As in the proof of [7, Lemma 11] it suffices to prove the theorem for sets U that are closed under the partial order $\leq$, meaning that if $\beta \in U$ and $\alpha \leq \beta$, then $\alpha \in U$. Also note for $g = \lambda s \in \Lambda'_X T'$, the set $gkG_0 \cdot v_\sigma \cap L(U)$ is empty unless $w(\alpha) \gg 1$ for all $\alpha \notin U$.

To count the number of lattice points, we use the following result from the geometry of numbers.

davgen **Proposition 15.** *Let E be $\mathbb{R}$ (resp. F_S) if F is a number field (resp. function field and S is a nonempty set of places). Let n be a positive integer. Let B be an open bounded and semialgebraic subset of E^n (resp. an open compact subset of E^n). Let K be any subset of $\mathrm{GL}_n(E)$ (resp. an open compact subset of $\mathrm{GL}_n(E)$). Let c be a real constant. Let L be a lattice in E^n. Then for any $k \in K$ and any $t = \mathrm{diag}(t_1,\ldots,t_n) \in \mathrm{GL}_n(E)$ with the additional condition, when F is a function field, that $|t_i|_v/|t_i|_{v'} < c$ for any $v,v' \in S$,*

$$\#\{tkB \cap L\} = \mathrm{Vol}_L(tkB) + O(\mathrm{Vol}(\mathrm{proj}(tkB))), \tag{22}$$ eq:daven

where Vol is some fixed volume measure on E^n, Vol_L is a constant multiple of Vol such that E^n/L has volume 1, and $\mathrm{Vol}(\mathrm{proj}(tkB))$ denotes the greatest d-dimensional volume of any projection of tkB 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 E, n, B, c, L and in the function field case, also on K.

When F is a number field, this result follows from Davenport [29] where the dependency on B is through the number and the degrees of the polynomial inequalities that define B which stay the same when a linear change of variable is applied. When F is a function field, see Proposition 33 in Appendix A.

Using Proposition 15 with $B = G_0 \cdot v_\sigma$ and $K = N''K'$, we have for any $k \in K$ and for any nonnegative real numbers k_α,

$$\begin{aligned}
&\int_{g\in\Lambda'_X T(c,c')} \#\{gkG_0\cdot v_\sigma \cap L(U)^{\mathrm{gen}}\} d^\times\lambda d^\times s \\
\ll\ & \int_{g\in\Lambda'_X T(c,c')} \big(\prod_{\alpha\notin U} |w(\alpha)|\big) |\delta_n(s)| d^\times s d^\times \lambda \\
\ll\ & \int_{g\in\Lambda'_X T(c,c')} \big(\prod_{\alpha\notin U} |w(\alpha)|\big)\big(\prod_{\alpha\in\min(U)} |w(\alpha)|^{k_\alpha}\big) |\delta_n(s)| d^\times s d^\times \lambda \\
\ll\ & X\int_{g\in\Lambda'_X T'} \big(\prod_{\alpha\in U} |w(\alpha)^{-1}|\big)\big(\prod_{\alpha\in\min(U)} |w(\alpha)|^{k_\alpha}\big) |\delta_n(s)| d^\times s d^\times \lambda.
\end{aligned}$$

Therefore, to prove (21) for a set U, it suffices to find nonnegative real numbers k_α for $\alpha\notin U$ such that $\sum k_\alpha < \#U$ and the exponents of each s_i in $\big(\prod_{\alpha\in U} w(\alpha)^{-1}\big)\big(\prod_{\alpha\in\min(U)} w(\alpha)^{k_\alpha}\big)\delta_n(s)$ are negative. The condition $\sum k_\alpha < \#U$ implies that the exponent of λ is also negative.

We now prove the theorem for $n=4$. Every element $(A,B)\in\mathcal{L}$ with $a_{11}=b_{11}=0$ (resp. $a_{11}=a_{12}=a_{13}=0$ or $a_{11}=a_{12}=a_{22}=0$) is reducible because one of the four points in $\mathbb{P}^2(\bar{F})$ corresponding to (A,B) is rational (resp. $\det(A)=0$; thus the cubic resolvent of (A,B) is reducible). Thus it is enough to consider sets U equal to $\{a_{11}\}$ and $\{a_{11},a_{12}\}$. For $U=\{a_{11}\}$, we can take the weight 1: that is $k_\alpha=0$ for all α. For $U=\{a_{11},a_{12}\}$, we take the weight $w(a_{12})$: that is $k_\alpha=1$ for $\alpha=a_{12}$ and 0 for all other α. The proof of the theorem when $n=5$ follows in an identical fashion from [7, Lemma 10] and [7, Table 1]. □

4.4 The main term

With notation as above, we have the following lemma.

Lemma 16. *For $g\in g_i^{-1}\mathcal{F}'_{i,X}$, we have*

$$\#\{(gG_0\cdot v_\sigma)_X\cap L\} = \mathrm{Vol}_L\big((gG_0\cdot v_\sigma)_X\big) + O(X|w(\alpha_0)|^{-1/d}),$$

where the volume is computed with respect to the Haar-measure of $V_n(F_S)$ normalized so that L has covolume 1 in $V_n(F_S)$ and where d is the degree of F over $\mathbb{Q}$ when F is a number field and is 1 when F is a function field.

Proof. Since the projection of $gG_0\cdot v_\sigma$ onto $V_n(F_{S\setminus S_\infty})$ is open compact, we may replace L by a union of finitely many lattices in $V_n(F_{S_\infty})$ and applying Proposition 15 to each of these lattices gives the main term. The error term is then the maximum of the volumes of the images onto coordinate hyperplanes of $V_n(F_{S_\infty})$. Since α_0 has minimal weight, we see that to achieve the maximum of the volumes (up to a bounded constant), we must include all the coordinate hyperplanes away from α_0. We are thus done in the function field case by Proposition 15. When F is a number field, $V_n(F_{S_\infty})$ is a real vector space of dimension $\dim(V_n)d$. By the definition of $T(c,c')$, the projection of $(gG_0\cdot v_0)_X$ onto the d $\mathbb{R}$-coordinates corresponding to α_0 all have sizes bounded above and below by an absolute constant times $|w(\alpha_0)|^{1/d}$, and the maximum of the volumes of all projections, up to a bounded constant, is then achieved by taking one of these d coordinates and projecting onto the coordinate hyperplanes corresponding to all the other coordinates. □

Integrating both sides of the equation in the above lemma over $g \in \cup_i g_i^{-1}\mathcal{F}'_{i,X}$, we obtain

$$\begin{aligned}
\int_{g\in g_i^{-1}\mathcal{F}'_{i,X}} \#\{(gG_0\cdot v_\sigma)_X \cap g_i^{-1}\mathcal{L}\} &= \int_{g\in g_i^{-1}\mathcal{F}'_{i,X}} \mathrm{Vol}_{g_i^{-1}\mathcal{L}}\big((gG_0\cdot v_\sigma)_X\big)dg + O(X^{1-1/\epsilon'_n}) \\
&= \int_{g\in \mathcal{F}'_{i,X}} \mathrm{Vol}_{\mathcal{L}}\big((gG_0\cdot v_\sigma)_X\big)dg + O(X^{1-1/\epsilon'_n}) \qquad (23) \\
&= \int_{g\in \mathcal{F}_i} \mathrm{Vol}_{\mathcal{L}}\big((gG_0\cdot v_\sigma)_X\big)dg + O(X^{1-1/\epsilon'_n}),
\end{aligned}$$

appdavlem

where $\epsilon'_2 = 2d$, $\epsilon'_3 = 6d$, $\epsilon'_4 = 12d$, and $\epsilon'_5 = 40d$. The first equality follows from an explicit computation for the integral of $|w(\alpha_0)|^{-1/d}$. The second equality follows since $g_i \in G_n(F_S)^1$ is measure preserving. The last equality follows from an element computation of the volume of $\mathcal{F}_i \backslash \mathcal{F}'_{i,X}$.

4.5 The number of nongeneric elements in the main body is negligible

sec: mainnongensmall

Let $\mathcal{L}^{\mathrm{ngen}}$ denote the set of elements in $\mathcal{L}$ that are not generic. In this subsection, we prove the following theorem.

Theorem 17. *With notations as above, we have*

$$\int_{\mathcal{F}'_{i,X}} \#\{(gG_0\cdot v_\sigma)_X \cap \mathcal{L}^{\mathrm{ngen}}\}dg = o(X). \qquad (24)$$

eqngenmb

Proof. Let τ be a local splitting type corresponding to some conjugacy class of S_n. In particular, τ is an unramified splitting type. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_S$, let $\mathcal{L}^{\mathfrak{p},\neq(\tau)}$ denote the set of elements in $v \in \mathcal{L}$ that do not have splitting type τ at $\mathfrak{p}$. Note that if $v \in \mathcal{L}$ is generic, then v must have splitting type τ at some (positive proportion of) primes. Therefore, we have

$$\mathcal{L}^{\mathrm{ngen}} \subset \bigcup_\tau \Big(\bigcap_{\mathfrak{p}} \mathcal{L}^{\mathfrak{p},\neq(\tau)}\Big).$$

The set $\mathcal{L}^{\mathfrak{p},\neq(\tau)}$ is contained in the inverse image under the reduction modulo $\mathfrak{p}$ map of the set $V_n(\mathbb{F}_{\mathfrak{p}}^{\neq(\tau)})$ consisting of elements in $V_n(\mathbb{F}_{\mathfrak{p}})$ that do not have splitting type (τ). Denote by $\mu_\tau(\mathfrak{p})$ the $\mathfrak{p}$-adic density of $\mathcal{L}^{\mathfrak{p},(\neq\tau)}$, that is, $\mu_\tau(\mathfrak{p}) \leq \#V_n(\mathbb{F}_{\mathfrak{p}}^{\neq(\tau)})/\#V_n(\mathbb{F}_{\mathfrak{p}})$. Then as $N\mathfrak{p}\to\infty$, $\mu_\tau(\mathfrak{p})$ is bounded above by a constant $c_\tau := 1/\#\mathrm{Aut}(\tau)$ which is strictly between 0 and 1; this follows from [19, Lemma 18], [3, Lemma 21], [4, Lemma 20] (see [5] for the definition of $\#\mathrm{Aut}(\tau)$).

Let $Y>0$ be fixed. Then from the results of the last subsection we see that

$$\int_{\mathcal{F}'_{i,X}} \#\{gG_0\cdot v_\sigma \cap \bigcap_{N(\mathfrak{p})<Y} \mathcal{L}^{\mathfrak{p},\neq(\tau)}\}dg \ll X \prod_{N(\mathfrak{p})<Y} \mu_\tau(\mathfrak{p}),$$

where the implied constant only depends on X. Letting Y tend to infinity, we obtain the result. $\square$

Remark: We note that an application of the Selberg Sieve used exactly as in [44] improves the right hand side of (24) to $O(X^{1-1/(5dd_n)+\epsilon})$, where d_n is the dimension of V_n.

4.6 Conclusion

By combining (18), (19), (20), (23), and (24), we obtain

$$\begin{aligned} N(\mathcal{L}^{(\sigma)},\Gamma;X) &= \frac{1}{\#\mathrm{Aut}(\sigma)\mathrm{Vol}(G_0)}\int_{g\in\mathcal{F}}\mathrm{Vol}_{\mathcal{L}}\big((gG_0\cdot v_\sigma)_X\big)dg+o(X) \\ &= \frac{1}{\#\mathrm{Aut}(\sigma)\mathrm{Vol}(G_0)}\int_{g\in G_0}\mathrm{Vol}_{\mathcal{L}}\big((\mathcal{F}g\cdot v_\sigma)_X\big)dg+o(X) \\ &= \frac{1}{\#\mathrm{Aut}(\sigma)}\mathrm{Vol}_{\mathcal{L}}\big(\mathcal{F}(X)\cdot v_\sigma\big)+o(X). \end{aligned} \qquad (25)$$

eqfinalcountnf

Therefore, we have the following theorem.

thmaincountgon **Theorem 18.** *Let $\mathcal{L}\subset V_n(F)$ be a sublattice commensurable with $V_n(\mathcal{O}_S)$ and let $\Gamma\subset G_n(F)$ be a subgroup commensurable with $G_n(\mathcal{O}_S)$ that preserves $\mathcal{L}$. Fix an S-specification σ and $v_\sigma\in V_n(F_S)^{(\sigma)}$. Let $\mathcal{F}(X)$ be a fundamental domain for the action of Γ on $G_n(F_S)^{(\sigma)}_X$ constructed in §4.1. Then*

$$N(\mathcal{L}^{(\sigma)},\Gamma;X)=\frac{1}{\#\mathrm{Aut}(\sigma)}\mathrm{Vol}_{\mathcal{L}}\big(\mathcal{F}(X)\cdot v_\sigma\big)+o(X).$$

Remark: As in the previous subsection, the error term of $o(X)$ in Theorem 18 can be improved to $O_{\mathcal{L}}(X^{1-1/(5dd_n)})$.

5 Congruence conditions and a squarefree sieve

sec:sieve

Let F be a fixed global field and let S again be a nonempty finite set of places of F that contains all the archimedean places. Fix lattices $\Gamma\subset G_n(F)$ and $\mathcal{L}\subset V_n(F)$ that are commensurable with $G_n(\mathcal{O}_S)$ and $V_n(\mathcal{O}_S)$, respectively, and such that Γ preserves $\mathcal{L}$. For each prime ideal $\mathfrak{p}\subset\mathcal{O}_S$, let $Z_\mathfrak{p}$ be a compact subset of $V_n(F_\mathfrak{p})^{\Delta\neq0}$ whose boundary has measure 0 and is preserved by $\Gamma_\mathfrak{p}$, where $\Gamma_\mathfrak{p}$ is the closure of Γ in $G_n(F_\mathfrak{p})$. To such a collection $(Z_\mathfrak{p})_\mathfrak{p}$, we associate the set $Z\subset\mathcal{L}$ consisting of elements $v\in\mathcal{L}$ such that when viewed as an element of $V_n(F_\mathfrak{p})$, $v\in Z_\mathfrak{p}$ for all primes $\mathfrak{p}$ of $\mathcal{O}_S$. Such a set Z is said to be *defined by congruence conditions*. We further say that Z is *large* if for all but finitely many primes $\mathfrak{p}$ in $\mathcal{O}_S$, the set $Z_\mathfrak{p}$ contains all the elements $v\in V_n(\mathcal{O}_\mathfrak{p})$ such that $\theta_{\mathcal{O}_\mathfrak{p}}(v)$ is a maximal rank n ring over $\mathcal{O}_\mathfrak{p}$ and $\theta_{F_\mathfrak{p}}(v)$ is a degree-n étale extension that is either unramified or have splitting type $(1^2\tau)$ where τ is an unramified splitting type of dimension $n-2$. We say $v\in V_n(\mathcal{O}_\mathfrak{p})$ have *extra ramification* if $\theta_{F_\mathfrak{p}}(v)$ is ramified and does not have splitting type $(1^2\tau)$ where τ is an unramified splitting type of dimension $n-2$. When the characteristic of F is not 2, being non-maximal or having extra ramification is equivalent to $\mathfrak{p}^2$ dividing the discriminant. When the characteristic of F is 2, we do not use squarefree discriminants to define largeness since the discriminant is always a square (even as a polynomial)! In this section, we prove the following theorem.

thsieve **Theorem 19.** *Let Z be a large Γ-invariant set as above defined via the local conditions $(Z_\mathfrak{p})_\mathfrak{p}$. Then*

$$N(Z^{(\sigma)},\Gamma;X)=\frac{1}{\#\mathrm{Aut}(\sigma)}\mathrm{Vol}_{\mathcal{L}}(\mathcal{F}(X)\cdot v_\sigma)\prod_{\mathfrak{p}\subset\mathcal{O}_S}\mathrm{Vol}(Z_\mathfrak{p})+o(X), \qquad (26)$$

eqaftersieve

where the volume of $Z_\mathfrak{p}$ is computed with respect to the Haar-measure on $V_n(\mathcal{O}_\mathfrak{p})$ normalized so that the total measure of $\mathcal{L}_\mathfrak{p}$ is 1.

When $Z_\mathfrak{p}=V(\mathcal{O}_\mathfrak{p})$ for all but finitely many primes of $\mathcal{O}_S$, and is defined via finitely many congruence conditions at the other finitely many primes, then Z is a Γ-invariant lattice and the results of Section 4 apply, yielding (26). When Z is defined via infinitely many congruence conditions, then we apply a simple sieve to obtain the result. The key ingredient in this sieve is the following tail estimate.

thunif **Theorem 20.** *For a prime $\mathfrak{p} \subset \mathcal{O}_S$, let $\mathcal{W}_\mathfrak{p}$ denote the set of elements in $V_n(\mathcal{O}_S)$ that are non-maximal or have extra ramification at $\mathfrak{p}$. Then*

$$\sum_{N\mathfrak{p}>M} N(\mathcal{W}_\mathfrak{p}, G_n(\mathcal{O}_S); X) = O(X/(M\log M)) + o(X), \tag{27}$$ equnif

where the implied constants are independent of M and X.

When $F = \mathbb{Q}$, this was proved in [8, §4.2]. Some mild arguments are needed to generalize it to arbitrary global fields. The rest of this section is dedicated to this generalization.

We write $\mathcal{W}_\mathfrak{p}$ as the union $\mathcal{W}_\mathfrak{p}^{(1)} \cup \mathcal{W}_\mathfrak{p}^{(2)}$. The set $\mathcal{W}_\mathfrak{p}^{(1)}$ consists of elements that are non-maximal but does not have extra ramification and the set $\mathcal{W}_\mathfrak{p}^{(2)}$ consists of elements that have extra ramification. When the characteristic of F is not 2, $\mathcal{W}_\mathfrak{p}^{(2)}$ consists of elements whose discriminants are divisible by $\mathfrak{p}^2$ for (mod $\mathfrak{p}$) reasons and we say their discriminants are strongly divisible by $\mathfrak{p}^2$ while for elements of $\mathcal{W}_\mathfrak{p}^{(1)}$, we say their discriminants are weakly divisible by $\mathfrak{p}^2$.

For elements with extra ramification, there exists a subscheme Y of $\mathbb{A}^{d_n}_{\mathcal{O}_S}$ of codimension 2 such that

$$\mathcal{W}_\mathfrak{p}^{(2)} \subset \{v \in V_n(\mathcal{O}_S) : v (\mathrm{mod}\ \mathfrak{p}) \in Y(k(\mathfrak{p}))\}.$$

Recalling the shape of the fundamental domain for the action of $G_n(\mathcal{O}_S)$ on $V_n(F_S)$ in Section 4.1, we see that in order to obtain the estimate (27) for $\mathcal{W}_\mathfrak{p}^{(2)}$, it suffices to obtain the following estimate.

thm:Th7F **Theorem 21.** *Let B be an open bounded region in $V_n(F_S)$, Y be a closed subscheme of $\mathbb{A}^{d_n}_{\mathcal{O}_S}$ of codimension $k \geq 2$ and let M be a positive real number. Let r be a positive real number when F is a number field or an integer when F is a function field of characteristic p along with a fixed embedding of $\mathbb{F}_p(u)$ into F. Let ι denote the embedding of $\mathbb{R}^+$ or $\mathbb{Z}$ in $G_n(F_S)$ described in Section 4.1. Then we have*

$$\begin{aligned} &\#\{a \in \iota(r)B \cap V_n(\mathcal{O}_S) : a (\mathit{mod}\ \mathfrak{p}) \in Y(k(\mathfrak{p}))\ \textit{for some prime}\ \mathfrak{p} \notin S\ \textit{with}\ N\mathfrak{p} > M\} \\ = \quad & O\left(\frac{|\chi(\iota(r))|^2}{M^{k-1}\log M}\right) + o(|\chi(\iota(r))|^2), \end{aligned} \tag{28}$$

as $|\chi(\iota(r))|$ tends to infinity, where the implied constant depends only on B, Y and F.

Proof. Let $\lambda \in F_S$ be such that $\iota(r) = g(\lambda)$. That is, when F is a number field, λ is the adele that is r^κ at all the infinite places and 1 elsewhere; and when F is a function field, λ is the adele that is u^r at all the places of S_∞ and 1 elsewhere. Since $g(\lambda)$ acts on V_n by scaling each coordinate by λ, we see that it scales the volume of any open bounded region by $|\lambda|^{d_n} = |\chi(g(\lambda))|^2$. This explains the order of magnitude in (28). The remainder of the estimate is then a direct generalization of [8, Theorem 3.3]. $\square$

To deal with $\mathcal{W}_\mathfrak{p}^{(1)}$, the key strategy of [8] is that for any $v \in \mathcal{W}_\mathfrak{p}^{(1)}$, there exists an element $g \in G_n(\mathbb{Q})$ such that $\Delta_n(g.v) = \Delta_n(v)/p^2$. Over a general global field, such a global element g might not exist due to the class group. However one can still do it locally. Define $B_\mathfrak{p}^{(1)}$ to be the subset of $V_n(\mathcal{O}_\mathfrak{p})$ consisting of elements that are non-maximal but does not have extra ramification.

Now take any element v of $\mathcal{W}_\mathfrak{p}^{(1)}$. Then its specialization $v_\mathfrak{p}$ when viewed as an element of $V_n(\mathcal{O}_\mathfrak{p})$ is in $B_\mathfrak{p}^{(1)}$. Since $\theta_{\mathcal{O}_\mathfrak{p}}(v_\mathfrak{p})$ is not maximal, there exists $g_\mathfrak{p} \in G_n(F_\mathfrak{p})$ such that $g_\mathfrak{p} v_\mathfrak{p} \in V_n(\mathcal{O}_\mathfrak{p})$ is maximal and with

$$|\Delta_n(g_\mathfrak{p} v_\mathfrak{p})|_\mathfrak{p} \leq |\Delta_n(v_\mathfrak{p})|_\mathfrak{p}/N\mathfrak{p}^2.$$

Consider the adele $g \in G_n(\mathbb{A}_S)$ that equals $g_\mathfrak{p}$ at the place $\mathfrak{p}$ and is 1 everywhere else. From the decomposition (13), there exists $\gamma \in \mathrm{cl}_S$, $h \in G_n(F)$, $h_{\mathfrak{p}'} \in G_n(\mathcal{O}_{\mathfrak{p}'})$ for any $\mathfrak{p}' \notin S$ such that $g' = (h_{\mathfrak{p}'})_{\mathfrak{p}' \notin S}\gamma h$ in $G_n(\mathbb{A}_S)$. Set $v' \in hv \in V_n(F)$. Then v' lies in $\mathcal{L}_\gamma$ with

$$|\Delta_n(v')| \leq C_1 \frac{|\Delta_n(v)|}{N\mathfrak{p}^2}$$

where $C_1 = |\chi(\gamma)|^{-2}$ is a constant depending only on G_n and F. We have therefore defined the following map

$$\pi_{\mathfrak{p}} : G_n(\mathcal{O}_S)\backslash\mathcal{W}_{\mathfrak{p}}^{(1)} \to \bigcup_{\gamma\in \mathrm{cl}_S} \Gamma_\gamma\backslash\mathcal{L}_\gamma$$

such that $|\Delta_n(\pi_{\mathfrak{p}}(v))| = C_1|\Delta_n(v)|/N\mathfrak{p}^2$. We remark that the choice of γ is unique as it is determined by the field extension corresponding to v (Theorem 11).

Finally the same argument as in [8, §4.2] shows that the fibers of $\pi_{\mathfrak{p}}$ have absolutely bounded sizes (in fact, they have cardinality at most 10). Hence we conclude that

$$N(\mathcal{W}_{\mathfrak{p}}^{(1)}, G_n(\mathcal{O}_S); X) = O(X/N\mathfrak{p}^2).$$

Summing over primes $\mathfrak{p}$ such that $N\mathfrak{p} > M$ gives the desired estimate (27) for $\mathcal{W}_{\mathfrak{p}}^{(1)}$, and we have proven Theorem 20.

Theorem 19 now follows from Theorems 18 and 20 via a sifting argument just as in [15, §2.7].

Remark: The error term of Theorem 19 can be improved as follows: first, note that by repeating the arguments of §4, the error term of Theorem 20 can be improved to $O(X/(M\log M) + X^{1-1/\epsilon'_n})$, where $\epsilon'_2 = 2d$, $\epsilon'_3 = 6d$, $\epsilon'_4 = 12d$, and $\epsilon'_5 = 40d$. Second, we use the inclusion exclusion sieve instead of a sifting argument to recover Theorem 19 from Theorems 18 and 20. Finally, from the improvement to Theorem 18 explained in the remark immediately following it, we see that the error term of Theorem 19 can be improved to $O_Z(X^{1-1/(5dd_n)})$.

6 Application to field counting

sec: fieldscounting

Let F be a fixed global field. Suppose the characteristic of F is not 2 when $n = 2$. Let S be a nonempty finite set of primes of F containing M_∞. Suppose S contains all places above 2 when $n = 2$. Let $\Sigma = (\Sigma_{\mathfrak{p}})$ be an acceptable collection of local specifications for degree-n extensions of F, such that $\Sigma_{\mathfrak{p}}$ for $\mathfrak{p} \in S$ consists of only one isomorphism class of extension of $F_{\mathfrak{p}}$. Thus $(\Sigma_{\mathfrak{p}})_{\mathfrak{p}\in S}$ defines an S-specification σ.

Let $N_{\Sigma,S}(\mathcal{L}_\beta, \Gamma_\beta; X)$ denote the number of Γ_β-orbits of elements v of $\mathcal{L}_\beta$ such that $|\Delta_n(v)|_S$ is at most X if F is a number field and is equal to X if F is a function field and such that $\theta_{F_{\mathfrak{p}}}(v) \in \Sigma_{\mathfrak{p}}$ for every prime $\mathfrak{p} \in S$, and $\theta_{\mathcal{O}_{\mathfrak{p}}}(v)$ is the ring of integers of a degree-n extension of $F_{\mathfrak{p}}$ contained in $\Sigma_{\mathfrak{p}}$ for every prime $\mathfrak{p} \notin S$. For any prime $\mathfrak{p} \notin S$, we write $V_n(\mathcal{O}_{\mathfrak{p}})^{\max}_{\Sigma_{\mathfrak{p}}}$ for the subset of $V_n(\mathcal{O}_{\mathfrak{p}})^{\max}$ consisting of elements whose $G(F_{\mathfrak{p}})$-orbit corresponds to a degree-n étale extension of $F_{\mathfrak{p}}$ contained in $\Sigma_{\mathfrak{p}}$.

We summarize the results of the previous sections in the following theorem.

thsieve22 **Theorem 22.** *With notations as above, we have*

$$N_{\Sigma,S}(\mathcal{L}_\beta, \Gamma_\beta; X) = \frac{\mathrm{Vol}_{\mathcal{L}_\beta}(\mathcal{F}(X)\cdot v_\sigma)}{\#\mathrm{Aut}(\sigma)} \prod_{\mathfrak{p}\notin S} \frac{\mathrm{Vol}_{\mathfrak{p}}(V_n(\mathcal{O}_{\mathfrak{p}})^{\max}_{\Sigma_{\mathfrak{p}}})}{\mathrm{Vol}_{\mathfrak{p}}(V_n(\mathcal{O}_{\mathfrak{p}}))} + o(X). \quad (29)$$ eq:sieve2

Let $N_{\Sigma,S}(F, \beta; X)$ denote the number of étale extensions L over F of degree n such that its normal closure has Galois group S_n, its local specification is contained in Σ, at places outside of S its S-Steinitz class is $(\chi(\beta))$, and the norm of the S-discriminant of L is at most X if F is a number field and equal to X if F is a function field. Suppose L is one such field corresponding to some $v \in \mathcal{L}_\beta^{\max}$. Theorem 11 gives the following equality of $\mathcal{O}_S$ fractional ideals,

$$\mathrm{Disc}_S(L) = (\chi(\beta))^2(\Delta_n(v)).$$

The norm of the ideal $\mathrm{Disc}_S(L)$ is then

$$N(\mathrm{Disc}_S(L)) = \prod_{\mathfrak{p}\notin S} |\mathrm{Disc}_S(L)|_{\mathfrak{p}}^{-1} = |\chi(\beta)|^{-2} \prod_{\mathfrak{p}\notin S} |\Delta_n(v)|_{\mathfrak{p}}^{-1} = |\chi(\beta)|^{-2} \prod_{\mathfrak{p}\in S} |\Delta_n(v)|_{\mathfrak{p}}. \quad (30)$$ eq:Snorm

Hence to count fields such that the norm of the S-discriminant is bounded by X, we may count Γ_β-orbits in $\mathcal{L}_\beta^{\max}$ such that the S-norm is bounded by $|\chi(\beta)|^2 X$. In other words,

$$N_{\Sigma,S}(F,\beta;X) = N_{\Sigma,S}(\mathcal{L}_\beta,\Gamma_\beta;|\chi(\beta)|^2X). \tag{31}$$

eq:numberoffields

We now compute all the local volumes appearing in (29). We abbreviate V_n, G_n to V, G.

7 Computing the product of local volumes

sec:volume

7.1 From volumes in V to volumes in G: Jacobian change of variable

Observe first that the groups and the representations that we have been using are all defined over $\mathbb{Z}$. Let $\underline{G}$ and $\underline{V}$ denote the corresponding group and vector space defined over $\mathbb{Z}$ so that G and V are the base changes of $\underline{G}$ and $\underline{V}$, respectively, to F. Let ω_G (resp. ω_V) be a top degree left-invariant differential form that generates the rank 1 module of top degree left-invariant differential forms on $\underline{G}$ (resp. $\underline{V}$). Then ω_G and ω_V are well-defined up to sign. They induce Haar measures $\omega_{G,\mathfrak{p}}, \omega_{G,S}$ on $G(F_\mathfrak{p})$ and $G(F_S)$ and similarly for V. Since V is a direct sum of copies of $\mathbb{G}_a$, the volume of $V(\mathcal{O}_\mathfrak{p})$ computed with respect to $\omega_{V,\mathfrak{p}}$ is 1 for every finite prime and the covolume of $\mathcal{O}_S$ in $V(\mathcal{O}_S)$ is $\sqrt{D_F}^{\dim V}$ where D_F is the absolute discriminant of F (see [48, §2.1.1]). Hence, we have

$$\mathrm{Vol}_{\mathcal{L}_\beta}(\mathcal{F}(X)\cdot v_\sigma) = \sqrt{D_F}^{-\dim V}\,|\chi(\beta)|^{-2}\int_{\mathcal{F}(X)\cdot v_\sigma}\omega_{V,S}(v). \tag{32}$$

eq:covolume

We wish to the compute the volumes of $\mathcal{F}(X)\cdot v_\sigma$ in $V(F_S)$ and of $V(\mathcal{O}_\mathfrak{p})^{\max}_{\Sigma_\mathfrak{p}}$ in $V(F_\mathfrak{p})$ by the volumes of $\mathcal{F}(X)$ in $G(F_S)$ and $G(\mathcal{O}_\mathfrak{p})$ in $G(F_\mathfrak{p})$ respectively. To do this, we require a Jacobian change-of-variable formula.

Let v be the generic point of $\underline{V}$. We have a morphism $\pi_v : \underline{G} \to \underline{V}$ defined over $\mathbb{Z}$ sending g to $\pi_v(g) = g.v$. Then there exists a polynomial $J : \underline{V} \to \mathbb{G}_a$ such that

$$(\pi_v^*\omega_V)(g) = J(v)\chi(g)^2\omega_G(g) \tag{33}$$

eqjac1

since the top degree form $(\pi_v^*\omega_V)(g)/\chi(g)^2$ is left-invariant on G (over $\mathbb{Z}$). For any $h \in \underline{G}$, considering the map $g \mapsto gh \mapsto gh.v$ shows that $J(h.v) = \chi(h)^2 J(v)$. This shows that J is an integer $\mathcal{J}$ times the relative invariant $\Delta_n(v)$.

We have the following proposition computing the value of $\mathcal{J}$.

propJvalue **Proposition 23.** *Let $\mathcal{J}$ be as above. Then $\mathcal{J} = 2$ when $n = 2$ and $\mathcal{J} = \pm 1$ when $n = 3, 4, 5$.*

Proof. When $n = 2$, the group $\underline{G_2} = \mathbb{G}_m$ acts on $\underline{V_2} = \mathbb{G}_a$ via $g \cdot v = g^2 v$. We tale $\omega_G = g^{-1}dg$ and $\omega_V = dv$. It is then easy to compute $\mathcal{J}$ to be 2.

When $n = 3, 4, 5$, we use Theorem 8 for the rings $\mathbb{Z}_p$ and $\mathbb{F}_p$ to compute the value of $|\mathcal{J}|_p$ for all primes p. Consider the set Y of elements in $\underline{V}(\mathbb{Z}_p)$ whose $\underline{G}(\mathbb{Z}_p)$-orbit corresponds to the rank n ring $\mathbb{Z}_p^n$. The set Y is a single $\underline{G}(\mathbb{Z}_p)$-orbit and the size of the stabilizer in $\underline{G}(\mathbb{Z}_p)$ of an element in Y is $n!$. From (33), we obtain

$$\mathrm{Vol}(Y) = \frac{|\mathcal{J}|_p}{n!}\mathrm{Vol}(\underline{G}(\mathbb{Z}_p)), \tag{34}$$

eqjp1

where the volumes of Y and $\underline{G}(\mathbb{Z}_p)$ are computed with respect to the measures induced by ω_V and ω_G, respectively.

The reduction $\bar{Y}$ of Y in $\underline{V}(\mathbb{F}_p)$ corresponds to the ring extension $\mathbb{F}_p^n$ of $\mathbb{F}_p$, and consists of a single $\underline{G}(\mathbb{F}_p)$-orbit. The size of the stabilizer in $\underline{G}(\mathbb{F}_p)$ of an element in $\bar{Y}$ is again $n!$. Hence we have $\#\bar{Y} = \#\underline{G}(\mathbb{F}_p)/n!$. The set Y is the inverse image of $\bar{Y}$ under the reduction modulo p map. Indeed if $v \in \underline{V}(\mathbb{Z}_p)$ such that the $\theta_{\mathbb{F}_p}(v \bmod \mathfrak{p}) = \mathbb{F}_p^n$, then $\Delta_n(v)$ is nonzero modulo p. Hence $\theta_{\mathbb{Q}_p}(v)$ is a product of unramified extensions of $\mathbb{Q}_p$, $\theta_{\mathbb{Z}_p}(v)$ is the product of their rings of integers and $\theta_{\mathbb{F}_p}(v$

mod $\mathfrak{p}$) is the product of their residue fields. Since all of these residue fields are $\mathbb{F}_p$ and the extensions of $\mathbb{Q}_p$ are unramified, it follows that the $\theta_{\mathbb{Q}_p}(v) = \mathbb{Q}_p^n$ and $v \in Y$. Hence we have

$$\mathrm{Vol}(Y) = \frac{\#\bar{Y}}{p^{\dim \underline{V}}} = \frac{1}{n!}\frac{\#\underline{G}(\mathbb{F}_p)}{p^{\dim \underline{G}}}, \tag{35}$$ eqjp2

since the dimension of $\underline{G}$ equals the dimension of $\underline{V}$. Finally by Hensel's lemma (cf. [33, Proposition 4.7]),

$$\mathrm{Vol}(\underline{G}(\mathbb{Z}_p)) = \frac{\#\underline{G}(\mathbb{F}_p)}{p^{\dim \underline{G}}}. \tag{36}$$ eqjp3

Combining equations (34), (35), and (36) gives $|\mathcal{J}|_p = 1$ for all primes p. Alternately, one can compute $\mathcal{J}$ by an explicit computation in the three cases. $\square$

We thus have the following Jacobian change of variable formula.

prop:Jchange **Proposition 24.** *Suppose the characteristic of F is not 2 if $n = 2$. Then there exists a constant $\mathcal{J} \in F^\times$ such that for any place $\mathfrak{p}$ of F, any nonzero element v_0 of $V(F_\mathfrak{p})$, any measurable function φ on $V(F_\mathfrak{p})$ and any measurable subset $\mathcal{F}$ of $G(F_\mathfrak{p})$, we have*

$$\int_{\mathcal{F}.v_0} \varphi(v)\omega_{V,\mathfrak{p}}(v) = |\Delta_n(v_0)|_\mathfrak{p}|\mathcal{J}|_\mathfrak{p}\int_{\mathcal{F}} \varphi(g.v_0)|\chi(g)|_\mathfrak{p}^2\omega_{G,\mathfrak{p}}(g), \tag{37}$$ eq:Jchange

where as before $\mathcal{F}.v_0$ is viewed as a multiset so that it is in bijection with $\mathcal{F}$. The value of $\mathcal{J}$ is 2 when $(G,V) = (G_2,V_2)$ and the value of $\mathcal{J}$ is ± 1 when $(G,V) = (G_n,V_n)$ for $n = 3,4,5$.

We recall the definition of $\mathcal{F}(X)$ from §4.1. Let Ω denote a fundamental domain for the action of Γ_β on $G(F_S)^1$ by left multiplication. When F is a number field, let Λ_X denote the image $\iota((0,(X/|\Delta_n(v_\sigma)|)^{1/2}])$ where ι is the embedding of $\mathbb{R}^+$ in $G(F_S)$ normalized such that $|\chi(\iota(r))| = r$ for every $r \in \mathbb{R}^+$. When F is a function field, let Λ_X denote an arbitrary element of $G(F_S)^{(\sigma)}_X$. Using Proposition 24, we obtain the following result:

$$\int_{\mathcal{F}(X)\cdot v_\sigma} \omega_{V,S}(v) = \begin{cases} |\Delta_n(v_\sigma)|\Big(\prod_{\mathfrak{p}\in S}|\mathcal{J}|_\mathfrak{p}\Big)\int_{\Lambda_X\Omega}|\chi(g)|^2\omega_{G,S}(g) & \text{if } F \text{ is a number field,}\\ X\Big(\prod_{\mathfrak{p}\in S}|\mathcal{J}|_\mathfrak{p}\Big)\int_{\Omega}\omega_{G,S}(g) & \text{if } F \text{ is a function field.}\end{cases} \tag{38}$$ eq:volinftyS2

For $V(\mathcal{O}_\mathfrak{p})^{\max}_{\Sigma_\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_S$, we break it up into $G(\mathcal{O}_\mathfrak{p})$-orbits:

$$V(\mathcal{O}_\mathfrak{p})^{\max}_{\Sigma_\mathfrak{p}} = \bigcup_{v_\mathfrak{p}\in G(\mathcal{O}_\mathfrak{p})\backslash V(\mathcal{O}_\mathfrak{p})^{\max}_{\Sigma_\mathfrak{p}}} G(\mathcal{O}_\mathfrak{p})v_\mathfrak{p}.$$

By Theorem 8, each orbit $G(\mathcal{O}_\mathfrak{p})v_\mathfrak{p}$ in $V(\mathcal{O}_\mathfrak{p})^{\max}_{\Sigma_\mathfrak{p}}$ corresponds uniquely to an étale extension K over $F_\mathfrak{p}$ of degree n with $|\Delta_n(v_\mathfrak{p})|_\mathfrak{p} = |\mathrm{Disc}(K/F_\mathfrak{p})|_\mathfrak{p}$ and $K \in \Sigma_\mathfrak{p}$, so

$$\begin{aligned}\int_{G(\mathcal{O}_\mathfrak{p})v_\mathfrak{p}} \omega_{V,\mathfrak{p}}(v) &= \frac{1}{\#\,\mathrm{Stab}_{G(\mathcal{O}_\mathfrak{p})}(v_\mathfrak{p})}\int_{G(\mathcal{O}_\mathfrak{p}).v_\mathfrak{p}}\omega_{V,\mathfrak{p}}(v)\\ &= \frac{1}{\#\,\mathrm{Stab}_{G(F_\mathfrak{p})}(v_\mathfrak{p})}|\Delta_n(v_\mathfrak{p})|_\mathfrak{p}|\mathcal{J}|_\mathfrak{p}\int_{G(\mathcal{O}_\mathfrak{p})}\omega_{G,\mathfrak{p}}(g)\\ &= \frac{|\mathrm{Disc}(K/F_\mathfrak{p})|_\mathfrak{p}}{\#\mathrm{Aut}(K/F_\mathfrak{p})}|\mathcal{J}|_\mathfrak{p}\int_{G(\mathcal{O}_\mathfrak{p})}\omega_{G,\mathfrak{p}}(g).\end{aligned}$$

Hence adding up all the $G(\mathcal{O}_\mathfrak{p})$-orbits gives

$$\int_{V(\mathcal{O}_\mathfrak{p})^{\max}_{\Sigma_\mathfrak{p}}} \omega_{V,\mathfrak{p}}(v) = \Big(\sum_{K\in\Sigma_\mathfrak{p}} \frac{|\mathrm{Disc}(K/F_\mathfrak{p})|_\mathfrak{p}}{\#\mathrm{Aut}(K/F_\mathfrak{p})} \Big) |\mathcal{J}|_\mathfrak{p} \int_{G(\mathcal{O}_\mathfrak{p})} \omega_{G,\mathfrak{p}}(g) = \frac{N\mathfrak{p}}{N\mathfrak{p}-1} m_{\mathfrak{p},S}(\Sigma_\mathfrak{p}) |\mathcal{J}|_\mathfrak{p} \int_{G(\mathcal{O}_\mathfrak{p})} \omega_{G,\mathfrak{p}}(g), \tag{39}$$

eq:volp2

where recall $m_{\mathfrak{p},S}(\Sigma_\mathfrak{p})$ is defined by

$$m_{\mathfrak{p},S}(\Sigma_\mathfrak{p}) = \frac{N\mathfrak{p}-1}{N\mathfrak{p}} \sum_{K\in\Sigma_\mathfrak{p}} \frac{|\mathrm{Disc}(K/F_\mathfrak{p})|_\mathfrak{p}}{\#\mathrm{Aut}(K/F_\mathfrak{p})}.$$

We now combine (31), (32), (38) and (39). Note that the local factors $|\mathcal{J}|_\mathfrak{p}$ cancel out due to the product formula. We summarize our computation in the following proposition.

prop:VtoG **Proposition 25.** *With notations as above, we have*

$$N_{\Sigma,S}(F,\beta;X) = \frac{\sqrt{D_F}^{-\dim V} |\chi(\beta)|^{-2} |\Delta_n(v_\sigma)|}{\#\mathrm{Aut}(\sigma)} \prod_{\mathfrak{p}\notin S} \Big(m_{\mathfrak{p},S}(\Sigma_\mathfrak{p}) \frac{N\mathfrak{p}}{N\mathfrak{p}-1} \int_{G(\mathcal{O}_\mathfrak{p})} \omega_{G,\mathfrak{p}}(v) \Big) \int_{\Lambda_{|\chi(\beta)|^2 X}\Omega} |\chi(g)|^2 \omega_{G,S}(g) + o(X)$$

if F is a number field, and

$$N_{\Sigma,S}(F,\beta;X) = \frac{\sqrt{D_F}^{-\dim V} X}{\#\mathrm{Aut}(\sigma)} \prod_{\mathfrak{p}\notin S} \Big(m_{\mathfrak{p},S}(\Sigma_\mathfrak{p}) \frac{N\mathfrak{p}}{N\mathfrak{p}-1} \int_{G(\mathcal{O}_\mathfrak{p})} \omega_{G,\mathfrak{p}}(v) \Big) \int_{\Omega} \omega_{G,S}(g) + o(X)$$

if F is a function field.

7.2 Product of the volumes over G: Tamagawa number

sec:product

We now compute the product of the local volumes over G using the Tamagawa number. See Section 2.3 for the definition of the Tamagawa number of a reductive group over a global field where the (global) character group has rank 1. The Tamagawa number of $G = G_n$ is 1 for $n = 2, 3, 4, 5$. Note also that $\dim G = \dim V$.

When F is a number field, we have

$$\begin{aligned} & \sqrt{D_F}^{-\dim V} |\chi(\beta)|^{-2} |\Delta_n(v_\sigma)| \Big(\prod_{\mathfrak{p}\notin S} \frac{N\mathfrak{p}}{N\mathfrak{p}-1} \int_{G(\mathcal{O}_\mathfrak{p})} \omega_{G,\mathfrak{p}}(v) \Big) \int_{\Lambda_{|\chi(\beta)|^2 X}\Omega} |\chi(g)|^2 \omega_{G,S}(g) \\ = \quad & |\chi(\beta)|^{-2} |\Delta_n(v_\sigma)| \operatorname*{Res}_{s=1} \zeta_S(s)\, \tau_G^1 \big(\prod_{\mathfrak{p}\notin S} G(\mathcal{O}_\mathfrak{p}) \times \Omega \big) \int_0^{(|\chi(\beta)|^2 X/|\Delta_n(v_\sigma)|)^{1/2}} \lambda^2 d^\times \lambda \\ = \quad & \frac{1}{2} \operatorname*{Res}_{s=1} \zeta_S(s) X\, \tau_G^1 \big(\prod_{\mathfrak{p}\notin S} G(\mathcal{O}_\mathfrak{p}) \times \Gamma_\beta \backslash G(F_S)^1 \big). \end{aligned}$$

When F is a function field over $\mathbb{F}_q$, we have

$$\sqrt{D_F}^{-\dim V} X \Big(\prod_{\mathfrak{p}\notin S} \frac{N\mathfrak{p}}{N\mathfrak{p}-1} \int_{G(\mathcal{O}_\mathfrak{p})} \omega_{G,\mathfrak{p}}(v) \Big) \int_\Omega \omega_{G,S}(g) = \log q \operatorname*{Res}_{s=1} \zeta_S(s) X\, \tau_G^1 \big(\prod_{\mathfrak{p}\notin S} G(\mathcal{O}_\mathfrak{p}) \times \Gamma_\beta \backslash G(F_S)^1 \big).$$

Hence by Proposition 25,

$$N_{\Sigma,S}(F,\beta;X) = c \frac{\mathrm{Res}_{s=1} \zeta_S(s) X}{\#\mathrm{Aut}(\sigma)} \tau_G^1 \big(\prod_{\mathfrak{p}\notin S} G(\mathcal{O}_\mathfrak{p}) \times \Gamma_\beta \backslash G(F_S)^1 \big) \prod_{\mathfrak{p}\notin S} m_{\mathfrak{p},S}(\Sigma_\mathfrak{p}) + o(X), \tag{40}$$

eq:VtoGtotau

where $c = \frac{1}{2}$ when F is a number field and $\log q$ when F is a global field over $\mathbb{F}_q$.

8 Proof of the main theorems

sec:proof

In this section we prove Theorems 1, 2 and 4 in the case where the characteristic of F is not 2 when $n=2$. In Theorem 4, we also assume that S contains all the places above 2 when $n=2$. In the next section, we handle the case of quadratic extensions in any characteristic and any S using a different representation.

We prove Theorem 4 first. Let $\Sigma=(\Sigma_{\mathfrak p})$ be an acceptable collection of local specifications. For every S-specification σ allowed in Σ, let $\Sigma(\sigma)$ denote the subset of Σ where the local specifications at places of S are given by σ. Summing up (40) over all the β, using the formula

$$\tau_G^1(G(F)\backslash G(\mathbb{A})^1)=\sum_{\beta\in \mathrm{cl}_S}\tau_G^1\Big(\prod_{\mathfrak p\notin S}G(\mathcal{O}_{\mathfrak p})\times\Gamma_\beta\backslash G(F_S)^1\Big),$$

and the fact that the Tamagawa number of G is 1, we obtain

$$\sum_{\beta\in\mathrm{cl}_S}N_{\Sigma(\sigma),S}(F,\beta;X)=c\ \mathrm{Res}_{s=1}\,\zeta_S(s)X\frac{1}{\#\mathrm{Aut}(\sigma)}\prod_{\mathfrak p\notin S}m_{\mathfrak p,S}(\Sigma_{\mathfrak p})+o(X). \tag{41}$$ eq: VtoGtotausumbeta

Adding up the S-specifications σ then gives the desired equation (6).

Finally we prove Theorem 2. Let $\Sigma=(\Sigma_{\mathfrak p})$ be an acceptable collection of local specifications. Let S be any nonempty finite set of places containing M_∞ and when $n=2$ and F is a number field, all the places above 2. Fix any S-specification $\sigma=(L_{\mathfrak p})_{\mathfrak p\in S}$ allowed in Σ. Define

$$\mathrm{Disc}(\sigma)=\prod_{\mathfrak p\in S-M_\infty}|\mathrm{Disc}(L_{\mathfrak p}/F_{\mathfrak p})|_{\mathfrak p}.$$

Suppose L is a degree-n extension of F whose normal closure has Galois group S_n and has local specification σ at places of S. Then

$$N(\mathrm{Disc}_S(L))=N(\mathrm{Disc}(L/F))\mathrm{Disc}(\sigma).$$

Hence, we have

$$\begin{aligned}
N_n(F,X) &= \sum_{\sigma}\sum_{\beta\in\mathrm{cl}_S}N_{\Sigma(\sigma),S}(F,\beta;X\mathrm{Disc}(\sigma))\\
&= c\ \mathrm{Res}_{s=1}\,\zeta_S(s)X\sum_{\sigma}\frac{\mathrm{Disc}(\sigma)}{\#\mathrm{Aut}(\sigma)}\prod_{\mathfrak p\notin S}m_{\mathfrak p,S}(\Sigma_{\mathfrak p})+o(X)\\
&= c\ \mathrm{Res}_{s=1}\,\zeta_S(s)X\prod_{\mathfrak p\in M_\infty}\sum_{K\in\Sigma_{\mathfrak p}}\frac{1}{\#\mathrm{Aut}(K/F_{\mathfrak p})}\prod_{\mathfrak p\notin M_\infty}\sum_{K\in\Sigma_{\mathfrak p}}\frac{|\mathrm{Disc}(K/F_{\mathfrak p})|_{\mathfrak p}}{\#\mathrm{Aut}(K/F_{\mathfrak p})}.
\end{aligned}$$

We have now proved Theoerem 2. Theorem 1 then follows from the formulae (9), (10), (11) for the masses.

9 Quadratic extensions of global fields

sec:quadratic

In this section, we count quadratic extensions of global fields, thereby finishing the proof of Theorems 1, 2, and 4. The R-orbits of the representation (G_2,V_2) described in Section 3 do not yield all quadratic extensions of a PID R if 2 is not invertible in R. To obtain a proof of the main theorems in the case $n=2$ that is uniform over global fields of all characteristics, we consider the following representation V of G, where for a ring R we have

$$\begin{aligned}
G(R) &= \Big\{\begin{pmatrix}1&\\ n&\lambda\end{pmatrix}:n\in R,\lambda\in R^\times\Big\},\\
V(R) &= \{x^2+axy+by^2:a,b\in R\}.
\end{aligned}$$

The group G acts on V via the action $\gamma \cdot f(x,y) = f((x,y)\cdot\gamma)$ for $\gamma \in G$ and $f \in V$. Note that the group G is not reductive. The techniques in Sections 3 through 8 do not apply generally to representations of non-reductive groups. However, they do apply in our case.

9.1 Parametrization of quadratic extensions

The ring of relative invariants for the action of G on V is freely generated by one element, namely, the discriminant $\Delta(f) = a^2 - 4b$ of the binary quadratic form $x^2 + axy + by^2$. The group of characters of G is generated by the determinant. For $\gamma \in G$ and $f \in V$, we have

$$\Delta(\gamma \cdot f) = \det(\gamma)^2 \Delta(f).$$

Let R be a fixed ring. Given an element $f \in V(R)$, we can construct a ring

$$R_f := R[x]/f(x,1)$$

that is rank-2 as an R module. The ring R_f is generated (as a module) by the elements 1 and x, and the ring structure on R_f is determined by the equation $x^2 = -ax - b$. There are two automorphisms of R_f over R: the trivial automorphism, and σ defined by $\sigma(1) = 1$ and $\sigma(x) = -a - x$. Note these two automorphisms are the same precisely when F has characteristic 2 and $\Delta(f) = 0$. We can then compute the discriminant of R_f over R to be

$$\operatorname{disc}(R_f) = \det\begin{pmatrix} 1 & x \\ 1 & -a-x \end{pmatrix}^2 = a^2 - 4b$$

and verify that

$$\operatorname{disc}(R_f) = \Delta(f).$$

Clearly, the ring R_f is independent of the $G(R)$-orbit of f.

Conversely, suppose R is a PID. If R' is a rank-2 ring over R, then we may find a basis of the form $\{1, \omega\}$ is for R' as a module over R and the ring structure of R' is determined by the equation $\omega^2 = -a\omega - b$ for some $a, b \in R$. Thus $R' \cong R_f$ for $f(x,y) = x^2 + axy + by^2$. The choice of w is well-defined up to $w \mapsto \lambda w - n$ for any $\lambda \in R^\times$ and $n \in R$. The effect on the multiplication table is exactly as the action of $G(R)$ on $V(R)$.

We therefore have the following theorem.

thparam2 **Theorem 26.** *Let R be a PID. There is a bijection between the set of $G(R)$-orbits on $V(R)$ and the set of rank-2 rings over R. For any $f \in V(R)$, with the additional assumption that $\Delta(f) \neq 0$ if F has characteristic 2, we have*

$$\operatorname{Aut}(R_f) \cong \operatorname{Stab}_{G(R)}(f) \cong \mathbb{Z}/2\mathbb{Z},$$

where R_f is the ring corresponding to R.

Proof. Only the last assertion requires proof. The automorphism group of R_f is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, independent of f. The theorem follows since the stabilizer in $G(R)$ of an element $f = x^2 + axy + by^2$ in $V(R)$ consists of two elements, namely the identity and the matrix $\begin{pmatrix} 1 & \\ a & -1 \end{pmatrix}$ in $G(R)$. □

The finiteness of class numbers for any affine algebraic group of finite type over a global field is proved by Borel [25, Theorem 5.1] in the number field case and by Conrad [27, Theorem 1.3.1] in the function field case. For the group G, this finiteness follows from a much easier argument (see below). The parametrization theorem for quadratic field extensions (cf. Theorem 11) then follows formally as in Section 3.

9.2 Class group, Tamagawa measure and reduction theory

The group G fits in a split exact sequence where i sends n to the matrix $\begin{pmatrix} 1 & \\ n & 1 \end{pmatrix}$ and j sends λ to the diagonal matrix $\begin{pmatrix} 1 & \\ & \lambda \end{pmatrix}$. Hence as far as the class group, the Tamagawa measure and the reduction theory of G are concerned, G behaves just like the cartesian product $\mathbb{G}_a \times \mathbb{G}_m$. More precisely, let S be any nonempty set of places of F containing M_∞. Then the maps $i : \mathbb{G}_a \to G$ and $j : \mathbb{G}_m \to G$ define the following bijections of sets

$$\begin{aligned}
\Big(\prod_{\mathfrak{p}\notin S} G(\mathcal{O}_\mathfrak{p})\Big)\backslash G(\mathbb{A}_S)/G(F) &\simeq \Big(\prod_{\mathfrak{p}\notin S} \mathbb{G}_a(\mathcal{O}_\mathfrak{p})\Big)\backslash \mathbb{G}_a(\mathbb{A}_S)/\mathbb{G}_a(F) \times \Big(\prod_{\mathfrak{p}\notin S} \mathbb{G}_m(\mathcal{O}_\mathfrak{p})\Big)\backslash \mathbb{G}_m(\mathbb{A}_S)/\mathbb{G}_m(F) \\
&= \Big(\prod_{\mathfrak{p}\notin S} \mathbb{G}_m(\mathcal{O}_\mathfrak{p})\Big)\backslash \mathbb{G}_m(\mathbb{A}_S)/\mathbb{G}_m(F) \\
G(\mathbb{A})^1 &\simeq \mathbb{G}_a(\mathbb{A}) \times \mathbb{G}_m(\mathbb{A})^1 \\
G(F)\backslash G(\mathbb{A})^1 &\simeq \mathbb{G}_a(F)\backslash\mathbb{G}_a(\mathbb{A}) \times \mathbb{G}_m(F)\backslash\mathbb{G}_m(\mathbb{A})^1 \\
G(\mathcal{O}_S)\backslash G(F_S)^1 &\simeq \mathbb{G}_a(\mathcal{O}_S)\backslash\mathbb{G}_a(F_S) \times \mathbb{G}_m(\mathcal{O}_S)\backslash\mathbb{G}_m(F_S)^1
\end{aligned}$$

The first bijection gives the finiteness of the class group of G. The second bijection defines the Tamagawa measure on $G(\mathbb{A})^1$. The third bijection shows that the Tamagawa number of G is 1. Finally, the last bijection gives a fundamental domain for the action of $G(\mathcal{O}_S)$ on $G(F_S)^1$. Note now once the height condition is imposed, the fundamental domain will be bounded so no cusp analysis needs to be done and the asymptotic for the number of integral orbits (cf. Theorem 18) follows as in Section 4. We note that in general, the main difficulty with non-reductive groups is the cusp analysis, which does not pose an issue for us in this case because the group is very simple.

9.3 Congruence conditions and a maximal sieve

Next we impose infinitely many congruence conditions to go from counting integral orbits to counting field extensions as in Sections 5 and 6. Since we are working with degree-2 extensions, there are no extra ramifications. The needed maximal sieve (cf. Theorem 20) then follows from the same method in Section 5 that dealt with $\mathcal{W}_\mathfrak{p}^{(1)}$.

We note that this argument implies that if R_f is non-maximal, then after a change of variable using an element of $G(\mathcal{O}_\mathfrak{p})$, $f(x,y) = x^2 + axy + by^2$ with $a \in \mathfrak{p}$ and $b \in \mathfrak{p}^2$. This is also evident from the parametrization of quadratic rings above. Indeed, if R_f is strictly contained in a rank-2 ring R'_f with basis $\{1, w\}$, then there exists a positive integer k such that $\{1, \pi_\mathfrak{p}^k w\}$ is a basis for R_f where $\pi_\mathfrak{p}$ is a uniformizer of $\mathcal{O}_\mathfrak{p}$. From the multiplication table we see that $a \in \mathfrak{p}^k$ and $b \in \mathfrak{p}^{2k}$. Note when the characteristic of F is 2, we have $\Delta(f) = a^2$ and so $\mathfrak{p}^2 \mid \Delta(f)$ if and only if $\mathfrak{p} \mid a$. This illustrates why squarefree-ness is not the correct condition to use in characteristic 2.

We now have the asymptotic for the number of quadratic extensions of an arbitrary global field in terms of various local volumes in V (cf. Theorem 22 and equation (31)).

9.4 Proof of the main theorems

We perform volume computations by pulling back to G as in Section 7. Since our parametrization theorem now works for any PID, the proof of Proposition 23 in the case $n = 3, 4, 5$ applies to show that $\mathcal{J} = \pm 1$. Alternatively, one may compute it directly using the differential forms $\omega_V = da \wedge db$, $\omega_G = \lambda^{-1} dn \wedge d^\times\lambda$ and the orbit map given by

$$\begin{pmatrix} 1 & \\ n & \lambda \end{pmatrix}.(a,b) = (\lambda a + 2n, \lambda^2 b + \lambda n a + n^2).$$

The Jacobian change of variable formula (cf. Proposition 24) then holds in any characteristic. We have shown above that the Tamagawa number of G is 1 and so we have the analogous cancelations to those in Section 7.2.

Finally Theorems 1, 2, and 4 follow from the same formal argument as in Section 8.

10 Unramified extensions of number fields

In this section, we prove Theorems 6 and 7. Before turning to the proofs of these theorems, we introduce the notion of splitting types. Let K be a local field and let L be a finite etale extension of K. Then $L = L_1 \oplus \cdots \oplus L_k$ is a sum of local field extensions of K. We say that the *splitting type* of L/K is $(f_1^{e_1} \dots f_k^{e_k})$, where f_i is the local degree of L_i/K and e_i is the ramification degree of L_i/K. If K is archimedian, we set $f_i = [L_i : K]$ and $e_i = 1$ for all i. For a global field F, a finite extension L/F, and a place $\mathfrak{p}$ of K, we say that the *splitting type* of L/F at $\mathfrak{p}$ is the splitting type of $L \otimes F_{\mathfrak{p}}/F_{\mathfrak{p}}$.

10.1 Proof of Theorem 6

Let F be a fixed global field. We first compute the average size of the 3-torsion subgroups of the relative class groups of quadratic extensions of F. Let L be a quadratic extension of F. By duality, the number of index-3 subgroups of $\mathrm{Cl}(L/F)$ is equal to $(h_3(L/F) - 1)/3$. Class field theory implies that the set of index-3 subgroups of $\mathrm{Cl}(L/F)$ is in bijection with the set of unramified cubic extensions L_3 of L such that L_3/F is Galois with Galois group S_3. There exists an intermediate extension K between L_3 and F with $[K : F] = 3$, unique up to conjugacy. Furthermore, K is nowhere overramified over F, i.e., no prime ideal $\mathfrak{p}$ of F splits as $\mathcal{P}^3$. Conversely, given a nowhere overramified cubic S_3-extension K of F, let L_3 denote the Galois closure of K over F. Then L_3 contains a unique subfield L that is a quadratic extension of F, and L_3/L is unramified and thus corresponds to an index-3 subgroup of $\mathrm{Cl}(L/F)$. Furthermore, the relative discriminants of K and L over F are the same. Given a place $\mathfrak{p}$ of F, the splitting type of L/F at $\mathfrak{p}$ is determined by the splitting type of K/F at $\mathfrak{p}$. These splitting types are easily computed using a short and elegant note of Wood [51], and we list them in the following table.

Splitting type of K at $\mathfrak{p}$	Splitting type of L at $\mathfrak{p}$
(111)	(11)
(3)	(11)
(12)	(2)
$(1^2 1)$	(1^2)

Table 2: Relation between cubic and quadratic splitting types tabcubicsp

Table 2 gives a map ρ from the cubic splitting types of K to the quadratic splitting types of L. Let $\Sigma = (\Sigma_{\mathfrak{p}})_{\mathfrak{p}}$ be an archimedeally pure acceptable collection of local specifications for quadratic extensions of F. We define the collection $\Lambda = (\Lambda_{\mathfrak{p}})_{\mathfrak{p}}$ of local specifications for cubic equations by setting $\Lambda_{\mathfrak{p}} = \rho^{-1}(\Sigma_{\mathfrak{p}})$. The acceptability of Σ implies that Λ is also acceptable. Furthermore, the above discussion implies that we have

$$\frac{\displaystyle\sum_{L \in S_{2,\Sigma}(F,X)} (h_3(L/F) - 1)/2}{\#S_{2,\Sigma}(F,X)} = \frac{N_{3,\Lambda}(F,X)}{2N_{2,\Sigma}(F,X)},$$

where the factor of 2 in the denominator appears since $N_{2,\Sigma}(F,X)$ counts quadratic extensions of F weighted by a factor of 1/2. Using Theorem 2, which computes the asymptotics for $N_{n,\Sigma}(F,X)$, we therefore obtain

$$\frac{\displaystyle\sum_{L\in S_{2,\Sigma}(F,X)} h_3(L/F)}{\#S_{2,\Sigma}(F,X)} = 1+\frac{\displaystyle\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})}{\displaystyle\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})}, \tag{42}$$

eqpf3tor2pf

where the quantities $m_{\mathfrak{p}}$ are defined in the statement of Theorem 2 and the products are taken over all places $\mathfrak{p}$ of F. For every non-archimedean place $\mathfrak{p}$, it is easy to see from Table 2 that $m_{\mathfrak{p}}(\Lambda) = m_{\mathfrak{p}}(\Sigma)$. When $F_{\mathfrak{p}} = \mathbb{C}$, we have $K \otimes \mathbb{F}_p = \mathbb{C}^2$ and $L \otimes \mathbb{F}_{\mathfrak{p}} = \mathbb{C}^3$, and it follows that $m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = 1/3$. If $F_{\mathfrak{p}} = \mathbb{R}$, then $\Sigma_{\mathfrak{p}}$ has two choices: either $\Sigma_{\mathfrak{p}} = \{\mathbb{C}\}$ which implies that $\Lambda_{\mathfrak{p}} = \{\mathbb{R}\times\mathbb{C}\}$ and $m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}}) = m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})$ or $\Sigma_{\mathfrak{p}} = \{\mathbb{R}^2\}$ which implies that $\Lambda_{\mathfrak{p}} = \{\mathbb{R}^3\}$ and $m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = 1/3$. Part (a) of Theorem 6 now follows from (42).

We now prove Part (b) of Theorem 6 by computing the average size of the 2-torsion subgroups of the relatice class groups of cubic extensions of a global field F.

This time, we take L to be a cubic extension of F. The number of index-2 subgroups of $\mathrm{Cl}(L/F)$ is equal to $h_2(L/F)-1$. The set of index-2 subgroups of $\mathrm{Cl}(L/F)$ is in bijection with the set of unramified quadratic extensions L_2 of L such that L_2/F is Galois with Galois group S_4. Denote the Galois closure of L_4 by F_{24}. This yields a quartic extension K of F contained in F_{24}, unique up to conjugacy, which is *nowhere overramified* over F, i.e., no prime in F has splitting type (1^21^2), (2^2), or (1^4) in K. Furthermore, the relative discriminants of L/F and K/F are the same. Conversely, given a quartic nowhere overramified S_4 extension K of F, let F_{24} denote the Galois closure of K over F. Let L denote the cubic resolvent field contained in K_{24}, and let L_2 denote the unique quadratic extension of L whose Galois closure over F is F_{24}. Then L_2/L is unramified. The following table relates the splitting types of not overramified primes in K to their splitting types in L.

Splitting type of L at $\mathfrak{p}$	Splitting type of K at $\mathfrak{p}$
(1111)	(111)
(22)	(111)
(112)	(12)
(4)	(12)
(13)	(3)
(1^211)	(1^21)
(1^22)	(1^21)
(1^31)	(1^3)

Table 3: Relation between quartic and cubic splitting types tabquarticsp

Table 2 gives a map ρ from the quartic splitting types of K to the cubic splitting types of L. For an an archimedeally pure acceptable collection of local specifications $\Sigma = (\Sigma_{\mathfrak{p}})_{\mathfrak{p}}$ for cubic extensions of F, we define the acceptable collection Λ and Λ^+ of local specifications for quartic equations by setting $\Lambda_{\mathfrak{p}} = \Lambda^+_{\mathfrak{p}} = \rho^{-1}(\Sigma_{\mathfrak{p}})$ for nonarchimedean $\mathfrak{p}$ and for $F_{\mathfrak{p}} = \mathbb{C}$, and setting $\Lambda_{\mathfrak{p}} = \{\mathbb{R}^4\}$, $\Lambda^+_{\mathfrak{p}} = \{\mathbb{R}^4, \mathbb{C}^2\}$ when $\Sigma_{\mathfrak{p}} = \{\mathbb{R}^3\}$, and setting $\Lambda_{\mathfrak{p}} = \Lambda^+_{\mathfrak{p}} = \{\mathbb{R}^2\oplus\mathbb{C}\}$ when $\Sigma_{\mathfrak{p}} = \{\mathbb{R}\oplus\mathbb{C}\}$. As in Part (a), applying Theorem 2 yields the following:

$$\begin{aligned}\frac{\displaystyle\sum_{L\in S_{3,\Sigma}(F,X)} h_2(L/F)}{\#S_{3,\Sigma}(F,X)} &= 1+\frac{\displaystyle\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})}{\displaystyle\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})};\\ \frac{\displaystyle\sum_{L\in S_{3,\Sigma}(F,X)} h_2^+(L/F)}{\#S_{3,\Sigma}(F,X)} &= 1+\frac{\displaystyle\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Lambda^+_{\mathfrak{p}})}{\displaystyle\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})}.\end{aligned} \tag{43}$$

eqpf3tor2pf1

The ratios $m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})$ and $m_{\mathfrak{p}}(\Lambda^+_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}})$ can be easily computed using Table 3, and are seen to be 1 when $\mathfrak{p}$ is nonarchimedean. When $F_{\mathfrak{p}} = \mathbb{C}$ the ratios are both $1/4$, when $\Sigma_{\mathfrak{p}} = \{\mathbb{R}^3\}$ we have $m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = 1/4$, $m_{\mathfrak{p}}(\Lambda^+_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = 1$, and when $\Sigma_{\mathfrak{p}} = \{\mathbb{R}\oplus\mathbb{C}\}$ we have $m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = m_{\mathfrak{p}}(\Lambda_{\mathfrak{p}})/m_{\mathfrak{p}}(\Sigma_{\mathfrak{p}}) = 1/2$. Part (b) of Theorem 6 thus follows from (43).

10.2 Proof of Theorem 7

We first prove Part (a). Fix $n \leq 5$, and let M be an S_n-extension of F having degree-$n!$. We denote the subfield (unique up to conjugacy) of M having degree-n over F by L, and the subfield having degree-2 over F by K. We call K the *quadratic resolvent* of L. It is known that M is unramified over K at a place $\mathfrak{p}$ if and only if L is simply ramified over F at $\mathfrak{p}$, i.e., the ramified terms in the splitting type at $\mathfrak{p}$ of L/F contain at most a 1^2. In particular, if $F_{\mathfrak{p}} = \mathbb{R}$, then $L \otimes F_{\mathfrak{p}}$ can only be $\mathbb{R}^n$ or $\mathbb{R}^{n-2} \oplus \mathbb{C}$, depending on whether $K \otimes \mathbb{F}_{\mathfrak{p}}$ is $\mathbb{R}$ or $\mathbb{C}$, respectively. In general, the splitting type of L determines the splitting type of the quadratic resolvent of L. When $n = 3$, this relation is listed in Table 2. When $n = 4$, this relation can be determined from Tables 2 and 3 since the quadratic resolvent of a quartic extension L of F is the quadratic resolvent of the cubic resolvent of L. The relation between the splitting types of quintic extensions L of F and their quadratic resolvents K are listed in the following table.

Splitting type of L at $\mathfrak{p}$	Splitting type of K at $\mathfrak{p}$
(11111)	(11)
(1112)	(2)
(113)	(11)
(122)	(11)
(14)	(2)
(23)	(2)
(5)	(11)
(1^2111)	(1^2)
(1^212)	(1^2)
(1^23)	(1^2)

Table 4: Relation between quintic and quadratic splitting types tabquinticsp

Therefore, for $n = 3$, 4, and 5, we have maps ρ from degree-n splitting types to quadratic splitting types. Now, given an archimedeally pure acceptable collection of local specifications Σ for quadratic extensions of F, we define the acceptable collection of local specifications Λ for degree-n extensions of F by defining $\Lambda_{\mathfrak{p}}$ to be $\rho^{-1}(\Sigma_{\mathfrak{p}})$. From the above discussion, it follows that we have

$$E_\Sigma(A_n, S_n) = \lim_{X\to\infty} \frac{N_{n,\Lambda}(F,X)}{2N_{2,\Sigma}(F,X)},$$

where the factor of 2 in the denominator arises because quadratic extensions of F are counted with weight $1/2$ in $N_{2,\Sigma}(F,X)$. From Theorem 2 we thus obtain

$$E_\Sigma(A_n, S_n) = \frac{\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Lambda)}{2\prod_{\mathfrak{p}} m_{\mathfrak{p}}(\Sigma)}.$$

The ratio $m_{\mathfrak{p}}(\Lambda)/m_{\mathfrak{p}}(\Sigma)$ is easily seen to be one for nonarchimedean $\mathfrak{p}$ from Tables 2, 3, and 4. If $F_{\mathfrak{p}} = \mathbb{C}$, then $\Sigma_{\mathfrak{p}} = \mathbb{C}^2$, $\Lambda_{\mathfrak{p}} = \mathbb{C}^n$, and $m_{\mathfrak{p}}(\Lambda)/m_{\mathfrak{p}}(\Sigma) = 2/n!$. For $F_{\mathfrak{p}} = \mathbb{R}$, there are two possible choices for $\Sigma_{\mathfrak{p}}$: if $\Sigma_{\mathfrak{p}} = \{\mathbb{R}^2\}$, then $\Lambda_{\mathfrak{p}} = \mathbb{R}^n$ and $m_{\mathfrak{p}}(\Lambda)/m_{\mathfrak{p}}(\Sigma) = 2/n!$, while if $\Sigma_{\mathfrak{p}} = \{\mathbb{C}\}$, then $\Lambda_{\mathfrak{p}} = \mathbb{R}^{n-2} \oplus \mathbb{C}$ and $m_{\mathfrak{p}}(\Lambda)/m_{\mathfrak{p}}(\Sigma) = 1/(n-2)!$. Part (a) of Theorem 7 therefore follows.

To prove Part (b), we proceed as follows. Fix $n = 2$, 3, or 4. Let K be a quadratic extension of F. Let L be a degree-n extension of F such that the relative discriminant of L over F divides the relative discriminant of K over F. Then the composite field extension M of the Galois closure of L over F and K is an $(S_n, S_n \times C_2)$-extension of K unramified at all finite places. If we further assumed that for every place $\mathfrak{p}$ of F such that $F_\mathfrak{p} = \mathbb{R}$, we have $L \otimes F_\mathfrak{p} = \mathbb{R}^n$ or $\mathbb{R}^{n-2} \oplus \mathbb{C}$ depending on whether $K \otimes F_\mathfrak{p} = \mathbb{R}^2$ or $\mathbb{C}$, respectively, then M is an unramifie $(S_n, S_n \times C_2)$-extension of K. In particular, note that every degree-n extension L of F, satisfying these archimedean conditions, contributes to unramified $(S_n, S_n \times C_2)$-extensions of infinitely many quadratic extensions K of F, namely those whose relative discriminants are divisible by the relative discriminant of L over F.

We fix a large integer Y. There are $\gg Y$ degree-n simply ramified extensions of F, satisfying any prescribed archimedean conditions whose relative discriminants have norm bounded by Y. We denote their relative discriminants, written with multiplicity, by $d_1, d_2, \dots, d_{tY}$. For sufficiently large X, each such degree-n field with relative discriminant d_i contributes to the count of unramified $(S_n, S_n \times C_2)$-extensions for $\gg X/N(d_i)$ quadratic extensions of F whose relative discriminant has norm bounded by X, namely those quadratic fields whose discriminants are divisible by d_i. Therefore, the average number of unramified $(S_n, S_n \times C_2)$-extensions of quadratic extensions of F whose discriminants have norm bounded by X is

$$\gg \frac{1}{N(d_1)} + \frac{1}{N(d_1)} + \cdots \frac{1}{N(d_{tY})}.$$

Since this sum diverges as Y goes to infinity, Part (b) of Theorem 7 follows.

11 General axioms for counting S-integral orbits

In this section, we summarize the general strategy of this paper in the form of several axioms. Unless specified otherwise, everything following an axiom assumes the validity of that axiom.

Let F be a fixed global field and let S be a finite nonempty set of places containing all the archimedean places. Let (G, V) be a representation of a reductive group G over $\mathcal{O}_S$. Our goal is to obtain a result analogous to Theorem 22.

AXIOM - (G, V): The representation (G, V) satisfies the following conditions.

1. The global character group $\mathrm{Hom}(G, \mathbb{G}_m)$ of G has rank 1 with $\mathbb{Z}$-basis $\{\chi\}$.
2. Let $V(F)^{\mathrm{irr}}$ be a fixed $G(F)$-invariant subset of $V(F)$. Elements of $V(F)^{\mathrm{irr}}$ are called *irreducible* and elements not in $V(F)^{\mathrm{irr}}$ are called *reducible*. □

Definition 27. *A polynomial Δ in the coordinates of V is a relative invariant of G with χ-*relative degree *d if for every $g \in G$ and every $v \in V$,*

$$\Delta(gv) = \chi(g)^d \Delta(v).$$

If the character χ is clear from the context, we call d the relative degree. *In any case, it is well-defined up to sign.*

For all the field-counting representations used this paper, we have the character χ, defined in (12), and the discriminant Δ_n as the unique relative invariant with χ-relative degree 2. Another example of interest is the action of $\mathbb{G}_m$ on $\mathbb{G}_a^n$ given by

$$\lambda.(c_1, \dots, c_n) = (\lambda^{w_1} c_1, \dots, \lambda^{w_n} c_n)$$

for some fixed integers $w_1, \dots, w_n$. When $n = 2$ and $w_1 = 4$, $w_2 = 6$, we have the representation used in the sequel ([20]) to enumerate elliptic curves over a global field. The character χ can be chosen to be the identity map on $\mathbb{G}_m$. The relative invariants are $c_1, \dots, c_n$ with relative degrees $w_1, \dots, w_n$.

Our next axiom specifies which rational orbits we are interested in. For any positive integer M, we say a function $\phi : F^M \to [0, 1]$ is *defined by congruence conditions* if there exist local functions $\phi_\mathfrak{p} : F_\mathfrak{p}^M \to [0, 1]$ for every place $\mathfrak{p}$ of F (including archimedean places) such that:

1. For all $w \in F^M$, the product $\prod_{\mathfrak{p}} \phi_{\mathfrak{p}}(w)$ converges to $\phi(w)$.
2. For each $\mathfrak{p}$, the function $\phi_{\mathfrak{p}}$ is measurable.

A subset of F^M is said to be *defined by congruence conditions* if its characteristic function is defined by congruence conditions.

AXIOM - Local Condition: Let $m_0 = \prod_{\mathfrak{p}} m_{0,\mathfrak{p}}$ be a weight function on $V(F)$ defined by congruence conditions such that:

1. $m_{0,\mathfrak{p}}$ is $G(F_{\mathfrak{p}})$-invariant;
2. For any $v \in V(F)^{\mathrm{irr}}$ with $m_0(v) \neq 0$, $\mathrm{Stab}_G(v) = \{g \in G : gv = v\}$ is a finite group scheme with absolutely bounded order and for any S-prime $\mathfrak{p}$, there exists $g_{\mathfrak{p}} \in G(F_{\mathfrak{p}})$ such that $g_{\mathfrak{p}} v \in V(\mathcal{O}_{\mathfrak{p}})$.

We will be weighting each rational orbit $G(F).v$ by $m_0(v)/\#\,\mathrm{Stab}_{G(F)}(v)$. □

Note only rational orbits with nonzero weight m_0 will be counted. In the representations for counting field extensions, this axiom has the effect of fixing the collection Σ of local specifications.

We now work towards defining the height of a rational orbit.

AXIOM - Height: For every places $\mathfrak{p}$, let $h_{\mathfrak{p}} : V(F_{\mathfrak{p}}) \to \mathbb{R}_{\geq 0}$ be a function such that for every $g \in G(F_{\mathfrak{p}})$ and every $v \in V(F_{\mathfrak{p}})$,

$$h_{\mathfrak{p}}(gv) = |\chi(g)|_{\mathfrak{p}}^{\deg(h)} h_{\mathfrak{p}}(v)$$

for some fixed rational number $\deg(h)$ independent on $\mathfrak{p}$. Moreover, for any $v \in V(F)$ with $m_0(v) \neq 0$, the product

$$h(v) = \prod_{\mathfrak{p}} h_{\mathfrak{p}}(v)$$

is finite. □

Note the product $h = \prod_{\mathfrak{p}} h_{\mathfrak{p}}$ is $G(F)$-invariant by the product formula. One common choice of $h_{\mathfrak{p}}$ is to take any relative invariant Δ and set $h_{\mathfrak{p}}(v) = |\Delta(v)|_{\mathfrak{p}}$ for all $v \in V(F_{\mathfrak{p}})$. Then $\deg h$ is the relative degree of Δ. When there are multiple relative invariants $\Delta_1, \ldots, \Delta_k$ of relative degrees $d_1, \ldots, d_k$, one may define

$$h_{\mathfrak{p}}(v) = \max\{|\Delta_1(v)|_{\mathfrak{p}}^{1/d_1}, \ldots, |\Delta_k(v)|_{\mathfrak{p}}^{1/d_k}\}.$$

Then $h_{\mathfrak{p}}(gv) = |\chi(g)|_{\mathfrak{p}} h_{\mathfrak{p}}(v)$ for every $g \in G(F_{\mathfrak{p}})$ and has $\deg h = 1$.

defn:Sheight **Definition 28.** *Suppose $v \in V(F)$ with $m_0(v) \neq 0$. For every S-prime $\mathfrak{p}$ ($\mathfrak{p} \notin S$), we say an element $u \in V(\mathcal{O}_{\mathfrak{p}})$ is* $\mathfrak{p}$-maximal *if $h_{\mathfrak{p}}(u)$ is minimal among $G(F_{\mathfrak{p}}).u \cap V(\mathcal{O}_{\mathfrak{p}})$. For every prime $\mathfrak{p} \notin S$, pick $g_{\mathfrak{p}} \in G(F_{\mathfrak{p}})$ such that $g_{\mathfrak{p}} v \in V(\mathcal{O}_{\mathfrak{p}})$ is $\mathfrak{p}$-maximal. We define the* S-height *of v to be*

$$h_S(v) = h(v) \prod_{\mathfrak{p} \notin S} h_{\mathfrak{p}}(g_{\mathfrak{p}} v)^{-1} = \prod_{\mathfrak{p} \notin S} |\chi(g_{\mathfrak{p}})|_{\mathfrak{p}}^{-\deg h} \prod_{\mathfrak{p} \in S} h_{\mathfrak{p}}(v). \qquad (44)$$ eq:Sheight

The $G(F)$-invariance of h gives the $G(F)$-invariance of h_S. We have then defined a function on the set of rational orbits.

In the case of the action of $\mathbb{G}_m$ on $\mathbb{G}_a^n$, this recovers the following definition on weighted projective spaces. (See also [32] where a Schanuel type count on the number of elements with bounded height was obtained.) Given any $(c_1, \ldots, c_n) \in F^n$, let I denote the $\mathcal{O}_S$-ideal

$$I = \{\lambda \in F : \lambda.(c_1, \ldots, c_n) \in \mathcal{O}_S^n\},$$

then,

$$h_S(c_1,\ldots,c_n) = (NI)\prod_{\mathfrak{p}\in S}\max(|c_1|_{\mathfrak{p}}^{1/w_1},\ldots,|c_n|_{\mathfrak{p}}^{1/w_n}). \tag{45}$$ eq:heightweighted

From the double coset decomposition (13), there exist $g'_{\mathfrak{p}} \in G(\mathcal{O}_{\mathfrak{p}})$ for every S-primes $\mathfrak{p}$, a unique $\beta \in \mathrm{cl}(G)$, and $h \in G(F)$ such that the adele $(g_{\mathfrak{p}}) \in G(\mathbb{A}_S)$ equals $(g'_{\mathfrak{p}})\beta h$. Then $v' = hv$ lies in

$$\mathcal{L}_\beta := V(F) \cap \beta^{-1}\prod_{\mathfrak{p}\notin S} V(\mathcal{O}_{\mathfrak{p}})\prod_{\mathfrak{p}\in S} V(F_{\mathfrak{p}}).$$

An element $v_0 \in \mathcal{L}_\beta$ is said to be S-maximal if for every $\mathfrak{p} \notin S$, βv_0 is $\mathfrak{p}$-maximal. Let $\mathcal{L}_\beta^{\max}$ denote the subset of $\mathcal{L}_\beta$ consisting of S-maximal elements. Then $v' \in \mathcal{L}_\beta^{\max}$. Computing heights, we have

$$h_S(v) = |\chi(\beta)|^{-\deg h}\prod_{\mathfrak{p}\in S} h_{\mathfrak{p}}(v'). \tag{46}$$ eq:Sh2

In the case of the representations used for counting field extensions, having minimal $h_{\mathfrak{p}}$ means that the ring corresponding to the integral orbit is maximal. Hence the notion of S-maximal defined here coincides with its definition in Section 3. Moreover, (46) recovers (30) for the S-norm of the discriminant. Proposition 10 states that if v_1 and v_2 are $G(F_{\mathfrak{p}})$-equivalent and have minimal $h_{\mathfrak{p}}$, then they are $G(\mathcal{O}_{\mathfrak{p}})$-equivalent and so for a given $v \in V(F)$, there is a unique β for which $G(F).v \cap \mathcal{L}_\beta \neq \emptyset$. In general, this might not hold. We deal with this using a second weight function.

For any subgroup G_0 of $G(F)$, any G_0-invariant subset V_0 of $V(F)$, and any G_0-invariant function $m : V_0 \to [0,1]$, let $N_m(V_0, G_0, X)$ denote the number irreducible G_0-orbits in V_0 of S-height bounded by X when F is a number field or equal to X when F is a function field, where each orbit $G_0 v$ is weighted by $m(v)/(\#\operatorname{Stab}_{G_0}(v))$. If m is identically 1 on V_0, we write $N(V_0, G_0, X)$ instead. We are interested in $N_{m_0}(V(F), G(F), X)$.

Recall the group

$$\Gamma_\beta := G(F) \cap \beta^{-1}\big(\prod_{\mathfrak{p}\notin S} G(\mathcal{O}_{\mathfrak{p}})\prod_{\mathfrak{p}\in S} G(F_{\mathfrak{p}})\big)\beta. \tag{47}$$ eq:gamma

Then Γ_β preserves $\mathcal{L}_\beta^{\max}$ and we have the following formula:

$$N_{m_0}(V(F), G(F), X) = \sum_\beta N_m(\mathcal{L}_\beta^{\max}, \Gamma_\beta, X), \tag{48}$$ eq:breakupclG

where the weight function m is defined by

$$m(v) = \frac{m_0(v)}{\#\operatorname{Stab}_{G(F)}(v)}\left(\sum_\beta\sum_{v_{\beta,i}}\frac{1}{\#\operatorname{Stab}_{\Gamma_\beta}(v_{\beta,i})}\right)^{-1}; \tag{49}$$ eq:defnofm

here $\{v_{\beta,i}\}$ denotes a complete set of representatives for the action of Γ_β on $G(F).v \cap \mathcal{L}_\beta^{\max}$. The weight function m is defined by congruence conditions by [43, Theorem 4.3.1].

We now turn to the estimation of $N_m(\mathcal{L}_\beta^{\max}, \Gamma_\beta, X)$ for some fixed $\beta \in \mathrm{cl}(G)$. Or more generally to the estimation of $N_m(V_0, G_0, X)$ where G_0 is a subgroup of $G(F)$ commeasurable with $G(\mathcal{O}_S)$, and V_0 is a G_0-invariant lattice in $V(F)$ commeasurable with $V(\mathcal{O}_S)$. Let $m_S = \prod_{\mathfrak{p}\in S} m_{\mathfrak{p}}$ be the product of all the weights at infinity. Given any $v \in V(F_S) = \prod_{\mathfrak{p}\in S} V(F_{\mathfrak{p}})$, we define $h'_S(v) = \prod_{\mathfrak{p}\in S} h_{\mathfrak{p}}(v)$. Note if $v \in \mathcal{L}_\beta^{\max}$, then

$$h_S(v) = |\chi(\beta)|^{-\deg h} h'_S(v).$$

Let $G(F_S)^1$ denote, as in Section 4.1, the subgroup of $G(F_S)$ consisting of elements g such that

$$|\chi(g)| = \prod_{\mathfrak{p}\in S}|\chi(g)|_{\mathfrak{p}} = 1.$$

Then h'_S is $G(F_S)^1$-invariant. Both $G(\mathcal{O}_S)$ and Γ_β are subgroups of $G(F_S)^1$. Being commensurable with $G(\mathcal{O}_S)$, G_0 is also a subgroup of $G(F_S)^1$. We view V_0 as a lattice in $V(F_S)$ and consider $N'_{m_S}(V_0, G_0, X)$, the number of irreducible G_0-orbit in V_0 having h'_S-height bounded by X when F is a number field and equals X when F is a function field, where each orbit is weighted by $m_S(v)/\#\operatorname{Stab}_{G_0}(v)$. Once a general estimate for $N'_{m_S}(V_0, G_0, X)$ is obtained, we introduce the weights at the S-primes and impose maximality conditions to sieve to $N_m(\mathcal{L}_\beta^{\max}, \Gamma_\beta, X)$.

Let $V(F_S)_X^{m_S}$ denote the subset of $V(F_S)$ consisting elements with nonzero weight m_S and whose h'_S-height is bounded by X when F is a number field and equal to X when F is a function field. Let $R(X)$ denote a fundamental domain for the action of $G(F_S)^1$ on $V(F_S)_X^{m_S}$. Let $\mathcal{F}_0$ be a fundamental domain for the left action of G_0 on $G(F_S)^1$. View $\mathcal{F}_0.R(X) \subset V(F_S)_X^{m_S}$ as a multiset where the multiplicity of $v \in \mathcal{F}_0.R(X)$ is the cardinality of the set $\{g \in \mathcal{F}_0 \mid v \in gR(X)\}$. Then $\mathcal{F}_0.R(X)$ maps surjectively onto a fundamental domain for the action of G_0 on $V(F_S)_X^{m_S}$ where the fiber above any orbit $G_0.v$ has size $\#\operatorname{Stab}_{G(F_S)^1}(v)/\#\operatorname{Stab}_{G_0}(v) = \#\operatorname{Stab}_{G(F_S)}(v)/\#\operatorname{Stab}_{G_0}(v)$.

Let $d\nu$ denote a left-invariant top differential on V defined over $\mathbb{Z}$ and denote by $\nu_S, \nu_\mathfrak{p}$ the induced measures on $V(F_S)$ and $V(F_\mathfrak{p})$ for any place $\mathfrak{p}$. The next axiom states that the number of G_0-orbits should asymptotically equal to the volume of the fundamental domain normalized so that the covolume of V_0 is 1. For the representations studied earlier in this paper, this axiom is the content of Theorem 19.

AXIOM - Counting: There exists a sequence of fundamental domains $R(X)$ for the action of $G(F_S)^1$ on $V(F_S)_X^{m_S}$ (independent of G_0 and V_0) such that as X goes to infinity

$$N'_{m_S}(V_0, G_0, X) \sim \sqrt{D_F}^{\,-\dim V} \Big(\prod_{\mathfrak{p}\notin S} \int_{V_{0,\mathfrak{p}}} d\nu_\mathfrak{p}\Big) \int_{v\in\mathcal{F}_0.R(X)} \frac{m_S(v)}{\#\operatorname{Stab}_{G(F_S)}(v)} d\nu_S(v), \tag{50}$$

eq:mainequal

where $V_{0,\mathfrak{p}}$ denotes the completion of V_0 in $V(F_\mathfrak{p})$. □

In practice, the region $R(X)$ will be homogeneously expanding in X, in which case AXIOM - Counting holds automatically if $\mathcal{F}_0$ is bounded. One example of this is the representation for counting quadratic extensions over a field of characteristic 2 in Section 9, even though the group used was not reductive. In general, the unboundedness of $\mathcal{F}_0$ requires averaging over a continuum of fundamental domains, breaking it up into a compact part and a cuspidal part, and showing that the cuspidal part does not contribute to irreducible orbits nor to volumes. In the sequel ([20, Section 3.2]), we work out sufficient conditions for AXIOM - Counting that are combinatorial in the characters of the maximal split torus of G.

We can now include weight functions at finitely many finite primes by breaking V_0 up into a finite disjoint union of sublattices on which the weight functions are constant and applying (50) to each sublattice. Adding in more and more finite primes gives the following upper bound, up to lower order error terms,

$$N_m(V_0, G_0, X) \le \sqrt{D_F}^{\,-\dim V} \Big(\prod_{\mathfrak{p}\notin S} \int_{V_{0,\mathfrak{p}}} m_\mathfrak{p}\, d\nu_\mathfrak{p}\Big) \int_{v\in\mathcal{F}_0.R(X)} \frac{m_S(v)}{\#\operatorname{Stab}_{G(F_S)}(v)} d\nu_S(v) \tag{51}$$

eq: countingmaininfuppp

Finally we restrict to Γ_β acting on $\mathcal{L}_\beta$ and impose the S-maximality conditions. For every $\mathfrak{p} \notin S$, let $V(\mathcal{O}_\mathfrak{p})^{\max}$ denote the subset of $\mathfrak{p}$-maximal elements in $V(\mathcal{O}_\mathfrak{p})$. Let $\mathcal{F}_\beta$ denote a fundamental domain for the left action of Γ_β on $G(F_S)^1$. Define

$$\nu_m^{\max}(\mathcal{F}_\beta.R(X)) = \sqrt{D_F}^{\,-\dim V} \Big(\prod_{\mathfrak{p}\notin S} \int_{\beta^{-1}V(\mathcal{O}_\mathfrak{p})^{\max}} m_\mathfrak{p}\, d\nu_\mathfrak{p}\Big) \int_{v\in\mathcal{F}_\beta.R(X)} \frac{m_S(v)}{\#\operatorname{Stab}_{G(F_S)}(v)} d\nu_S(v). \tag{52}$$

eq:mu

Then we have, up to lower order error terms,

$$N_m(\mathcal{L}_\beta, \Gamma_\beta, X) \le \nu_m^{\max}(\mathcal{F}_\beta.R(|\chi(\beta)|^{\deg h} X)).$$

In order to obtain a lower bound, we need the following uniformity estimate.

AXIOM - Uniformity Estimate: For any $\beta \in \mathrm{cl}(G)$ and any $\mathfrak{p} \notin S$, let $W_{\beta,\mathfrak{p}}$ denote the set of elements v of $\mathcal{L}_\beta$ such that $m_{\mathfrak{p}}(v) \neq 1$ or βv is not $\mathfrak{p}$-maximal. Then

$$\lim_{M\to\infty} \limsup_{X\to\infty} \frac{N(\bigcup_{N\mathfrak{p}>M} W_{\beta,\mathfrak{p}}, \Gamma_\beta, X)}{\nu_m^{\max}(\mathcal{F}_\beta . R(|\chi(\beta)|^{\deg h} X))} = 0. \tag{53}$$

eq:uniform

In other words, the overestimate in the upper bound approaches 0 as we impose more and more congruence conditions. □

We refer to the sequel ([20, Section 3.3]) for a list of methods one can use to check AXIOM - Uniformity Estimate.

We can now state our main theorem.

thm: countingmainS

Theorem 29. *Let F be a global field with absolute discriminant D_F and let S be a finite nonempty set of places of F containing all the archimedean places. Let (G,V) be a representation over the $\mathcal{O}_S$ and let χ generate the global character group. Let $V(F)^{\mathrm{irr}}$ be a $G(F)$-invariant subset of $V(F)$. Let $m_0 = m_{0,S} \prod_{\mathfrak{p}\notin S} m_{0,\mathfrak{p}}$ be a weight function on $V(F)$ defined by congruence conditions. Let $G(F_S)^1$ denote the subgroup of $G(F_S)$ consisting of elements with $|\chi(g)| = 1$. Let $R(X)$ be a sequence of fundamental domains for the action of $G(F_S)^1$ on $V(F_S)$ and for every $\beta \in \mathrm{cl}(G)$, let $\mathcal{F}_\beta$ be a fundamental domain for the action of Γ_β, defined in (47), on $G(F_S)^1$. Suppose the following axioms hold.*

1. *AXIOM - (G,V),*
2. *AXIOM - Local Condition,*
3. *AXIOM - Height,*
4. *AXIOM - Counting.*

Define the S-height h_S of a rational orbit as in (44) and let $\deg h$ denote the rational number in AXIOM - Height. For every $\mathfrak{p} \notin S$, let $V(\mathcal{O}_{\mathfrak{p}})^{\max}$ denote the set of elements $v \in V(\mathcal{O}_{\mathfrak{p}})$ such that $h_{\mathfrak{p}}(v)$ is minimal among $G(F_{\mathfrak{p}}).v \cap V(\mathcal{O}_{\mathfrak{p}})$. Then the number of $G(F)$-orbits in $V(F)^{\mathrm{irr}}$ with S-height at most X if F is a number field, equal to X if F is a function field, where each orbit $G(F).v$ is weighted by $m_0(v)/\#\operatorname{Stab}_{G(F)}(v)$ is, up to lower order error terms, bounded above by

$$\sum_{\beta\in\mathrm{cl}(G)} \sqrt{D_F}^{\,-\dim V} \Big(\prod_{\mathfrak{p}\notin S} \int_{\beta^{-1}V(\mathcal{O}_{\mathfrak{p}})^{\max}} m_{0,\mathfrak{p}}\, d\nu_{\mathfrak{p}} \Big) \int_{v\in\mathcal{F}_\beta . R(|\chi(\beta)|^{\deg h} X)} \frac{m_{0,S}(v)}{\#\operatorname{Stab}_{G(F_S)}(v)} d\nu_S(v). \tag{54}$$

eq:average

If moreover AXIOM - Uniformity Estimate also holds, then this upper bound is also the lower bound.

In practice, the fundamental domains $R(X)$ are usually constructed so that the extra factor of $|\chi(\beta)|^{\deg h}$ in the region of integration over $V(F_S)$ cancels out with the extra factor of β^{-1} in the region of integration over $\prod_{\mathfrak{p}\notin S} V(F_{\mathfrak{p}})$. Note also the integrand in the integral over $V(F_S)$ is $\mathcal{F}_\beta$-invariant. Hence when doing the volume computations, the G-volumes of the $\mathcal{F}_\beta$'s usually factor out and their summation over all $\beta \in \mathrm{cl}(G)$ gives the Tamagawa number of G. We now illustrate this principle under the further assumption that the representation is prehomogeneous.

AXIOM - Prehomogeneous: For any $\mathfrak{p} \in S$, the subset $\{v \in V(F_{\mathfrak{p}}) \mid m_{0,\mathfrak{p}}(v) \neq 0\}$ breaks up into finitely many $G(F_{\mathfrak{p}})$-orbits, with representatives $v_{\mathfrak{p},1}, \dots, v_{\mathfrak{p},n_{\mathfrak{p}}}$ for some positive integer $n_{\mathfrak{p}}$. Moreover, $\dim G = \dim V$.

A $G(F_S)$-orbit in $V(F_S)$ is called an *S-specification.* AXIOM - Prehomogeneous gives the finiteness of S-specifications and we evaluate the integral over $V(F_S)$ in (54) by breaking it up into a sum over S-specifications. Let σ be an S-specification and let $V(F_S)^{(\sigma)}$ denote the set of elements $(v_\mathfrak{p})_{\mathfrak{p}\in S}$ such that $v_\mathfrak{p}$ is in the $G(F_\mathfrak{p})$-orbit corresponding to σ. Let v_σ be some fixed element in $V(F_S)^{(\sigma)}$. Then $\mathrm{Stab}_{G(F_S)}(v)$ for any $v \in V(F_S)^{(\sigma)}$ is isomorphic to $\mathrm{Stab}_{G(F_S)}(v_\sigma)$ which we rename to $\mathrm{Aut}(\sigma)$.

AXIOM - Counting gives a sequence $R(X)$ of fundamental domains so that (50) holds. To compute the volumes, we may take any choice for $\mathcal{F}_\beta.R(X)$. When F is a number field, there is an embedding $\iota : \mathbb{R}^+ \to G(F_S)$ such that $\chi(\iota(\lambda)) = \lambda$ for all $\lambda \in \mathbb{R}^+$. Let Λ_X denote the image of the interval $(0, (X/h'_S(v_\sigma))^{1/\deg(h)}]$ under ι. When F is a function field, we take Λ_X to be any element in $G(F_S)$ such that $|\chi(\Lambda_X)|^{\deg h} = X/h'_S(v_\sigma)$. Then we take $R(X) = \Lambda_X.v_\sigma$ for the purpose of the volume computation.

We use a Jacobian change of variable formula to transfer the volume computations in V to computations in G. For any $g \in G$, let $\varphi_g : V \to V$ denote the action map sending any $v \in V$ to gv. Then there exists an integer $\deg J$ such that

$$\varphi_g^* d\nu = \chi(g)^{\deg J} d\nu. \tag{55}$$ eq:degJ

For any $v \in V$, let $\pi_v : G \to V$ be the orbit map sending g to gv. Let $d\omega$ denote a top degree left-invariant differential form on G over $\mathcal{O}_S$. Then as in (33), there exists a polynomial J in the coordinate of V of χ-relative degree $\deg J$ such that

$$\pi_v^* d\nu = J(v)\chi(g)^{\deg J} d\omega(g). \tag{56}$$ eq:Jgen

For the representations studied earlier in this paper, $J(v)$ is an integer times the discriminant of v.

We may then proceed as in Section 7 to obtain the following analogues of (38) and (39).

$$\int_{\mathcal{F}_\beta.R(|\chi(\beta)|^{\deg h}X)} \frac{m_{0,S}(v)}{\#\,\mathrm{Stab}_{G(F_S)}(v)} d\nu_S(v) = \begin{cases} \dfrac{|J(v_\sigma)| m_{0,S}(v_\sigma)}{\#\mathrm{Aut}(\sigma)} \displaystyle\int_{\mathcal{F}_\beta \Lambda_{|\chi(\beta)|^{\deg h}X}} |\chi(g)|^{\deg J} d\omega_S(g) & \text{if } F \text{ is a number field,} \\ \left(\dfrac{|\chi(\beta)|^{\deg h}X}{h'_S(v_\sigma)}\right)^{\frac{\deg J}{\deg h}} \dfrac{|J(v_\sigma)| m_{0,S}(v_\sigma)}{\#\mathrm{Aut}(\sigma)} \displaystyle\int_{\mathcal{F}_\beta} d\omega_S(g) & \text{if } F \text{ is a function field.} \end{cases}$$

$$\int_{\beta^{-1}V(\mathcal{O}_\mathfrak{p})^{\max}} m_{0,\mathfrak{p}}\, d\nu_\mathfrak{p} = |\chi(\beta)|_\mathfrak{p}^{-\deg J} \Bigg(\sum_{v_\mathfrak{p} \in G(\mathcal{O}_\mathfrak{p})\backslash V(\mathcal{O}_\mathfrak{p})^{\max}} \frac{|J(v_\mathfrak{p})|_\mathfrak{p} m_{0,\mathfrak{p}}(v_\mathfrak{p})}{\#\,\mathrm{Stab}_{G(\mathcal{O}_\mathfrak{p})}(v_\mathfrak{p})} \Bigg) \int_{G(\mathcal{O}_\mathfrak{p})} d\omega_\mathfrak{p}$$

We define the various local masses by

$$M_{\mathfrak{p},S}(m_0) = \begin{cases} \dfrac{N\mathfrak{p}-1}{N\mathfrak{p}} \displaystyle\sum_{v_\mathfrak{p} \in G(\mathcal{O}_\mathfrak{p})\backslash V(\mathcal{O}_\mathfrak{p})^{\max}} \frac{|J(v_\mathfrak{p})|_\mathfrak{p} m_{0,\mathfrak{p}}(v_\mathfrak{p})}{\#\,\mathrm{Stab}_{G(\mathcal{O}_\mathfrak{p})}(v_\mathfrak{p})} & \text{if } \mathfrak{p} \notin S, \\ \displaystyle\sum_{v_\mathfrak{p} \in G(F_\mathfrak{p})\backslash V(F_\mathfrak{p})} \frac{|J(v_\mathfrak{p})|_\mathfrak{p} m_{0,\mathfrak{p}}(v_\mathfrak{p})}{h_\mathfrak{p}(v_\mathfrak{p})^{\deg J/\deg h} \#\,\mathrm{Stab}_{G(F_\mathfrak{p})}(v_\mathfrak{p})} & \text{if } \mathfrak{p} \in S. \end{cases} \tag{57}$$ eq:localmass

Then we have the following analogue of (6):

$$(54) = c\,\tau\ \mathrm{Res}_{s=1}\,\zeta_S(s) X^{\deg J/\deg h} \prod_\mathfrak{p} M_{\mathfrak{p},S}(m_0), \tag{58}$$

where τ denotes the Tamagawa number of G and

$$c = \begin{cases} 1/\deg J & \text{if } F \text{ is a number field,} \\ \log q & \text{if } F \text{ is a function field over } \mathbb{F}_q. \end{cases}$$

In practice, we usually have $\deg J = \deg h$ and $h_\mathfrak{p}(v_\mathfrak{p}) = |\epsilon|_\mathfrak{p} |J(v_\mathfrak{p})|_\mathfrak{p}$ for some $\epsilon \in \mathcal{O}_S^\times$, for all $\mathfrak{p}$. Then formula (57) simplifies to an analogue of (7) and the number of rational orbits grows asymptotically linear in S-height. We expect there to be interesting representations where $\deg h \neq \deg J$ for which the general formula (57) will be used.

Appendix A: Lattice-point counting over function fields

In this appendix, we prove Proposition 15 in the function field case estimating the number of lattice points in an open compact region over function fields. We believe the results here may also be of independent use elsewhere in applications involving geometry-of-numbers over function fields.

Fix a smooth projective and geometrically connected algebraic curve $\mathcal{C}$ over $\mathbb{F}_q$ and let F be its field of rational functions. The goal of this appendix is to prove Proposition 15 relating the number of lattice points inside a nice region to the volume of the region in the case of function fields. The main technique we use is the theory of Fourier analysis and Poisson summation over function fields which we recall from [47].

For any place v of F, choose a uniformizer π_v and denote by $q_v = q^{\deg v}$ the size of the residue field $k(v) = \mathcal{O}_v/\pi_v\mathcal{O}_v$. Let k_v denote the canonical exponent of v and let χ_v be the (continuous) additive character $F_v \to \mathbb{C}^\times$ defined in [47, §2.1.2]. The divisor class of $\sum_v k_v[v]$ is the canonical class of $\mathcal{C}$. It will not be important to us what the precise definitions of k_v and χ_v are. Note that since F_v is a locally compact group, the image of χ_v lands inside the unit circle. Let $d_v x$ denote the Haar measure on F_v normalized so that the measure of $\mathcal{O}_v$ is $q_v^{-k_v/2}$.

Let S be a nonempty finite set of places of F. Write F_S for the product $\prod_{v\in S} F_v$; χ_S for the character $\prod_{v\in S}\chi_v$ on F_S; and $d_S x$ for the measure $\prod_{v\in S} d_v x_v$ on F_S. The Fourier transform of an integrable continuous function f with respect to S is defined to be

$$\mathcal{F}_S f(y) = \int_{F_S} f(x)\chi_S(xy)d_S x \quad \forall y \in F_S. \tag{59}$$ eq:defFourier

In stark contrast to the archimedean case, the following lemma implies that the Fourier transform takes a continuous function with compact support to a continuous function with compact support.

lem:FourCC **Lemma 30.** ([47, §2.1.3]) *For any subset B of F_S, denote by χ_B its characteristic function. Let n_v be fixed integers for $v \in S$. Then*

$$\mathcal{F}_S \chi_{\prod_{v\in S}\pi_v^{n_v}\mathcal{O}_v} = \left(\prod_{v\in S} q_v^{-k_v/2}\right)\chi_{\prod_{v\in S}\pi_v^{-n_v-k_v}\mathcal{O}_v}. \tag{60}$$ eq:FourCC

For any continuous function f on F_S with compact support, define its *conductor* $c(f)$ to be the biggest open neighborhood of 0 in F_S such that $f(x+y) = f(x)$ for any $x \in F_S$ and $y \in c(f)$. Then Lemma 30 implies that

$$c(f) = \prod_{v\in S}\pi_v^{c_v}\mathcal{O}_v \Rightarrow \mathrm{Supp}(\mathcal{F}_S f) \subset \prod_{v\in S}\pi_v^{-c_v-k_v}\mathcal{O}_v. \tag{61}$$ eq:support

Theorem 31. (Poisson Summation [47, Lemma 3.5.9] *Define*

$$\begin{aligned} \mathcal{O}_S &= \{x \in F : v(x) \geq 0, \forall v \notin S\}, \\ \mathcal{O}_S^\perp &= \{y \in F : v(y) \geq -k_v, \forall v \notin S\}, \end{aligned}$$

where $v(x), v(y)$ denote the valuations of x, y with respect to v respectively. Then for any continuous function f on F_S with continuous Fourier transform, we have

$$\sum_{x\in\mathcal{O}_S} f(x) = \prod_{v\notin S} q_v^{-k_v/2}\sum_{y\in\mathcal{O}_S^\perp}\mathcal{F}_S f(y). \tag{62}$$ eq:poisson

For any place v, the v-adic norm $|\alpha|_v$ of some $\alpha \in F_v$ is defined to be $|\alpha|_v = q_v^{-v(\alpha)}$. (This is the same definition as given in Section 2.1.) For any $t = (t_v) \in F_S$, its S-norm is defined to be

$$|t|_S = \prod_{v\in S}|t|_v = q^{-\sum_{v\in S} v(t)\deg v},$$

where we have abbreviated $v(t_v)$ and $|t_v|_v$ to $v(t)$ and $|t|_v$ respectively. We are interested in the number of lattice points in a homogeneously expanding region in F_S.

prop:homoexp **Proposition 32.** *Let B be an open compact subset of F_S. Let c be a positive real constant. Then for any $t = (t_v) \in F_S$ such that $|t|_v/|t|_{v'} < c$ for every $v, v' \in S$,*

$$\#\{tB \cap \mathcal{O}_S\} = \prod_{v \notin S} q_v^{-k_v/2} \mathrm{Vol}(tB) + O(1) = \mathrm{Vol}_{\mathcal{O}_S}(tB) + O(1) \tag{63}$$ eq:homoexp

where Vol *denotes the volume computed with respect to d_S, and $\mathrm{Vol}_{\mathcal{O}_S}$ is a constant multiple of* Vol *such that $F_S/\mathcal{O}_S$ has volume 1. The implied constant in the second summand depends only on F, B and c. The dependency on B is through a bound M on the S-norm of elements of B and the conductor $c(\chi_B)$ of the characteristic function of B.*

Proof. Since B is bounded, there exists a constant M such that for any $b \in B$, $|b|_S < M$. Suppose first that $|t|_S \le 1/M$. Then for any $b \in B$, $|tb|_S < 1$ and so

$$\sum_{v \in S} v(tb) \deg(v) > 0.$$

On the other hand, if $b' \in \mathcal{O}_S$, then $v(b') \ge 0$ for every $v \notin S$ and $\sum_v v(b') \deg(v) = 0$. Hence we see that $tB \cap \mathcal{O}_S = \emptyset$ while tB is contained in the bounded open ball defined by $|b'|_S < 1$. In this case, both sides of (63) are bounded by an absolute constant.

Suppose from now on that $|t|_S > 1/M$. Then the sum $\sum_{v \in S} -v(t) \deg(v)$ is bounded below by $-\log_q M$. By assumption on the proximity of $|t|_v$ for different v, we see that each individual $-v(t)$, for $v \in S$, is bounded below by some constant C_1 depending only on M and c. Write the conductor of χ_B as $\prod_{v \in S} \pi_v^{c_v} \mathcal{O}_v$ and so $c(\chi_{tB}) = \prod_{v \in S} \pi_v^{c_v + v(t)} \mathcal{O}_v$. Hence by (61),

$$\mathrm{Supp}(\mathcal{F}_S \chi_{tB}) \subset \prod_{v \in S} \pi_v^{-c_v - v(t) - k_v} \mathcal{O}_v.$$

If $y \in \mathrm{Supp}(\mathcal{F}_S \chi_{tB}) \cap \mathcal{O}_S^\perp$ is nonzero, then we must have

$$\begin{aligned} v(y) &\ge -k_v, \quad \forall v \notin S, \\ v(y) &\ge -c_v - v(t) - k_v, \quad \forall v \in S. \end{aligned}$$

Adding these up over all v gives

$$0 = \sum_v v(y) \deg v \ge -\sum_v k_v \deg v - \sum_{v \in S} c_v \deg v - \sum_{v \in S} v(t) \deg v.$$

Hence the sum $\sum_{v \in S} -v(t) \deg(v)$ is also bounded above by some constant C_2 depending only on F and $c(\chi_B)$. We write $S(t)$ for the $|S|$-tuple $(v(t)) \in \mathbb{Z}^{|S|}$.

Suppose now that $\sum_{v \in S} -v(t) \deg(v) \le C_2$. Then $S(t)$ belongs to some finite subset of $\mathbb{Z}^{|S|}$ depending only on F, M, $c(\chi_B)$ and c. If $y \in \mathrm{Supp}(\mathcal{F}_S \chi_{tB}) \cap \mathcal{O}_S^\perp$ is nonzero, then y is a global section of some line bundle on $\mathcal{C}$ that depends only on $S(t)$. Hence $\mathrm{Supp}(\mathcal{F}_S \chi_{tB}) \cap \mathcal{O}_S^\perp$ is contained in a finite subset U of $\mathcal{O}_S^\perp$ depending only on F, M, $c(\chi_B)$ and c. Write B as a finite disjoint union of translates $B = \cup_b b + c(B)$ of its conductor. Note the number of translates needed to cover B is bounded above in terms of M and $c(\chi_B)$ by taking the volume of B. Then tB is a finite union of translates $tb + c(tB)$. Hence the volume of tB is bounded by a constant depending only on F, M, $c(\chi_B)$ and c. By the translation property of the Fourier transform and Lemma 30, we see that $|\mathcal{F}_S \chi_{tb + c(tB)}(y)|$ for any $y \in \mathcal{O}_S^\perp$ depends only on $c(\chi_B)$, $S(t)$ and y. Finally we apply Poisson summation (62) to the continuous function χ_{tB}. The sum in the right hand side of (62) is bounded above by a finite sum

$$\sum_b \sum_{y \in U} |\mathcal{F}_S \chi_{tb + c(tB)}(y)|$$

which depends only on F, M, $c(\chi_B)$ and c.

Finally suppose that $\sum_{v\in S} -v(t)\deg(v) > C_2$. Then $\mathrm{Supp}(\mathcal{F}_S\chi_{tB}) \cap \mathcal{O}_S^{\perp}$ contains no nonzero element. Therefore,

$$\#\{tB\cap \mathcal{O}_S\} = \sum_{x\in\mathcal{O}_S} \chi_{tB}(x) = \prod_{v\notin S} q_v^{-k_v/2}\mathcal{F}_S\chi_{tB}(0) = \prod_{v\notin S} q_v^{-k_v/2}\mathrm{Vol}(tB).$$

The second equality in (63) follows because $\mathrm{Vol}(F_S/\mathcal{O}_S) = \prod_{v\notin S} q_v^{-k_v/2}$ ([47, Proposition 3.5.1]). Note there is no error term in this case. ☐

For our applications, we need a more general version of Proposition 32 where B is an open compact subset of F_S^n and is first hit by some linear transform g belonging to some open compact subset of $\mathrm{GL}_n(F_S)$ and then scaled by some diagonal matrix t.

prop:skewexp **Proposition 33.** *Let B be an open compact subset of F_S^n. Let K be an open compact subset of $\mathrm{GL}_n(F_S)$. Let c be a positive real constant. Then for any $g\in K$ and for any $t=\mathrm{diag}(t_1,\dots,t_n)\in \mathrm{GL}_n(F_S)$ such that for any $i=1,\dots,n$, $|t_i|_v/|t_i|_{v'} < c$ for any $v,v'\in S$,*

$$\#\{tgB\cap \mathcal{O}_S^n\} = \mathrm{Vol}_{\mathcal{O}_S^n}(tgB) + O(\mathrm{Vol}(\mathrm{proj}(tgB))), \tag{64}$$ eq:skew

where $\mathrm{Vol}_{\mathcal{O}_S^n}$ is a constant multiple of Vol such that $F_S^n/\mathcal{O}_S^n$ has volume 1, and $\mathrm{Vol}(\mathrm{proj}(tgB))$ denotes the greatest d-dimensional volume of any projection of tgB 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 F, B, K and c.

Proof. The definition of the Fourier transform (59) generalizes to higher dimensions where one replaces xy by $x_1y_1+\cdots+x_ny_n$ when $x=(x_1,\dots,x_n)$, and $y=(y_1,\dots,y_n)$. The Poisson summation formula (62) generalizes to

$$\sum_{x\in\mathcal{O}_S^n} f(x) = \left(\prod_{v\notin S} q_v^{-k_v/2}\right)^n \sum_{y\in(\mathcal{O}_S^{\perp})^n} \mathcal{F}_S f(y), \tag{65}$$ eq:poissonhigh

for any continuous function f with continuous Fourier transform. The notion of conductor also generalizes and we write

$$c(B) = \prod_{v\in S}(\pi_v^{c_{v,1}}\mathcal{O}_v\times\cdots\times\pi_v^{c_{v,n}}\mathcal{O}_v) \subset \prod_{v\in S} K_v^n.$$

As g varies in the open compact set K, the conductor $c(\chi_{gB})$ of the characteristic function of gB takes only finitely many possibilities and the number of translates of $c(\chi gB)$ needed to cover gB also has finitely many possibilities. Moreover, there is a real constant M that bounds the S-norm of every $\mathcal{O}_S$-coordinate of gb for any $g\in K$ and any $b\in B$. These are the only dependency on K and B. In what follows, we replace gB by B.

As in the proof of Proposition 32, we may assume that each $-v(t_i)$ is bounded below by some constant C_1 depending only on M and c. For each $i=1,\dots,n$, we define the constants

$$C_{2,i} = \sum_v k_v\deg v + \sum_{v\in S} c_{v,i}\deg v.$$

Let I be a subset of $\{1,\dots,n\}$. Suppose

$$\begin{aligned}\sum_{v\in S} -v(t_i)\deg(v) &> C_2, \quad \forall i\in I\\ \sum_{v\in S} -v(t_i)\deg(v) &\leq C_2, \quad \forall i\notin I.\end{aligned}$$

Then if $(y_1,\dots,y_n)\in \mathrm{Supp}(\mathcal{F}_S\chi_{tB})\cap(\mathcal{O}_S^{\perp})^n$, we have $y_i=0$ for all $i\in I$. When $I=\{1,\dots,n\}$, then $\mathrm{Supp}(\mathcal{F}_S\chi_{tB})\cap(\mathcal{O}_S^{\perp})^n$ contains no nonzero element and just as in the proof of Proposition 32, we get the main term $\mathrm{Vol}_{\mathcal{O}_S^n}(tB)$ in (64).

Suppose now I is a proper subset of $\{1,\dots,n\}$. Without loss of generality, we may assume $I=\{i,\dots,n\}$ for some $i\geq 2$. We write $\mathrm{proj}_{i,\dots,n}$ for the projection onto the last $n-i+1$ coordinates and $\mathrm{proj}_{1,\dots,i-1}$ for the projection on the first $i-1$ coordinates. Our goal is to show that

$$\#\{tB\cap\mathcal{O}_S^n\}\leq C_3\mathrm{Vol}(\mathrm{proj}_{i,\dots,n}(tB))$$

for some constant C_3 depending only on F, the bound of the S-norm of elements of B, the conductor $c(B)$ of B, and c.

Any element $(y_1,\dots,y_n)$ of $\mathrm{Supp}(\mathcal{F}_S\chi_{tB})\cap(\mathcal{O}_S^{\perp})^n$ has the property that $y_j=0$ for any $j=i,\dots,n$, and for any $j=1,\dots,i-1$,

$$\begin{aligned} v(y_j) &\geq -k_v, \quad \forall v\notin S,\\ v(y_j) &\geq -c_{v,j}-v(t_j)-k_v \quad \forall v\in S. \end{aligned}$$

As before, all the possible $(i-1)$-tuples $(y_1,\dots,y_{i-1})$, as t varies, belong to some finite set U depending only on F, C_1 and C_2.

For any $(x_i,\dots,x_n)\in\mathrm{proj}_{i,\dots,n}(tB)$, let $B(t,x_i,\dots,x_n)$ denote the (open compact) subset of F_S^{i-1} consisting of elements $(x_1,\dots,x_{i-1})$ such that $(x_1,\dots,x_n)\in tB$. Then $\mathrm{Supp}(\mathcal{F}_S\chi_{B(t,x_i,\dots,x_n)})$ is contained in U. This follows because the conductor of $B(t,x_i,\dots,x_n)$ contains $\mathrm{proj}_{1,\dots,i-1}(c(tB))$. Let C_S denote the constant $\prod_{v\notin S}q_v^{-k_v/2}$. Then

$$\begin{aligned}
\#\{tB\cap\mathcal{O}_S^n\} &= C_S^n\sum_{y\in U}\mathcal{F}_S\chi_{tB}(y,0,\dots,0)\\
&= C_S^n\sum_{y\in U}\int_{\substack{(x_i,\dots,x_n)\\ \in\mathrm{proj}_{i,\dots,n}(tB)}}\int_{\substack{(x_1,\dots,x_{i-1})\\ \in B(t,x_i,\dots,x_n)}}\chi_S(x_1y_1+\cdots+x_{i-1}y_{i-1})d_Sx\\
&= C_S^n\int_{\substack{(x_i,\dots,x_n)\\ \in\mathrm{proj}_{i,\dots,n}(tB)}}\sum_{y\in U}\mathcal{F}_S\chi_{B(t,x_i,\dots,x_n)}(y)\\
&= C_S^{n-i+1}\int_{\substack{(x_i,\dots,x_n)\\ \in\mathrm{proj}_{i,\dots,n}(tB)}}\#\{B(t,x_i,\dots,x_n)\cap\mathcal{O}_S^{i-1}\}d_Sx\\
&\leq C_S^{n-i+1}\int_{\substack{(x_i,\dots,x_n)\\ \in\mathrm{proj}_{i,\dots,n}(tB)}}\#\{\mathrm{proj}_{1,\dots,i-1}(tB)\cap\mathcal{O}_S^{i-1}\}d_Sx\\
&= C_S^{n-i+1}\mathrm{Vol}(\mathrm{proj}_{i,\dots,n}(tB))\#\{\mathrm{proj}_{1,\dots,i-1}(tB)\cap\mathcal{O}_S^{i-1}\}.
\end{aligned}$$

Finally the same argument as in the proof of Proposition 32 shows that

$$\#\{\mathrm{proj}_{1,\dots,i-1}(tB)\cap\mathcal{O}_S^{i-1}\}\leq C_4$$

for some constant C_4 depending only on F, the bound of the S-norm of elements of B, the conductor $c(B)$ of B, and c. This completes the proof of Proposition 33.

□

Acknowledgments

The first and third authors were supported by a Simons Investigator Grant, and we thank the Simons Foundation for their kind support of this work.

References

Artn [1] E. Artin, Questions de base minimale dans la théorie des nombres algébriques, *Collected papers of Emil Artin*, Addison-Wesley, Reading, MA, 1965, 229–321.

BII [2] M. Bhargava, Higher composition laws. II. On cubic analogues of Gauss composition, *Ann. of Math. (2)* **159** no. 2 (2004), 865–886.

BIII [3] M. Bhargava, Higher composition laws. III. The parametrization of quartic rings, *Ann. of Math. (2)* **159** no. 3 (2004), 1329–1360.

BIV [4] M. Bhargava, Higher composition laws. IV. The parametrization of quintic rings, *Ann. of Math. (2)* **167** no. 1 (2008), 53–94.

Bmass [5] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Int. Math. Res. Not. IMRN* no. 17 (2007), 20 pp.

dodqf [6] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* **162**, 1031–1063.

dodpf [7] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math.* (2), **172** (2010), no. 3, 1559–1591.

Bgeosieve [8] M. Bhargava, The geometric sieve and the density of squarefree values of polynomial discriminants and other invariant polynomials, `http://arxiv.org/abs/1402.0031`.

B [9] M. Bhargava, Most hyperelliptic curves over $\mathbb{Q}$ have no rational points, `http://arxiv.org/abs/1308.0395`.

hasse [10] M. Bhargava, A positive proportion of plane cubics fail the Hasse principle, `http://arxiv.org/abs/1402.1131`.

squarefree [11] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials, `http://arxiv.org/abs/1402.0031`.

BG1 [12] M. Bhargava and B. Gross, The average size of the 2-Selmer group of the Jacobians of hyperelliptic curves with a rational Weierstrass point, `http://arxiv.org/abs/1208.1007`, in: *Automorphic Representations and L-functions*, *TIFR Studies in Math.* **22** (2013), pp. 23–91.

BGW [13] M. Bhargava, B. Gross, and X. Wang, A positive proportion of locally soluble hyperelliptic curves over Q have no rational points over any odd degree extension, *J. Amer. Math. Soc.* **30** (2017), 451–493.

BH2 [14] M. Bhargava and W. Ho, Average sizes of Selmer groups in families of elliptic curves, Preprint.

BS2 [15] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, *Ann. of Math. (2)* **181** (2015), no. 1, 191–242.

TC [16] M. Bhargava and A. Shankar, Ternary cubic forms having bounded invariants and the existence of a positive proportion of elliptic curves having rank 0, *Ann. of Math. (2)* **181** (2015), no. 2, 587–621.

foursel [17] M. Bhargava and A. Shankar, The average number of elements in the 4-Selmer groups of elliptic curves is 7, `http://arxiv.org/abs/1312.7333`.

fivesel [18] M. Bhargava and A. Shankar, The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, `http://arxiv.org/abs/1312.7859`.

BST [19] M. Bhargava, A. Shankar and J. Tsimerman, On the Davenport-Heilbronn theorems and second order terms, *Invent. Math.* **193** (2013), no. 2, 439–499.

BSW [20] M. Bhargava, A. Shankar and X. Wang, Geometry-of-numbers methods over global fields II: Coregular representations. In preparation.

rankone [21] M. Bhargava and C. Skinner, A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one, *J. Ramanujan Math. Soc.* **29** (2014), no. 2, 221–242.

bsddensity [22] M. Bhargava, C. Skinner, and W. Zhang, A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer Conjecture, `http://arxiv.org/abs/1407.1826`.

BV [23] M. Bhargava and I. Varma, The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders, *Proc. Lond. Math. Soc. (3)* **112** (2016), no. 2, 235–266.

BV2 [24] M. Bhargava and I. Varma, On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields, Duke Math. J. **10** (2015), 1911–1933.

Brl [25] A. Borel, Some finiteness properties of adele groups over number fields, *Publ. Math. IHES* **16** (1983), 5–30.

BP [26] A. Borel, G. Prasad, Finiteness thoerems for discrete subgroups of bounded covolume in semi-simple groups, *Publ. Math. IHES* **69** (1989), 119–171.

Cnrd [27] B. Conrad, Finiteness theorems for algebraic groups over function fields, *Compos. Math.* **148** No.2 (2012), 555–639.

DW [28] B. Datskovsky and D. Wright, Density of discriminants of cubic extensions, *J. Reine Angew.* **386** (1998). 116–138.

Lipschitz [29] H. Davenport, On a principle of Lipschitz, *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: "On a principle of Lipschitz ", *J. London Math. Soc.* **39** (1964), 580.

DH [30] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields, II, *Proc. Roy. Soc. London Ser. A* **322** no.1551 (1971), 405–420.

DF [31] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

AWD [32] A. W. Deng, Rational points on weighted projective spaces, `http://arxiv.org/abs/math/9812082`.

G [33] B. Gross, On the motive of a reductive group, *Invent. math.* no. 130 (1997), 287–313.

JP [34] M. Jarden and G. Prasad, Appendix on the discriminant quotient formula for global field, *Inst. Hautes Études Sci. Publ. Math.* no. 69 (1989), 115–117.

KW [35] A. Kable and D. Wright, Uniform distribution of the Steinitz invariants of quadratic and cubic extensions, *Compos. Math.* **142** no. 1 (2006), 84–100.

KL [36] Z. Klagsbrun, Davenport-Heilbronn Theorems for Quotients of Class Groups `http://arxiv.org/abs/1701.02834`.

Mlnr [37] J. Milnor, *Introduction to Algebraic K-theory*, Princeton University Press and University of Tokyo Press, 1971.

Os [38] J. Oesterle, Nombres de Tamagawa et groupes unipotents en caractéristique p, *Invent. Math.* **78** no. 1 (1984), 13–88.

PS2 [39] B. Poonen, M. Stoll, Most odd degree hyperelliptic curves have only one rational point, *Ann. of Math. (2)* **180** (2014), no. 3, 1137–1166.

SK [40] M. Sato and T. Kimura, A classification of irreducible prehomogeneous vector spaces and their relative invariants, *Nagoya Math. J.* **65** (1977), 1–155.

Smass [41] J.P. Serre, Une "formule de masse" pour les extensions totalement ramifiés de degré donné d'un corps local, *C. R. Acad. Sci. Paris Sér. A-B* **286** no. 22 (1978), A1031–A1036.

SW [42] A. Shankar, and X. Wang, Average size of the 2-Selmer group for monic even hyperelliptic curves, `http://arxiv.org/ab s/1307.3531`.

ST [43] A. Shankar. The average rank of elliptic curves over number fields, Ph.D thesis, Princeton 2012.

AJ [44] A. Shankar and J. Tsimerman, Counting S_5-fields with a power saving error term, *Forum Math. Sigma* **2** (2014), e13 (8 pages).

Sp [45] T. A. Springer, Reduction theory over global fields, *Proc. Indian Acad. Sci. (Math. Sci.)* **104** (1994), 207–216.

Th [46] J. Thorne, E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3, *Forum of Mathematics,* Π, Vol. 3 (2015), e1.

VF [47] M. van Frankenhuijsen, The Riemann hypothesis for function fields, *London Mathematics Society Student Texts* **80**, Cambridge University Press 2014.

Weil [48] A. Weil, *Adeles and algebraic groups*, Birkhäuser, 1982.

WoodThesis [49] M. M. Wood, Moduli spaces for rings and ideals, Ph.D. Th esis, Princeton University, June 2009.

WoodQuartic [50] M. M. Wood, Parametrizing quartic algebras over an arbitrary base, *Algebra* & *Number Theory*, **5-8** (2011), 1069–1094.

MWsp [51] M. M. Wood, How to determine the splitting type of a prime, unpublished note, available at http://www.math.wisc.edu/∼mmwood/Splitting.pdf.

WY [52] D. J. Wright and A. Yukie, Prehomogeneous vector spaces and field extensions, *Invent. Math.* **110** (1992), 283–314.