Asymptotics of extensions of simple $\mathbb{Q}$-algebras

Fabian Gundlach[*†] Béranger Seguin[*‡]

Abstract. We answer various questions concerning the distribution of extensions of a given central simple algebra K over a number field. Specifically, we give asymptotics for the count of inner Galois extensions L/K of fixed degree and center with bounded discriminant. We also relate the distribution of outer extensions of K to the distribution of field extensions of its center $Z(K)$. This paper generalizes the study of asymptotics of field extensions to the noncommutative case in an analogous manner to the program initiated by Deschamps and Legrand to extend inverse Galois theory to division algebras.

MSC 2020: 11N45 · 12E15 · 11R52

Contents

1. Introduction 1
2. Inner Galois extensions 6
3. Outer extensions 23
4. General extensions 28

1. Introduction

1.1. Context

The study of statistics of field extensions turns inverse Galois theory into a quantitative problem, replacing the question of the existence of extensions with a given Galois group by the question of their asymptotic distribution. The main conjecture in this area was introduced by Malle in [Mal02, Mal04] as a proposed generalization of results of Mäki and Wright for abelian extensions of number fields [Mäk85, Wri89]. This conjecture has received a lot of attention and has been studied using various methods: for some recent articles, see for example [Wan21, Klü22, ETW23, ESZB23, KP23, Mot23]. Another active area concerns the distribution of extensions of fixed degree without specifying a Galois group, see [Coh54, DH71, Bha05, Bha10] for small degrees and [Sch95, EV06, Cou20, BSW22, LT22] for all degrees.

Noncommutative Galois theory was developed in [Jac40, Jac47, Car47]. We will define the notions we need, but readers wanting to learn more may refer to [Coh95, Jac56] or to the introductory sections of [Des18, Des23]. In [DL20], a program was initiated[1] to extend inverse Galois theory to division rings. Since then, this question has been vastly explored, and fundamental results were

[*]Universität Paderborn, Fakultät EIM, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany.
[†]Email: fabian.gundlach@uni-paderborn.de.
[‡]Email: math@beranger-seguin.fr.

[1]One may argue that first steps towards this program were taken by research concerning *admissible* groups, cf. for example [Sch68, HHK11].

obtained in the articles [ALP20, Beh21, Des21, BDL22, Leg22a, Leg22b, Leg24]. This article aims, in a similar manner, to study the quantitative aspects of extensions of noncommutative algebras.

1.2. Focus of this work

Our objects of study are (finite-dimensional) simple $\mathbb{Q}$-algebras. If K is such an algebra, its center $Z(K)$ is a number field.

Definition 1.1. An *extension* of a simple $\mathbb{Q}$-algebra K is a simple $\mathbb{Q}$-algebra L equipped with an injective $\mathbb{Q}$-algebra homomorphism $K \hookrightarrow L$. We usually think of K as a subalgebra of L via this embedding. An *isomorphism* between extensions L_1 and L_2 of K with embeddings $e_1 : K \hookrightarrow L_1$ and $e_2 : K \hookrightarrow L_2$ is a $\mathbb{Q}$-algebra isomorphism $i : L_1 \xrightarrow{\sim} L_2$ such that $e_2 = i \circ e_1$.

Let L/K be an extension of simple $\mathbb{Q}$-algebras. We denote by $\mathrm{Aut}(L/K)$ the automorphism group of L/K, i.e., the set of $\mathbb{Q}$-algebra automorphisms of L which act trivially on K. The *degree* is defined as $[L : K] := \frac{\dim_{\mathbb{Q}}(L)}{\dim_{\mathbb{Q}}(K)}$. If K is a division algebra, the degree agrees with the dimension of L both as a left K-vector space and as a right K-vector space. In Subsection 1.4, we define a quantity $d(L/K) \in \mathbb{Q}_{>0}$, which we treat as "(the absolute value of) the norm of the relative discriminant of L/K". One may then ask the following question:

Question 1.2. Let K be a simple $\mathbb{Q}$-algebra and $n \geq 2$. How many isomorphism classes of extensions L/K of degree n are there which satisfy the bound $d(L/K) \leq X$, asymptotically as $X \to +\infty$?

Question 1.2 is very general. For instance, the extensions it aims to count include field extensions of number fields, which are notoriously hard to parametrize. Instead of studying this general problem, we address two more specific questions, focusing only on certain types of extensions. More precisely, we study the asymptotics of "inner Galois extensions" and of "outer extensions", defined below. The former question turns out to admit a complete answer which we give in Theorem 2.16, whereas the latter reduces to well-studied questions concerning the distribution of commutative field extensions, as we explain in Section 3. These two types of extensions are representative of all extensions of K, as by Theorem 4.2 every extension L/K of simple algebras splits "naturally" into a tower $L/L'/K$ where L/L' is inner Galois and L'/K is outer. (Here, L' is the double-centralizer of K in L.) This fact could be used to address more general variants of Question 1.2, as we briefly discuss in Section 4.

Throughout the article, we make a special effort to include simple algebras which are not division algebras in all discussions, but we also systematically prove the corresponding statements focusing exclusively on division algebras.

1.2.1. Inner Galois extensions.

In Section 2, we restrict our attention to *inner Galois extensions* of a simple $\mathbb{Q}$-algebra K, where an extension L/K is:

- *inner* if all of its automorphisms are inner, i.e., given by conjugation by an element of $L^\times$;
- *Galois* if K equals the algebra $L^{\mathrm{Aut}(L/K)} := \{x \in L \,|\, \forall \sigma \in \mathrm{Aut}(L/K), \sigma(x) = x\}$.

As we explain in Lemma 2.3, an extension L/K is inner Galois if and only if $Z(L) \subseteq Z(K)$.

In Theorem 2.16, we give asymptotics for the number of inner Galois extensions L/K with given degree n and given center $Z = Z(L)$ that satisfy the discriminant bound $d(L/Z) \leq X$. These asymptotics take the form $CX^{1/a}(\log X)^{b-1}$ for explicitly given constants a and b, and for a real number C which is positive unless no inner Galois extension of K of degree n with center Z exists.

Fixing the center lets us reduce the problem to a question about central simple Z-algebras. The count of all inner Galois extensions of K of degree n (with any center) can in principle be obtained by summing the resulting asymptotics over the finitely many subfields Z of $Z(K)$.

In the case $K = Z(K) = Z$, the extensions we are counting are exactly the central simple Z-algebras of degree n satisfying the discriminant bound $d(L/Z) \leq X$. This special case of Theorem 2.16 was already established in [LMPT18, Theorem 1.5 and Lemma 3.2].

Previous work on this question also includes [FKS81, Corollary 4], where (combined with [Stacks, Theorem 074Z]) the authors prove that infinitely many central simple Z-algebras L contain a given commutative field extension $K = Z(K)$ of Z as a maximal subfield (i.e., $[L : Z] = [K : Z]^2$). The definition of the main exponent $1/a$ in our final asymptotics relies on a group-theoretical lemma they prove to this end (Lemma 2.8).

Our proof strategy is similar to that of [LMPT18]: we reduce the problem to counting central simple Z-algebras satisfying certain local conditions, we parametrize these algebras by elements of the Brauer group $\mathrm{Br}(Z)$, and we set up a Dirichlet series counting them. The local-global principle for Brauer groups lets us write the Dirichlet series as a sum of finitely many Euler products. Finally, we determine its rightmost "pole" by comparison with Artin L-functions and apply a Tauberian theorem to prove Theorem 2.16. Additional computations ensure that the leading coefficients of our asymptotics are positive when there is at least one such extension. We also give the asymptotics when K is a division algebra and we count only extensions which are division algebras.

We also prove Theorem 2.20, which is a variant of Theorem 2.16 in which discriminants are replaced by products of ramified primes. The proof strategy is identical.

1.2.2. Outer extensions. An extension L of K is *outer* if it has no nontrivial inner automorphisms. In Section 3, we prove Theorem 3.3, which shows that outer extensions L/K are exactly those of the form $L = F' \otimes_{Z(K)} K$ for a field extension F' of $Z(K)$. This generalizes a theorem of Deschamps and Legrand [DL20, Corollaire 2]. A consequence of this theorem is that the problem of counting outer extensions of K reduces to the notoriously difficult problem of counting field extensions of $Z(K)$. Additional computations let us characterize extensions which are division algebras and compute discriminants in terms of invariants of the extension $F'/Z(K)$ (Theorem 3.6). We give a few applications of these ideas in Subsection 3.3.

1.2.3. General extensions. In Section 4, we briefly discuss the possibility of adapting the methods of Sections 2 and 3 in order to count more general extensions L/K by decomposing them into inner and outer extensions. We highlight a few helpful facts, but also analytic difficulties specific to this problem.

1.3. Preliminaries and notation

1.3.1. Brauer groups of local and global fields.

Central simple algebras. In this article, simple algebras are systematically assumed to be finite-dimensional over their center. If F is a field and K is a central simple F-algebra, we denote by $[K] \in \mathrm{Br}(F)$ the class of K in the Brauer group of F. The *index* of K is the integer $\mathrm{ind}(K)$ such that K is isomorphic to a matrix algebra over a central division F-algebra of dimension $\mathrm{ind}(K)^2$. Note that K is a division algebra if and only if $[K : F] = \mathrm{ind}(K)^2$. The *exponent* of K is the order of $[K]$ in $\mathrm{Br}(F)$. When F is a global or local field, which is systematically true in this article, the exponent of K equals its index [Rei03, (31.4), (32.19)] (see [DesInd] for counterexamples in the general case).

Brauer groups of local fields. Brauer groups of local fields admit explicit descriptions:

- The Brauer group of $\mathbb{C}$ is trivial. We identify it with the trivial subgroup of $\mathbb{Q}/\mathbb{Z}$ via the trivial group homomorphism $\mathrm{inv} : \mathrm{Br}(\mathbb{C}) \to \mathbb{Q}/\mathbb{Z}$.

- The Brauer group of $\mathbb{R}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, generated by the class of the algebra of Hamilton quaternions over $\mathbb{R}$. We identify it with the subgroup $\{0, \frac{1}{2}\}$ of $\mathbb{Q}/\mathbb{Z}$ via the group homomorphism $\mathrm{inv} : \mathrm{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}$ mapping the nontrivial element to $\frac{1}{2}$.
- If F is a non-archimedean local field, then there is an isomorphism $\mathrm{inv} : \mathrm{Br}(F) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ [Rei03, (31.8)].

The *Hasse invariant* of a central simple algebra over a local field is the image in $\mathbb{Q}/\mathbb{Z}$ of its class.

Brauer groups of global fields. Assume that F is a global field. If K is a central simple F-algebra and v is a place of F, we denote by F_v the completion of F at v and by $K_v := K \otimes_F F_v$ the completion of K at v, which is a central simple algebra over the local field F_v. We call the element $\mathrm{inv}(K_v) \in \mathbb{Q}/\mathbb{Z}$ the *local invariant* of K at v.

Let $\mathcal{P}$ be the set of all places of F. The local-global principle for Brauer groups of global fields (the Albert–Brauer–Hasse–Noether theorem) is summed up by the exact sequence [Rei03, (32.13)]:

$$1 \to \mathrm{Br}(F) \to \bigoplus_{v \in \mathcal{P}} \mathrm{Br}(F_v) \xrightarrow[\sum_v \mathrm{inv}_v]{} \mathbb{Q}/\mathbb{Z} \to 1 \tag{1.1}$$

where $\sum_v \mathrm{inv}_v$ is the sum in $\mathbb{Q}/\mathbb{Z}$ of the Hasse invariants of the coordinates of an element of $\bigoplus_{v \in \mathcal{P}} \mathrm{Br}(F_v)$. Thus, a central simple F-algebra is uniquely determined (up to isomorphism) by its dimension M^2 and by the collection of its local invariants in $\mathbb{Q}/\mathbb{Z}$ (indexed by places of F), on which the only constraints are the following:

- all local invariants have order dividing M in $\mathbb{Q}/\mathbb{Z}$;
- all but finitely many local invariants are trivial;
- the local invariants at complex places are trivial;
- the local invariants at real places are either trivial or equal to $\frac{1}{2}$;
- the sum of the local invariants over all places of F is trivial.

1.3.2. Terminology and notation. If S is a finite set, we denote by $|S|$ its cardinality. We denote by $\mathrm{e} : \mathbb{C} \to \mathbb{C}$ the function $z \mapsto \exp(2\pi i z)$. If R is a ring, we denote by $\mathfrak{M}_n(R)$ the algebra of $n \times n$ matrices over R and by $\mathrm{End}_R(A)$ the algebra of endomorphisms of a (left or right) R-module A. We denote by $\|p\|$ the norm of a prime p of a number field F.

For $n \in \mathbb{N}$, we see $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of $\mathbb{Q}/\mathbb{Z}$, namely that of elements whose order divides n: if $a \in \mathbb{Z}/n\mathbb{Z}$, we denote by $\frac{a}{n}$ the corresponding element of $\mathbb{Q}/\mathbb{Z}$. When speaking about elements of $\mathbb{Z}/n\mathbb{Z}$, the phrases "a divides b", "a is the greatest common divisor (resp. the least common multiple) of b and c" and "b and c are coprime" must be interpreted as statements about the corresponding principal ideals, identified with positive divisors of n. For instance, the greatest common divisor of b and c is the unique positive divisor of n generating the same ideal of $\mathbb{Z}/n\mathbb{Z}$ as b and c together, i.e., $\gcd\left(\widetilde{b}, \widetilde{c}, n\right)$ where $\widetilde{b}, \widetilde{c} \in \mathbb{N}$ are arbitrary representatives of b, c.

If L is a $\mathbb{Q}$-algebra and K is a subalgebra of L, we use the following notation:

- The *centralizer* $\mathrm{Cent}_L(K)$ is the subalgebra of L consisting of those elements that commute with all elements of K;
- $\mathrm{Inn}(L/K)$ is the normal subgroup of $\mathrm{Aut}(L/K)$ consisting of inner automorphisms, i.e., those corresponding to conjugation by an element of $\mathrm{Cent}_L(K)^\times$.

Two elements of $\mathrm{Cent}_L(K)^\times$ induce the same inner automorphism if and only if they differ by an element of the center of L. Therefore, $\mathrm{Inn}(L/K) \simeq \mathrm{Cent}_L(K)^\times / Z(L)^\times$.

1.4. Discriminants

We associate to an extension L/K of simple $\mathbb{Q}$-algebras a number $d(L/K)$, which we use as a substitute for the absolute value of the norm of the relative discriminant of L over K. When L/K is an extension of number fields, $d(L/K)$ has precisely that meaning.

1.4.1. The case $K \subseteq Z(L)$. Assume that K is contained in the center of L. In this case, there is a well-defined notion of discriminant: the number field K has a unique maximal $\mathbb{Z}$-order, namely its ring of integers $\mathcal{O}_K$, and one can choose a maximal $\mathcal{O}_K$-order Λ in L [Rei03, (10.4)]. Although Λ is not unique in general, the discriminant of $\Lambda/\mathcal{O}_K$ does not depend on the choice of Λ [Rei03, (25.3)]. Therefore, we simply denote by $d(L/K)$ the integer obtained as the absolute value of the norm of the discriminant of $\Lambda/\mathcal{O}_K$, for any choice of maximal order Λ in L.

First, consider the case $K = Z(L)$. Then, L is a central simple K-algebra of some dimension m^2. For each prime p of K, let $\lambda_p \in \mathbb{Z}/m\mathbb{Z}$ be such that $\mathrm{inv}(L_p) = \frac{\lambda_p}{m}$. The local index $m_p = \mathrm{ind}(L_p)$ is the reduced denominator of this fraction, i.e., $m_p = \frac{m}{\gcd(m, \lambda_p)}$. By comparing dimensions, we see that L_p is an algebra of $\kappa_p \times \kappa_p$-matrices over a central division K_p-algebra of dimension m_p^2, where $\kappa_p = \frac{m}{m_p}$. A formula for the norm of the relative discriminant of $L/Z(L)$ follows from [Rei03, (25.10)]:

$$d(L/Z(L)) = \left(\prod_p \|p\|^{(m_p - 1)\kappa_p} \right)^m$$

where the product is taken over primes p of $Z(L)$. This can be rewritten in the following ways:

$$d(L/Z(L)) = \prod_p \|p\|^{m^2\left(1 - \frac{1}{m_p}\right)} = \prod_p \|p\|^{m\left(m - \gcd(m, \lambda_p)\right)}. \tag{1.2}$$

When K is a subfield of $Z(L)$, the computation of $d(L/K)$ reduces to the central case using the following "relative discriminant formula", which is a special case of [Rei03, Exercise 25.1a]:

$$d(L/K) = d(L/Z(L)) \cdot d(Z(L)/Z(K))^{[L:Z(L)]}. \tag{1.3}$$

1.4.2. A general definition. To measure the "size" of a general extension of simple $\mathbb{Q}$-algebras, we use the following quantity, which is both natural (cf. Proposition 1.4) and mysterious (cf. Remark 1.5):

Definition 1.3. Let L/K be an extension of simple $\mathbb{Q}$-algebras. We denote by $d(L/K)$ the positive rational number

$$d(L/K) := \frac{d(L/\mathbb{Q})}{d(K/\mathbb{Q})^{[L:K]}}.$$

Proposition 1.4. *Definition 1.3 is the only possible definition of a height $d(L/K)$ which coincides with the norm of the relative discriminant when $K \subseteq Z(L)$, and which satisfies the relative discriminant formula $d(M/K) = d(M/L)d(L/K)^{[M:L]}$ for every tower of extensions $M/L/K$.*

Proof. The uniqueness follows from the case $K = \mathbb{Q}$ of the relative discriminant formula for an arbitrary extension M/L. The relative discriminant formula for a tower $M/L/K$ of extensions follows formally from the "usual" relative discriminant formula for commutative fields combined with Equation (1.3). □

Remark 1.5. The number $d(L/K)$ is in general not an integer. For example, no prime but 2 is ramified in the $\mathbb{Q}$-algebra $L = \mathbb{Q}(i, j, k)$ of Hamilton quaternions, so $d(L/\mathbb{Q})$ is a power of 2, but L contains the commutative subfield $K = \mathbb{Q}(i+j+k) \simeq \mathbb{Q}(\sqrt{-3})$ in which 3 is ramified, so $3 \mid d(K/\mathbb{Q})$. Hence, the denominator of $d(L/K)$ is divisible by 3.

1.5. Acknowledgements

This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) — Project-ID 491392403 — TRR 358 (project A4). The authors thank Bruno Deschamps, Markus Kirschmer, and the anonymous referee for helpful discussions and feedback.

2. Inner Galois extensions

In this section, we state and prove Theorem 2.16, which gives asymptotics for the distribution of inner Galois extensions of a given (finite-dimensional) simple $\mathbb{Q}$-algebra, of fixed degree and center.

Subsection 2.1 contains useful lemmas concerning inner Galois extensions. In Subsection 2.2, we fix some notation and state the main theorem, Theorem 2.16.

The proof of Theorem 2.16 is spread over Subsections 2.3 to 2.7. In Subsection 2.3, we rephrase the problem in combinatorial terms. In Subsection 2.4, we set up the Dirichlet series for this counting problem. In Subsection 2.5, we describe analytic properties of the Dirichlet series and apply a Tauberian theorem. In Subsection 2.6, we check that the leading coefficient in our estimates is positive under the assumption that an extension exists (this proves the main statement Theorem 2.16 (i)). Finally, in Subsection 2.7, we establish Theorem 2.16 (ii), which is the result when one excludes extensions which are not division algebras.

In Subsection 2.8, we explain how to adapt the proof in order to prove Theorem 2.20, a variant of Theorem 2.16 where the height by which we count is the product of ramified primes. Finally, in Subsection 2.9, we give criteria for the existence of an extension as in Theorem 2.16.

2.1. General facts about inner Galois extensions

In this subsection, we establish general properties of inner Galois extensions. We begin with a characterization (Lemma 2.3), explain why inner Galois extensions of a simple algebra K with center Z can be identified with central simple Z-algebras in which K embeds (Proposition 2.4), and prove a criterion to decide whether there is an embedding between two simple algebras (Lemma 2.5).

We first prove the two following lemmas, which are not specific to inner Galois extensions:

Lemma 2.1. *Let K be a (finite-dimensional) algebra over an infinite field F. For every $x \in K$, there is a $\lambda \in F$ such that $x - \lambda$ is invertible.*

Proof. Embedding K into an algebra of matrices over F lets one see x as a square matrix with coefficients in F. Since its characteristic polynomial has finitely many roots and F is infinite, there is an element $\lambda \in F$ such that $x - \lambda$ is invertible. □

Lemma 2.2. *Let L/K be an extension of simple $\mathbb{Q}$-algebras. Then $L^{\mathrm{Inn}(L/K)} = \mathrm{Cent}_L(\mathrm{Cent}_L(K))$.*

Proof. Elements of $\mathrm{Inn}(L/K)$ are given by conjugation by elements of $\mathrm{Cent}_L(K)^\times$. Thus, $L^{\mathrm{Inn}(L/K)} = \mathrm{Cent}_L(\mathrm{Cent}_L(K)^\times)$. In particular, $\mathrm{Cent}_L(\mathrm{Cent}_L(K)) \subseteq L^{\mathrm{Inn}(L/K)}$. Conversely, if $x \in L^{\mathrm{Inn}(L/K)}$ and $y \in \mathrm{Cent}_L(K)$, use Lemma 2.1 to pick a $\lambda \in \mathbb{Q}$ such that $y - \lambda I \in \mathrm{Cent}_L(K)^\times$; since x belongs to $L^{\mathrm{Inn}(L/K)} = \mathrm{Cent}_L(\mathrm{Cent}_L(K)^\times)$, it commutes with $y - \lambda I$ and thus with y. □

The following lemma characterizes inner Galois extensions in a simple manner:

Lemma 2.3. *An extension L/K of simple $\mathbb{Q}$-algebras is inner Galois if and only if $Z(L) \subseteq Z(K)$.*

Proof.

(⇒) Since L/K is inner Galois, we have $K = L^{\mathrm{Inn}(L/K)} = \mathrm{Cent}_L(\mathrm{Cent}_L(K))$, where the second equality comes from Lemma 2.2. Hence:

$$Z(L) \subseteq \mathrm{Cent}_L(K) \cap \mathrm{Cent}_L(\mathrm{Cent}_L(K)) = \mathrm{Cent}_L(K) \cap K = Z(K).$$

($\Leftarrow$) By the Skolem–Noether theorem, the extension $L/Z(L)$ is inner. Since K contains $Z(K)$ and thus $Z(L)$, this implies that L/K is also inner. Proving that L/K is Galois then amounts to proving that the $Z(L)$-algebra K equals $L^{\mathrm{Inn}(L/K)}$, which is $\mathrm{Cent}_L(\mathrm{Cent}_L(K))$ by Lemma 2.2. The equality $K = \mathrm{Cent}_L(\mathrm{Cent}_L(K))$ follows from the centralizer theorem [Stacks, Theorem 074T]. □

Proposition 2.4. *The map sending an isomorphism class of inner Galois extensions L/K with center Z (as defined in Definition 1.1) to the isomorphism class of L as a Z-algebra (forgetting about the embedding $K \hookrightarrow L$) is injective.*

Proof. Let L_1, L_2 be central simple Z-algebras, isomorphic via an isomorphism $i : L_1 \xrightarrow{\sim} L_2$, and in which K embeds respectively via embeddings e_1 and e_2. By the form of the Skolem–Noether theorem given in [Stacks, Theorem 074Q], there is an (inner) automorphism α of L_2 such that $\alpha \circ i \circ e_1 = e_2$. Hence, (L_1, e_1) and (L_2, e_2) are isomorphic extensions of K in the sense of Definition 1.1. □

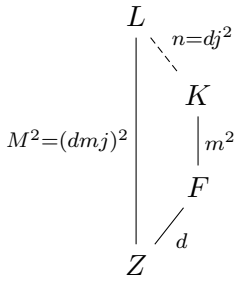
A consequence of Proposition 2.4 is that the problem of counting inner Galois extensions of K with center Z can be equivalently rephrased as counting central simple Z-algebras in which K embeds. This rephrasing is especially useful when combined with the following criterion, which lets one decide whether a simple Z-algebra K embeds into a central simple Z-algebra L:

Lemma 2.5. *Let F/Z be a field extension of degree d. Let L be a central simple Z-algebra of dimension M^2 and K be a central simple F-algebra of dimension m^2. The following are equivalent:*

(i) There is an embedding $K \hookrightarrow L$ of Z-algebras.

(ii) The number $j := \frac{M}{dm}$ is an integer, and there is a central simple F-algebra R of dimension j^2 such that $[L \otimes_Z F] = [K] + [R]$ in the Brauer group of F.

The degree of L over K is then $n := dj^2$. The situation is summed up by the following diagram:



Proof of Lemma 2.5.

(i) $\Rightarrow$ (ii) Assume that K embeds in L and see K as a subring of L via this embedding. Let $R = \mathrm{Cent}_L(K)$. By the centralizer theorem [Stacks, Theorem 074T], R is a simple Z-algebra of dimension $\frac{M^2}{dm^2}$ whose centralizer $\mathrm{Cent}_L(R)$ is K. Thus

$$Z(R) = R \cap \mathrm{Cent}_L(R) = \mathrm{Cent}_L(K) \cap K = Z(K) = F.$$

So R is a central simple F-algebra of dimension $\frac{M^2}{d^2m^2} = j^2$. In particular, j is an integer. See L as a right $(K^{\mathrm{op}} \otimes_Z L)$-module via the action induced by the formula $\lambda.(a \otimes \lambda') = a\lambda\lambda'$ for $\lambda, \lambda' \in L$ and $a \in K$. An endomorphism φ of the right $(K^{\mathrm{op}} \otimes_Z L)$-module L is determined by the element $\varphi(1)$. This lets us identify $\mathrm{End}_{K^{\mathrm{op}} \otimes_Z L}(L)$ with a subset of L. We let the reader check that this subset is precisely $\mathrm{Cent}_L(K) = R$. By [Stacks, Lemma 074F], the Z-algebra $K^{\mathrm{op}} \otimes_Z L$ is simple because both K and L are simple and $Z(L) = Z$. By [Stacks, Lemma 074E (5)], the equality $\mathrm{End}_{K^{\mathrm{op}} \otimes_Z L}(L) = R$ then implies that $\mathrm{End}_R(L) = K^{\mathrm{op}} \otimes_Z L = K^{\mathrm{op}} \otimes_F (F \otimes_Z L)$. Moreover, $\mathrm{End}_R(L)$ is a matrix algebra over R by [Stacks, Lemma 074E (6)]. Therefore, the classes of $K^{\mathrm{op}} \otimes_F (F \otimes_Z L)$ and of R coincide in the Brauer group of F, which implies $[F \otimes_Z L] - [K] = [R]$ and finally (ii).

(ii) ⇒ (i) Let $K' := K \otimes_F R$. By assumption, we have $[L \otimes_Z F] = [K']$ in the Brauer group of F. Since $\dim_F(L \otimes_Z F) = \dim_Z(L) = M^2 = (dmj)^2$ and $\dim_F(K') = \dim_F(K) \cdot \dim_F(R) = (mj)^2$, this implies that $L \otimes_Z F \simeq \mathfrak{M}_d(K')$.

Consider the central simple Z-algebra $\mathrm{End}_Z(K') \simeq \mathfrak{M}_{\dim_Z(K')}(Z)$. There are embeddings $K' \hookrightarrow \mathrm{End}_Z(K')$ and $(K')^{\mathrm{op}} \hookrightarrow \mathrm{End}_Z(K')$ coming from the respective actions of K' on itself via left and right multiplication. The images of these two embeddings commute as K' is associative.

Let $A = \mathrm{End}_Z(K') \otimes_Z \mathfrak{M}_d(Z)$. The embedding $K' \hookrightarrow \mathrm{End}_Z(K')$ induces the following embedding of L in A:

$$L \hookrightarrow L \otimes_Z F \simeq \mathfrak{M}_d(K') \simeq K' \otimes_Z \mathfrak{M}_d(Z) \hookrightarrow \mathrm{End}_Z(K') \otimes_Z \mathfrak{M}_d(Z) = A.$$

We see L as a subalgebra of A via this embedding. Let $C := \mathrm{Cent}_A(L)$. As L and A are central simple Z-algebras, we have $L \otimes_Z C \simeq A$ by [Stacks, Lemma 074U]. Since $A \simeq \mathfrak{M}_{\dim_Z(K') \cdot d}(Z)$, it follows that $[L] = [C^{\mathrm{op}}]$ in the Brauer group of Z. We have $\dim_Z(L) = M^2 = (dmj)^2$ and:

$$\dim_Z(C^{\mathrm{op}}) = \dim_Z(C) = \frac{\dim_Z(A)}{\dim_Z(L)} = \frac{\dim_Z(K')^2 \cdot d^2}{(dmj)^2} = \frac{(dm^2j^2)^2 \cdot d^2}{(dmj)^2} = (dmj)^2.$$

Therefore, there is an isomorphism $L \simeq C^{\mathrm{op}}$.

The inclusions $L \hookrightarrow K' \otimes_Z \mathfrak{M}_d(Z) \hookrightarrow A$ imply that $C = \mathrm{Cent}_A(L)$ contains $\mathrm{Cent}_A(K' \otimes_Z \mathfrak{M}_d(Z))$. The elements in the image of the embedding $(K')^{\mathrm{op}} \hookrightarrow \mathrm{End}_Z(K') \hookrightarrow A$ commute with those of $K' \otimes_Z \mathfrak{M}_d(Z)$ because they come from right multiplication by elements of K'. Therefore, these elements belong to C. This defines an embedding $(K')^{\mathrm{op}} \hookrightarrow C$, from which we finally obtain an embedding $K \hookrightarrow K \otimes_F R = K' = \left((K')^{\mathrm{op}}\right)^{\mathrm{op}} \hookrightarrow C^{\mathrm{op}} \simeq L$ as claimed. □

Remark 2.6. Several cases of Lemma 2.5 are classical:

- A commutative field extension F of Z of degree M is contained in a central simple Z-algebra L of dimension M^2 (as a maximal subfield) if and only if it is a splitting field, i.e., $L \otimes_Z F \simeq \mathfrak{M}_M(F)$. This is the case $m = j = 1$. Our proof of Lemma 2.5 draws inspiration from the proof of this special case given in [Stacks, Theorem 074Z].
- Two central simple Z-algebras L and K of the same dimension M^2 are isomorphic if and only if $[L] = [K]$ in the Brauer group of Z. This is the case $d = j = 1$.
- When $F = Z$ (i.e., $d = 1$), Lemma 2.5 specializes to a criterion for the inclusion of a central simple Z-algebra into another. This criterion appears in [Des23, Section 5] (cf. the definition and description of what Deschamps calls the Brauer group $\mathrm{Br}(K)$ of a central simple Z-algebra K):

  Corollary 2.7 (Deschamps). *Let Z be a field, let L be a central simple Z-algebra of dimension M^2 containing a central simple Z-algebra K of dimension m^2. Then, there is a central simple Z-algebra R of dimension $\left(\frac{M}{m}\right)^2$ such that $L \simeq R \otimes_Z K$, namely $R = \mathrm{Cent}_L(K)$.*

2.2. Notation and main theorem

In this subsection, after introducing the necessary terminology and notation, we state our main theorem, Theorem 2.16. The notations we fix here are in effect throughout all of Section 2.

2.2.1. The centers. We fix an extension F/Z of number fields and we let $d = [F : Z]$. We denote the set of places of Z by $\mathcal{P}$. For every place w of F, lying above a place v of Z, the *local degree of F/Z at w* is the integer $d_w := [F_w : Z_v]$.

We let G be the Galois group of the Galois closure $\widehat{F}$ of F/Z. The transitive action of G on the d embeddings of F into $\widehat{F}$ lets us see G as a transitive subgroup of $\mathfrak{S}_d$. For an unramified prime p of Z, we let $\mathrm{Frob}(p)$ be the conjugacy class of G consisting of the Frobenius automorphisms for primes of $\widehat{F}$ above p.

For an element $g \in G$, we denote by $\operatorname{cycgcd} g$ the greatest common divisor of the sizes of all the orbits of the action of g on $\{1, \dots, d\}$. Note that $\operatorname{cycgcd} g$ divides d, the sum of the sizes of all orbits. Since $\operatorname{cycgcd} g$ only depends on the conjugacy class of g, we use the same notation when g is a conjugacy class of G. Finally, we let:

$$U := \operatorname*{lcm}_{g \in G} \operatorname{cycgcd} g.$$

Lemma 2.8. *We have $U \geq 2$, unless $F = Z$.*

Proof. Assume that $F \neq Z$, i.e., $d \geq 2$. By a theorem of Fein, Kantor and Schacher[2] [FKS81, Theorem 1], the transitive subgroup G of $\mathfrak{S}_d$ contains a fixed-point-free element g whose order is a prime power p^k. Its orbits all have sizes divisible by p, so $p \mid \operatorname{cycgcd} g \mid U$. □

We describe U explicitly in two special cases:

Lemma 2.9. *If F/Z is Galois, then $\operatorname{cycgcd} g = \operatorname{ord}(g)$ for all $g \in G$, and U is the exponent of G.*

Proof. We have $d = |G|$ and $G \hookrightarrow \mathfrak{S}_d$ is the regular embedding. The orbits of $g \in G$ all have size $\operatorname{ord}(g)$ and thus $\operatorname{cycgcd} g = \operatorname{ord}(g)$. Finally, $U = \operatorname{lcm}_{g \in G} \operatorname{ord}(g)$ is the exponent of G. □

Lemma 2.10. *If $d = p^k$ is a prime power with $k \geq 1$, then $U = p^{k'}$ for some $1 \leq k' \leq k$.*

Proof. By Lemma 2.8, we have $U \geq 2$. On the other hand, U is by definition a divisor of d. □

2.2.2. The central simple algebra. We fix a central simple F-algebra K of dimension m^2. For every place w of F, we denote by κ_w the element of $\mathbb{Z}/m\mathbb{Z}$ such that the local invariant $\operatorname{inv}(K_w) \in \mathbb{Q}/\mathbb{Z}$ of K at w is $\frac{\kappa_w}{m}$.

Definition 2.11. We say that a place v of Z is *exceptional* if it is archimedean, or ramified in F, or if $\kappa_w \neq 0$ for some place $w|v$ of F. We denote by $\mathcal{P}^{\mathrm{ex}}$ the finite set of exceptional places of Z.

2.2.3. The degree. We fix an integer $j \geq 1$. We let $n = dj^2$ and $M = dmj$. In the rest of Section 2, our goal is to count inner Galois extensions L/K of degree n with center $Z(L) = Z$. If $n = 1$, then $d = j = 1$ and there is exactly one such extension, namely the trivial extension $L = K$. From now on, we exclude this case, and we assume that $n \geq 2$. Since $n = dj^2 \geq 2$, we have $j \geq 2$ or $d \geq 2$. By Lemma 2.8, it follows that $Uj \geq 2$. Hence, the following definition makes sense:

Definition 2.12. We denote by u the smallest prime number dividing Uj.

Definition 2.13. We define the rational number $\beta \in (0, 1]$ as follows:

$$\beta := \frac{1}{|G|} \cdot \Big|\Big\{g \in G \,\Big|\, u \text{ divides } j \cdot \operatorname{cycgcd}(g)\Big\}\Big| = \begin{cases} 1 & \text{if } u|j, \\ \frac{1}{|G|} \cdot \Big|\Big\{g \in G \,\Big|\, u \text{ divides } \operatorname{cycgcd} g\Big\}\Big| & \text{otherwise.} \end{cases}$$

[2] Thanks to Michael Giudici for pointing this theorem to us. Note that the proof of Fein, Kantor and Schacher relies on the classification of finite simple groups.

Note that u divides $j \cdot \operatorname{cycgcd}(g) = \frac{M}{dm/\operatorname{cycgcd}(g)}$ if and only if $\frac{dm}{\operatorname{cycgcd} g}$ divides $\frac{M}{u}$. Hence:

$$\beta = \frac{1}{|G|} \cdot \left| \left\{ g \in G \,\middle|\, \frac{dm}{\operatorname{cycgcd} g} \text{ divides } \frac{M}{u} \right\} \right|. \tag{2.1}$$

The following remarks help understand the constants u and β:

Remark 2.14. If F/Z is a Galois extension or d is a prime power, then u is the smallest prime factor of dj by Lemmas 2.9 and 2.10. Moreover, if F/Z is Galois and u does not divide j, then β is the proportion of elements of G whose order is divisible by u.

Remark 2.15. In the non-Galois case, the number u is not necessarily the smallest prime factor of dj. For instance, take $j = 1$, $Z = \mathbb{Q}$, and any number field F of degree 6 whose Galois closure has Galois group $\left\langle (1\ 4)(2\ 5), (1\ 3\ 5)(2\ 4\ 6) \right\rangle \subseteq \mathfrak{S}_6$, which is the transitive permutation group `6T4` in GAP notation and is isomorphic to A_4. This group contains no permutations whose cycles all have even sizes, i.e., $u \neq 2$. Instead, we have $u = 3$ as there are elements consisting of two 3-cycles.

2.2.4. Statement of the main theorem. Using the notation introduced above, we state the main result of this section:

Theorem 2.16.

(i) There is a real number $C \geq 0$ such that the number $N(X)$ of inner Galois extensions L/K of degree $n = dj^2$ with center Z and with $d(L/Z) \leq X$ satisfies

$$N(X) \underset{X \to \infty}{\sim} C X^{1/a} (\log X)^{b-1}$$

where $a = M^2 \left(1 - \frac{1}{u}\right)$ and $b = (u-1)\beta$. When $C = 0$, this is taken to mean that there is no such extension for any X.

(ii) The same holds if we restrict to inner Galois extensions L/K which are division algebras (with a possibly smaller constant C).

Remark 2.17. The relative discriminants $d(L/K)$ and $d(L/Z)$ differ by a constant factor that only depends on K and Z (cf. Subsection 1.4):

$$d(L/Z) = d(K/Z)^n \cdot d(L/K).$$

Hence, Theorem 2.16 continues to hold, with a different constant C, if we replace the condition $d(L/Z) \leq X$ by $d(L/K) \leq X$.

Proving Theorem 2.16 is the focus of Subsections 2.3 to 2.7. In Subsection 2.9, we give additional criteria to check the existence of an extension, in order to determine whether the leading coefficient C in Theorem 2.16 is positive.

Remark 2.18. We obtain a finer version of Theorem 2.16 where we constrain the behavior of L at finitely many places. Let S be a finite set of places of Z and let $\xi : S \to \mathbb{Z}/M\mathbb{Z}$ be a map. Then, Theorem 2.16 holds (with possibly smaller constants C) if one restricts to extensions whose local invariants at the places $v \in S$ are given by $\frac{\xi(v)}{M}$.

Remark 2.19. Our methods yield expressions for the leading coefficient C in Theorem 2.16, see Equation (2.10) and Equation (2.11). These expressions involve an infinite product over all primes of Z and the values at $s = 1$ (resp. the residue, for the trivial character) of the Artin L-functions of the irreducible characters of $G = \operatorname{Gal}(\widehat{F}/Z)$ (cf. the proof of Lemma 2.31). In Remark 2.35, we remark that in certain cases, including the case $F = Z$, only the residue of the Dedekind zeta function of Z at 1 (which is given by the class number formula) is needed.

2.2.5. Counting by the product of ramified primes. In [Woo10], Wood popularized the question of counting number fields not by discriminant, but by the product of ramified primes, which in her language is a *fair counting function* for abelian extensions. For any simple $\mathbb{Q}$-algebra L with center Z, we define:

$$\operatorname{ram}(L) = \prod_{\substack{p \text{ prime of } Z \\ \text{ramified in } L}} \|p\|.$$

In Subsection 2.8, we explain how to adapt the proof of Theorem 2.16 to count inner Galois extensions by the product of their ramified primes. This leads to the following result:

Theorem 2.20.

(i) There is a real number $C \geq 0$ such that the number $N(X)$ of inner Galois extensions L/K of degree $n = dj^2$ with center $Z(L) = Z$ and with $\operatorname{ram}(L) \leq X$ satisfies

$$N(X) \underset{X\to\infty}{\sim} CX(\log X)^{b^*-1}$$

where $b^* = j\left(\frac{1}{|G|}\sum_{g\in G} \operatorname{cycgcd} g\right) - 1$. When $C = 0$, this is taken to mean that there is no such extension for any X.

(ii) The same holds if we restrict to inner Galois extensions L/K that are division algebras (with a possibly smaller constant C).

Remark 2.21. We have $b^* > 0$ because we have assumed that $j \geq 2$ or $d \geq 2$, which by Lemma 2.8 implies $\operatorname{cycgcd} g \geq 2$ for some $g \in G$.

2.3. Combinatorial formulation of the counting problem

In this subsection, we rephrase the counting problem combinatorially with the help of the Albert–Brauer–Hasse–Noether theorem. First, we specialize the criterion from Lemma 2.5 to the case of number fields:

Lemma 2.22. *Let L be a central simple Z-algebra of dimension M^2. For every place v of Z, let λ_v be the element of $\mathbb{Z}/M\mathbb{Z}$ such that $\operatorname{inv}(L_v) = \frac{\lambda_v}{M}$. Then, the following are equivalent:*

(i) There is an embedding $K \hookrightarrow L$ of Z-algebras.

(ii) For each place w of F, lying above a place v of Z, we have $dm \mid d_w\lambda_v - dj\kappa_w$ in $\mathbb{Z}/M\mathbb{Z}$.

Proof. By Lemma 2.5, K embeds in L if and only if there is a central simple F-algebra R of dimension j^2 such that $[L \otimes_Z F] = [K] + [R]$ in $\operatorname{Br}(F)$. This amounts to the condition that the index of $[L \otimes_Z F] - [K]$ divide j. Since index and exponent coincide, and by the exact sequence of Equation (1.1), this means that for every place w of F, we have $j \cdot ([L \otimes_Z F_w] - [K_w]) = 0$ in $\operatorname{Br}(F_w)$. By [Rei03, (31.9)], if w is place of F lying above a place v of Z, then $\operatorname{inv}(L \otimes_Z F_w) = [F_w : Z_v] \cdot \operatorname{inv}(L_v) = d_w \frac{\lambda_v}{M}$. Recall also that $\operatorname{inv}(K_w) = \frac{\kappa_w}{m}$. We finally obtain that K embeds in L if and only if, for each place w of F, lying above a place v of Z, the following equality holds in $\mathbb{Q}/\mathbb{Z}$:

$$\begin{aligned} 0 &= j \cdot \left(d_w \frac{\lambda_v}{M} - \frac{\kappa_w}{m}\right) \\ &= \frac{d_w\lambda_v}{dm} - \frac{j\kappa_w}{m}. \end{aligned}$$

This equality amounts to the divisibility $dm \mid d_w\lambda_v - dj\kappa_w$ in $\mathbb{Z}/M\mathbb{Z}$. □

We now give a combinatorial description of inner Galois extensions of K of degree n with center Z:

Definition 2.23. Let Λ be the set of maps $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ with finite support (i.e., identically zero outside a finite set) satisfying the following conditions:

(I) For all complex places $v \in \mathcal{P}$, we have $\lambda(v) = 0$.

(II) For all real places $v \in \mathcal{P}$, we have $\lambda(v) \in \{0, \frac{M}{2}\}$ (necessarily, $\lambda(v) = 0$ if M is odd).

(III) For all places $v \in \mathcal{P}$ and all places $w|v$ of F, we have $dm \mid d_w\lambda(v) - dj\kappa_w$ in $\mathbb{Z}/M\mathbb{Z}$.

(IV) $\sum_{v\in\mathcal{P}} \lambda(v) = 0$ in $\mathbb{Z}/M\mathbb{Z}$.

Let $\Lambda' \subseteq \Lambda$ be the set of maps that additionally satisfy:

(V) $\gcd_v \lambda(v) = 1$ in $\mathbb{Z}/M\mathbb{Z}$.

Theorem 2.24. *There is a bijection between the set of isomorphism classes of inner Galois extensions L/K of degree $n = dj^2$ with center $Z(L) = Z$ and the set Λ. Let L be such an extension and $\lambda \in \Lambda$ be the corresponding map. Then, L is a division algebra if and only if λ lies in Λ'. Moreover, the norm $d(L/Z)$ of the relative discriminant of L over its center Z equals the following quantity $d(\lambda)$, computed in terms of the map λ alone:*

$$d(\lambda) := \prod_{p \text{ prime of } Z} \|p\|^{M\left(M-\gcd\left(M,\lambda(p)\right)\right)}.$$

Proof. By Proposition 2.4, isomorphism classes of inner Galois extensions of K of degree n with center Z are in bijection with equivalence classes of central simple Z-algebras of dimension M^2 in which K embeds. By the characterizations of Paragraph 1.3.1, specifying a central simple Z-algebra L of dimension M^2 is the same as giving a map $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ with finite support satisfying conditions (I), (II) and (IV) of Definition 2.23. The local invariant of L at a place v of Z is then given by $\frac{\lambda(v)}{M} \in \mathbb{Q}/\mathbb{Z}$. By Lemma 2.22, the existence of an embedding of K into L is equivalent to condition (III).

The central simple algebra L is a division algebra if and only if it has index M. Since index and exponent coincide for central simple algebras over number fields, this is equivalent to the condition that the invariants $\mathrm{inv}(L_v)$ have least common denominator M, which is in turn equivalent to (V).

The formula for the discriminant follows from Paragraph 1.4.1. □

For non-exceptional places, condition (III) of Definition 2.23 takes a much simpler form:

Lemma 2.25. *Let $v \in \mathcal{P} \setminus \mathcal{P}^{\mathrm{ex}}$. Then, condition (III) of Definition 2.23 holds for all $w|v$ if and only if $\frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(v))}$ divides $\lambda(v)$.*

Proof. Since the prime v is not exceptional, we have $\kappa_w = 0$ for primes $w|v$ of F. Thus, condition (III) amounts to $\lambda(v)$ being a multiple of $\frac{dm}{\gcd(dm,d_w)}$ for all $w|v$. This means that $\lambda(v)$ is a multiple of $\mathrm{lcm}_{w|v} \frac{dm}{\gcd(dm,d_w)} = \frac{dm}{\gcd_{w|v} \gcd(dm,d_w)}$. Since $\gcd_{w|v} d_w$ divides $\sum_{w|v} d_w = d$, we have $\gcd_{w|v} \gcd(dm, d_w) = \gcd_{w|v} d_w$. To conclude, it remains to show that $\gcd_{w|v} d_w = \mathrm{cycgcd}(\mathrm{Frob}(v))$.

Since the prime v is non-exceptional, it is unramified in F. Pick a representative $g \in G$ of the conjugacy class $\mathrm{Frob}(v)$. Orbits of the action of g on $\{1, \dots, d\}$ correspond bijectively to primes $w|v$ of F, and the size of an orbit is the corresponding local degree d_w. Hence, $\gcd_{w|v} d_w$ is the greatest common divisor of the sizes of the orbits of g. By definition, this is $\mathrm{cycgcd}(\mathrm{Frob}(v))$. □

2.4. Setting up the Dirichlet series

In this subsection, we set up a Dirichlet series for the counting problem and rewrite it as a sum of Euler products.

We fix a divisor τ of M, which is used in Subsection 2.7 to sieve out extensions which are not division algebras. (For proving just part (i) of Theorem 2.16, one can take $\tau = 1$.)

Let S be a finite set of places of Z containing $\mathcal{P}^{\mathrm{ex}}$. Let ξ be a map $S \to \mathbb{Z}/M\mathbb{Z}$ satisfying conditions (I)–(III) of Definition 2.23 for all $v \in S$, and such that τ divides $\xi(v)$ for all $v \in S$. Define

$$\sigma_\xi := \sum_{v \in S} \xi(v)$$

and let $d(\xi)$ denote the contribution of places in S to the discriminant:

$$d(\xi) := \prod_{p \in S} \|p\|^{M\left(M - \gcd\left(M, \xi(p)\right)\right)}.$$

Let $\Lambda_{S,\xi,\tau} \subseteq \Lambda$ be the set of maps $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ in Λ whose restriction to S is ξ and such that τ divides $\lambda(v)$ for all places $v \in \mathcal{P}$. Via the bijection of Theorem 2.24, elements of $\Lambda_{S,\xi,\tau}$ correspond to isomorphism classes of central simple Z-algebras of dimension M^2 in which K embeds, whose local invariants at places $v \in S$ are given by $\frac{\xi(v)}{M}$, and whose index divides $\frac{M}{\tau}$. Moreover, if $\lambda \in \Lambda_{S,\xi,\tau}$ and L/K is the corresponding extension, then $d(L/Z) = d(\lambda)$. We are thus led to count maps $\lambda \in \Lambda_{S,\xi,\tau}$ with $d(\lambda) \leq X$. For this, we introduce the Dirichlet series:

$$f_{S,\xi,\tau}(s) = \sum_{\lambda \in \Lambda_{S,\xi,\tau}} d(\lambda)^{-s}.$$

To specify a map $\lambda \in \Lambda_{S,\xi,\tau}$, we only need to specify its restriction to $\mathcal{P} \setminus S$. Unraveling definitions and using Lemma 2.25, this lets us write:

$$f_{S,\xi,\tau}(s) = d(\xi)^{-s} \sum_{\text{(see below)}} \prod_{\substack{p \in \mathcal{P} \setminus S \\ \lambda(p) \neq 0}} \|p\|^{-sM\left(M - \gcd\left(M, \lambda(p)\right)\right)}. \tag{2.2}$$

where the sum is taken over finitely supported maps $\lambda\colon \mathcal{P} \setminus S \to \mathbb{Z}/M\mathbb{Z}$ such that:

(i) $\sigma_\xi + \sum_{p \in \mathcal{P} \setminus S} \lambda(p) = 0$ in $\mathbb{Z}/M\mathbb{Z}$, and

(ii) for all primes $p \in \mathcal{P} \setminus S$, both τ and $\frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(p))}$ divide $\lambda(p)$.

We encode condition (i) by the character sum

$$\frac{1}{M} \sum_{k=0}^{M-1} \mathrm{e}\left(\frac{k}{M}\left(\sigma_\xi + \sum_{p \in \mathcal{P} \setminus S} \lambda(p)\right)\right) = \frac{1}{M} \sum_{k=0}^{M-1} \mathrm{e}\left(\frac{k\sigma_\xi}{M}\right) \prod_{\substack{p \in \mathcal{P} \setminus S \\ \lambda(p) \neq 0}} \mathrm{e}\left(\frac{k\lambda(p)}{M}\right).$$

which equals 1 if (i) holds and 0 otherwise. We also let $\eta_{\tau,p} := \mathrm{lcm}(\frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(p))}, \tau)$, so that condition (ii) can be rewritten as $\eta_{\tau,p} | \lambda(p)$. Plugging this into Equation (2.2) lets us write the Dirichlet series as a finite sum of Euler products:

$$f_{S,\xi,\tau}(s) = \frac{d(\xi)^{-s}}{M} \sum_{k=0}^{M-1} \left(\mathrm{e}\left(\frac{k\sigma_\xi}{M}\right) \prod_{p \in \mathcal{P} \setminus S} \sum_{\substack{\lambda \in \mathbb{Z}/M\mathbb{Z} \\ \eta_{\tau,p} | \lambda}} \mathrm{e}\left(\frac{k\lambda}{M}\right) \|p\|^{-sM\left(M - \gcd(M,\lambda)\right)} \right). \tag{2.3}$$

We give a name to the Euler factor:

$$\mathbf{f}_{\tau,k,p}(s) := \sum_{\substack{\lambda \in \mathbb{Z}/M\mathbb{Z} \\ \eta_{\tau,p} | \lambda}} \mathrm{e}\left(\frac{k\lambda}{M}\right) \|p\|^{-sM\left(M - \gcd(M,\lambda)\right)}.$$

Then, Equation (2.3) can be rewritten as:

$$f_{S,\xi,\tau}(s) = \frac{d(\xi)^{-s}}{M} \sum_{k=0}^{M-1} \mathrm{e}\left(\frac{k\sigma_\xi}{M}\right) \prod_{p \in \mathcal{P} \setminus S} \mathbf{f}_{\tau,k,p}(s). \tag{2.4}$$

Split up the sum defining $\mathbf{f}_{\tau,k,p}(s)$, grouping values of λ according to the greatest common divisor $g = \gcd(M, \lambda)$, which must satisfy $\eta_{\tau,p} \mid g$ and $g \mid M$, and writing $\lambda = g\lambda'$ with $\lambda' \in \left(\mathbb{Z}/\frac{M}{g}\mathbb{Z}\right)^\times$. We have:

$$\begin{aligned}
\mathbf{f}_{\tau,k,p}(s) &= \sum_{\substack{g \geq 1 \text{ such that} \\ \eta_{\tau,p} | g \text{ and } g | M}} \sum_{\lambda' \in \left(\mathbb{Z}/\frac{M}{g}\mathbb{Z}\right)^\times} \mathrm{e}\left(\frac{kg\lambda'}{M}\right) \|p\|^{-sM(M-g)} \\
&= 1 + \sum_{\substack{1 \leq g < M \text{ such that} \\ \eta_{\tau,p} | g \text{ and } g | M}} \sum_{\lambda' \in \left(\mathbb{Z}/\frac{M}{g}\mathbb{Z}\right)^\times} \mathrm{e}\left(\frac{kg\lambda'}{M}\right) \|p\|^{-sM(M-g)}.
\end{aligned}$$

Finally, for $g | M$, define

$$g_k\left(\frac{M}{g}\right) = \sum_{\lambda' \in (\mathbb{Z}/\frac{M}{g}\mathbb{Z})^\times} \mathrm{e}\left(\frac{kg\lambda'}{M}\right)$$

so that

$$\mathbf{f}_{\tau,k,p}(s) = 1 + \sum_{\substack{1 \leq g < M \text{ such that} \\ \eta_{\tau,p} | g \text{ and } g | M}} g_k\left(\frac{M}{g}\right) \|p\|^{-sM(M-g)}. \tag{2.5}$$

Remark 2.26. The multiplicative function g_k takes the following value at an arbitrary $\frac{M}{g}$ dividing M:

$$g_k\left(\frac{M}{g}\right) = \frac{\varphi\left(\frac{M}{g}\right)}{\varphi\left(\frac{M}{\gcd(gk,\, M)}\right)} \cdot \mu\left(\frac{M}{\gcd(gk,\, M)}\right).$$

For instance, the function g_0 is Euler's totient function φ, and g_1 is the Möbius function μ.

2.5. Analytic properties of the Dirichlet series

All notations are as in the previous subsection. We define $a = M\left(M - \frac{M}{u}\right)$ as in Theorem 2.16. Our goal is to describe the behavior of the Euler products $\prod_{p \in \mathcal{P} \setminus S} \mathbf{f}_{\tau,k,p}(s)$ in the half-plane $\{\Re(s) \geq \frac{1}{a}\}$. We first show that the most significant term in each Euler factor $\mathbf{f}_{\tau,k,p}(s)$ is determined by the Frobenius automorphism associated to p (Lemma 2.27). We later use this information to relate the analytic properties of $\prod_p \mathbf{f}_{\tau,k,p}(s)$ to those of a product of powers of the Artin L-functions associated to the field extension $\widehat{F}/Z$ (Lemma 2.29 and Lemma 2.31). We then obtain asymptotics for the distribution of inner Galois extensions of L/K with degree n and center Z using Delange's Tauberian theorem (Corollary 2.34). This establishes most of Theorem 2.16 (i), the only missing point being that the leading coefficient is positive when such an extension exists.

Let $\psi_{\tau,k} \colon G \to \mathbb{C}$ be the following class function:

$$\psi_{\tau,k}(g) := \begin{cases} g_k(u) & \text{if } \operatorname{lcm}\left(\frac{dm}{\operatorname{cycgcd} g}, \tau\right) \text{ divides } \frac{M}{u}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.6}$$

We use $\psi_{\tau,k}$ to approximate the Euler factor $\mathbf{f}_{\tau,k,p}(s)$ as follows:

Lemma 2.27. *There is a constant $\varepsilon > 0$ such that, for $\Re(s) \geq \frac{1}{a}$:*

$$\mathbf{f}_{\tau,k,p}(s) = 1 + \psi_{\tau,k}(\mathrm{Frob}(p))\|p\|^{-as} + \mathcal{O}\Big(\|p\|^{-(1+\varepsilon)as}\Big),$$

where both ε and the implied constant in the $\mathcal{O}$-term are independent of p and s.

Proof. Consider the expression of $\mathbf{f}_{\tau,k,p}(s)$ given in Equation (2.5). If a proper divisor g of M occurs for a summand in $\mathbf{f}_{\tau,k,p}(s)$, then $\frac{M}{g}$ divides $\frac{M}{\eta_{\tau,p}}$, which divides $\frac{M}{dm/\operatorname{cycgcd}(\mathrm{Frob}(p))} = j \cdot \operatorname{cycgcd}(\mathrm{Frob}(p))$, which divides jU. By definition, the smallest divisor of jU besides 1 is u. Hence, the largest occurring proper divisor g of M is at most $\frac{M}{u}$. The corresponding summand, if it occurs, is $g_k(u)\|p\|^{-as}$. It follows that, for some $\varepsilon > 0$:

$$\begin{aligned}\mathbf{f}_{\tau,k,p}(s) &= \begin{cases} 1 + g_k(u)\|p\|^{-as} + \mathcal{O}\Big(\|p\|^{-(1+\varepsilon)as}\Big) & \text{if } \eta_{\tau,p} \mid \frac{M}{u} \\ 1 + \mathcal{O}\Big(\|p\|^{-(1+\varepsilon)as}\Big) & \text{otherwise} \end{cases} \\ &= 1 + \psi_{\tau,k}(\mathrm{Frob}(p))\|p\|^{-as} + \mathcal{O}\Big(\|p\|^{-(1+\varepsilon)as}\Big). \end{aligned}$$

□

An analytic lemma. We now prove Lemma 2.29, in which we approximate "Frobenian" Euler products using products of Artin L-functions. (See [FLN22, Section 2] for an introduction to Frobenian functions.) This is used later to analyze the behavior of $\prod_p f_{\tau,k,p}(s)$.

Definition 2.28. When z is a complex number, we define the holomorphic non-vanishing function $s \mapsto (s-1)^z$ on the open half-plane $\{\Re(s) > 1\}$ as $s \mapsto \exp(z \log(s-1))$, where log is the unique determination of the complex logarithm on the open half-plane $\{\Re(s) > 0\}$ taking real values on the positive real half-line.

Consider any irreducible representation ρ of G and let $\chi : G \to \mathbb{C}$ be the corresponding character. It is well-known that the Artin L-function $L(\rho, s)$ is holomorphic non-vanishing for $\Re(s) \geq 1$, except for a simple pole at $s = 1$ when ρ is the trivial representation. (See [Hei67, p. 225].) For every place $p \in \mathcal{P}$, let $\mathbf{h}_{\chi,p}(s)$ be the Euler factor at p in the Euler product defining the L-function $L(\rho, s)$ (cf. [Neu13, Chap. VII, (10.1)]), so that $L(\rho, s) = \prod_{p \in \mathcal{P}} \mathbf{h}_{\chi,p}(s)$. By definition, the Euler factors $\mathbf{h}_{\chi,p}(s)$ are holomorphic and non-vanishing for $\Re(s) > 0$, and the product $\prod_{p \in \mathcal{P}} \mathbf{h}_{\chi,p}(s)$ is absolutely convergent when $\Re(s) > 1$. When $p \in \mathcal{P}$ is an unramified prime, the Euler factor is given by

$$\mathbf{h}_{\chi,p}(s) = \det\Big(I - \rho(\mathrm{Frob}(p))\|p\|^{-s}\Big)^{-1}.$$

Expanding the characteristic polynomial, we obtain the following estimate for $\Re(s) \geq \frac{1}{2}$:

$$\begin{aligned}\mathbf{h}_{\chi,p}(s) &= \Big(1 - \operatorname{tr}(\rho(\mathrm{Frob}(p)))\|p\|^{-s} + \mathcal{O}(\|p\|^{-2s})\Big)^{-1} \\ &= 1 + \operatorname{tr}(\rho(\mathrm{Frob}(p)))\|p\|^{-s} + \mathcal{O}(\|p\|^{-2s}) \\ &= 1 + \chi(\mathrm{Frob}(p))\|p\|^{-s} + \mathcal{O}(\|p\|^{-2s}).\end{aligned}$$

We now consider an arbitrary class function $\psi : G \to \mathbb{C}$. We define its *average* as its inner product with the trivial character:

$$\operatorname{avg}(\psi) := \frac{1}{|G|} \sum_{g \in G} \psi(g).$$

Recall that ψ decomposes as a sum over the finitely many irreducible characters χ of G:

$$\psi = \sum_{\chi} \langle \psi, \chi \rangle \chi.$$

We extend the definition of $\mathbf{h}_{\psi,p}$ to class functions ψ which are not irreducible characters, by setting

$$\mathbf{h}_{\psi,p} := \prod_{\chi} \mathbf{h}_{\chi,p}^{\langle \psi,\chi\rangle}$$

in which the power is interpreted as follows: for every irreducible character χ, the function $\mathbf{h}_{\chi,p}$ is holomorphic non-vanishing on the open simply connected subset $\{\Re(s) > 0\}$, and thus admits a logarithm $\log \mathbf{h}_{\chi,p}$; note that $\mathbf{h}_{\chi,p}(s) \underset{s\to\infty}{\longrightarrow} 1$ and choose the logarithm specifically so that $\log \mathbf{h}_{\chi,p}(s) \underset{s\to\infty}{\longrightarrow} 0$, which uniquely determines it; now set $\mathbf{h}_{\chi,p}^{\langle \psi,\chi\rangle} = \exp(\langle \psi,\chi\rangle \log \mathbf{h}_{\chi,p})$.

Lemma 2.29. *Let ψ be a class function $G \to \mathbb{C}$. Then:*

(i) $\mathbf{h}_{\psi,p}$ is holomorphic non-vanishing on the open half-plane $\{\Re(s) > 0\}$ for all places $p \in \mathcal{P}$.

(ii) For $\Re(s) \geq \frac{1}{2}$, and all unramified primes $p \in \mathcal{P}$,

$$\mathbf{h}_{\psi,p}(s) = 1 + \psi(\mathrm{Frob}(p))\|p\|^{-s} + \mathcal{O}_{\psi}\Big(\|p\|^{-2s}\Big)$$

where the implied constant in the $\mathcal{O}$-term is independent of both p and s.

(iii) The product $(s-1)^{\mathrm{avg}(\psi)} \prod_{p\in\mathcal{P}} \mathbf{h}_{\psi,p}(s)$, which is absolutely convergent for $\Re(s) > 1$, extends to a holomorphic non-vanishing function h_ψ on the closed half-plane $\{\Re(s) \geq 1\}$ with

$$h_\psi(1) = (\mathrm{Res}_{s=1}\zeta_Z(s))^{\mathrm{avg}(\psi)} \prod_{\chi\neq 1} L(\chi,1)^{\langle\psi,\chi\rangle}.$$

Proof. We have shown these properties for irreducible characters $\psi = \chi$ above. Now, consider an arbitrary class function $\psi = \sum_\chi \langle\psi,\chi\rangle\chi$. Point (i) follows immediately from the definition. For (ii), we compute

$$\begin{aligned}
\mathbf{h}_{\psi,p}(s) &= \prod_{\chi} \Big(1 + \chi(\mathrm{Frob}(p))\|p\|^{-s} + \mathcal{O}(\|p\|^{-2s})\Big)^{\langle\psi,\chi\rangle} \\
&= 1 + \sum_{\chi} \langle\psi,\chi\rangle\chi(\mathrm{Frob}(p))\|p\|^{-s} + \mathcal{O}(\|p\|^{-2s}) \\
&= 1 + \psi(\mathrm{Frob}(p))\|p\|^{-s} + \mathcal{O}(\|p\|^{-2s}).
\end{aligned}$$

For (iii), note that

$$(s-1)^{\mathrm{avg}(\psi)} \prod_{p\in\mathcal{P}} \mathbf{h}_{\psi,p}(s) = (s-1)^{\langle\psi,1\rangle} \prod_{p\in\mathcal{P}} \prod_{\chi} \mathbf{h}_{\chi,p}^{\langle\psi,\chi\rangle}(s) = h_1^{\langle\psi,1\rangle} \cdot \prod_{\chi\neq 1} h_\chi^{\langle\psi,\chi\rangle}.$$

Each of the finitely many factors extends to a holomorphic non-vanishing function on the closed half-plane $\{\Re(s) \geq 1\}$ as shown above. This establishes (iii) with $h_\psi = \prod_\chi h_\chi^{\langle\psi,\chi\rangle}$. □

Remark 2.30. A very similar result can be found in [FLN22, Proposition 2.3], with essentially the same proof. The main difference is that they use Euler factors of the form $1+\psi(\mathrm{Frob}(p))\|p\|^{-s}$, which (as they point out in their Remark 2.4) can vanish for small primes. They therefore need to exclude all primes p with $\|p\| \leq \max_{g\in G}|\psi(g)|$, which would be somewhat inconvenient for us. Moreover, our expression for $h_\psi(1)$ is a finite product, whereas the expression in [FLN22, Equation (2.5)] is an infinite product that is only conditionally convergent.

Application. Denote by $h_{\psi_{\tau,k}}$ the function associated as in Lemma 2.29 (iii) to the class function $\psi_{\tau,k}$ from Equation (2.6).

Lemma 2.31. *The function*

$$\widetilde{f}_{S,\tau,k}(s) := (s-1)^{\mathrm{avg}(\psi_{\tau,k})} \prod_{p\in\mathcal{P}\setminus S} \mathbf{f}_{\tau,k,p}\left(\frac{s}{a}\right) \tag{2.7}$$

extends to a non-vanishing holomorphic function on the closed half-plane $\{\Re(s)\geq 1\}$*, given by the expression*

$$\widetilde{f}_{S,\tau,k}(s) = h_{\psi_{\tau,k}}(s)\left(\prod_{p\in S}\mathbf{h}_{\psi_{\tau,k},p}(s)^{-1}\right)\left(\prod_{p\in\mathcal{P}\setminus S}\mathbf{f}_{\tau,k,p}\left(\frac{s}{a}\right)\mathbf{h}_{\psi_{\tau,k},p}(s)^{-1}\right), \tag{2.8}$$

in which the infinite product is absolutely convergent on the closed half-plane $\{\Re(s)\geq 1\}$*.*

Proof. For $\Re(s)>1$, the expression for $\widetilde{f}_{S,\tau,k}(s)$ in Equation (2.8) follows directly from unfolding the definition of $h_{\psi_{\tau,k}}$ (Lemma 2.29 (iii)). The first factor $h_{\psi_{\tau,k}}$ is holomorphic non-vanishing on the closed half-plane $\{\Re(s)\geq 1\}$ by Lemma 2.29 (iii). The second factor (the product over primes in S) is holomorphic non-vanishing on the open half-plane $\{\Re(s)>0\}$ as a finite product of such functions, cf. Lemma 2.29 (i). We now check that the third factor, which is an infinite product, is absolutely convergent on the closed half-plane $\{\Re(s)\geq 1\}$. To this end, we describe the asymptotic behavior of its factors as $\|p\|\to\infty$. By Lemma 2.27, we have:

$$\mathbf{f}_{\tau,k,p}(s) = 1+\psi_{\tau,k}(\mathrm{Frob}(p))\|p\|^{-as}+O(\|p\|^{-(1+\varepsilon)as}).$$

Any prime not in S is unramified, thus by Lemma 2.29 (ii), we have:

$$\mathbf{h}_{\psi_{\tau,k},p}(s) = 1+\psi_{\tau,k}(\mathrm{Frob}(p))\|p\|^{-s}+\mathcal{O}\Big(\|p\|^{-2s}\Big).$$

Therefore:

$$\mathbf{f}_{\tau,k,p}\left(\frac{s}{a}\right)\mathbf{h}_{\psi_{\tau,k},p}(s)^{-1} = 1+\mathcal{O}(\|p\|^{-\min(2,\,1+\varepsilon)s}).$$

Hence, the infinite product in Equation (2.8) is absolutely convergent on the open half-plane $\{\Re(s)>\frac{1}{\min(2,\,1+\varepsilon)}\}$. □

Remark 2.32. Lemma 2.31 can be interpreted as saying that $\prod_{p\in\mathcal{P}\setminus S}\mathbf{f}_{\tau,k,p}(s)$ has its rightmost "pole" at $s=a$, and that the "order" of this "pole" is the rational number $\mathrm{avg}(\psi_{\tau,k})$. However, a is often not an actual pole as the infinite product is not meromorphic on the closed half-plane when $\mathrm{avg}(\psi_{\tau,k})$ is not an integer.

Since u is prime, the number $g_k(u)$ is easy to compute:

$$g_k(u) = \sum_{\lambda'\in(\mathbb{Z}/u\mathbb{Z})^\times}\mathrm{e}\left(\frac{k\lambda'}{u}\right) = \left(\sum_{\lambda'\in\mathbb{Z}/u\mathbb{Z}}\mathrm{e}\left(\frac{k\lambda'}{u}\right)\right)-1 = \begin{cases} u-1 & \text{if } u|k \\ -1 & \text{otherwise.}\end{cases} \tag{2.9}$$

Lemma 2.33. *Let* $k\in\{0,\dots,M-1\}$*. For* $\tau=1$*, we have:*

$$\mathrm{avg}(\psi_{1,k}) = \begin{cases}(u-1)\beta & \text{if } u|k,\\ -\beta & \text{otherwise}\end{cases}$$

and, for any $\tau\mid M$*, we have* $\mathrm{avg}(\psi_{\tau,k})\leq(u-1)\beta$*.*

Proof. By Equation (2.6), we have

$$\mathrm{avg}(\psi_{\tau,k}) = \frac{1}{|G|}\sum_{g\in G}\psi_{\tau,k}(g) = \frac{g_k(u)}{|G|}\left|\left\{g\in G\,\middle|\,\mathrm{lcm}\left(\frac{dm}{\mathrm{cycgcd}\,g},\tau\right)\ \text{divides}\ \frac{M}{u}\right\}\right|.$$

The claims follow using Equation (2.9) and Equation (2.1). □

Application of Delange's Tauberian theorem. We have the following expression for the Dirichlet series $f_{S,\xi,\tau}$ counting elements of $\Lambda_{S,\xi,\tau}$ by discriminant:

$$\begin{aligned} f_{S,\xi,\tau}(s) &= \frac{d(\xi)^{-s}}{M}\sum_{k=0}^{M-1} \mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big) \prod_{p\in\mathcal{P}\setminus S} \mathbf{f}_{\tau,k,p}(s) && \text{by Equation (2.4)} \\ &= \frac{d(\xi)^{-s}}{M}\sum_{k=0}^{M-1} \mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big) \widetilde{f}_{S,\tau,k}(as)(as-1)^{-\operatorname{avg}(\psi_{\tau,k})} && \text{by Equation (2.7).} \end{aligned}$$

This already implies a weak form of Theorem 2.16 (i):

Corollary 2.34. *We have the asymptotic estimate:*

$$|\{\lambda\in\Lambda_{S,\xi,\tau} \mid d(\lambda)\le X\}| = C_{S,\xi,\tau}X^{1/a}\log(X)^{(u-1)\beta-1} + o\Big(X^{1/a}\log(X)^{(u-1)\beta-1}\Big)$$

where

$$C_{S,\xi,\tau} = \frac{1}{a^{(u-1)\beta-1}\cdot\Gamma((u-1)\beta)}\cdot\frac{d(\xi)^{-1/a}}{M}\sum_{\substack{0\le k\le M-1\\ \operatorname{avg}(\psi_{\tau,k})=(u-1)\beta}} \mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)\widetilde{f}_{S,\tau,k}(1). \tag{2.10}$$

Proof. We apply Delange's Tauberian theorem [Del54, Théorème III] as follows: Let

$$\alpha(t) := |\{\lambda\in\Lambda_{S,\xi,\tau} \mid d(\lambda)\le e^t\}|,$$

so that the function $f(s)$ in Delange's notation is

$$\begin{aligned} f(s) = \int_0^\infty e^{-st}\alpha(t)\mathrm{d}t \;&=\; s^{-1}\sum_{\lambda\in\Lambda_{S,\xi,\tau}} d(\lambda)^{-s} \;=\; s^{-1}f_{S,\xi,\tau}(s) \\ &= s^{-1}\frac{d(\xi)^{-s}}{M}\sum_{k=0}^{M-1} a^{-\operatorname{avg}(\psi_{\tau,k})}\mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)\widetilde{f}_{S,\tau,k}(as)\left(s-\frac{1}{a}\right)^{-\operatorname{avg}(\psi_{\tau,k})}. \end{aligned}$$

By Lemma 2.33, the largest value taken by $\operatorname{avg}(\psi_{\tau,k})$ is $(u-1)\beta$. Hence, in Delange's notation, $\omega=(u-1)\beta$, and the function $g(s)$ in front of the factor $(s-\frac{1}{a})^{-(u-1)\beta}$ is obtained by summing over values of k at which this maximal average is reached:

$$g(s) = s^{-1}a^{-(u-1)\beta}\frac{d(\xi)^{-s}}{M}\sum_{\substack{0\le k\le M-1\\ \operatorname{avg}(\psi_{\tau,k})=(u-1)\beta}} \mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)\widetilde{f}_{S,\tau,k}(as).$$

Then, Delange's theorem implies:

$$\begin{aligned} &|\{\lambda\in\Lambda_{S,\xi,\tau} \mid d(\lambda)\le X\}| \\ &= \alpha(\log X) \\ &= \left(\frac{g(\frac{1}{a})}{\Gamma((u-1)\beta)}+o(1)\right)X^{1/a}\log(X)^{(u-1)\beta-1} \\ &= \left(\frac{1}{a^{(u-1)\beta-1}\Gamma((u-1)\beta)}\cdot\frac{d(\xi)^{-1/a}}{M}\sum_{\substack{0\le k\le M-1\\ \operatorname{avg}(\psi_{\tau,k})=(u-1)\beta}} \mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)\widetilde{f}_{S,\tau,k}(1)+o(1)\right)X^{1/a}\log(X)^{(u-1)\beta-1}. \end{aligned}$$

(Technically, Delange only states the asymptotic equivalence $\alpha(\log X)\sim CX^{1/a}\log(X)^{(u-1)\beta-1}$, assuming that the resulting constant C is nonzero. However, one can check that the claim $\alpha(\log X) = (C+o(1))X^{1/a}\log(X)^{(u-1)\beta-1}$ follows in the same way, even when $C=0$. Alternatively, one can apply Delange's theorem to two functions $f_1(s)$ and $f_2(s)$ with $f(s)=f_1(s)-f_2(s)$ and such that $f_2(s)$ has a positive constant C_2, and then subtract the resulting asymptotic statements. There are many sources of such functions $f_1(s)$, $f_2(s)$: for example one can take $f_2(s) := \prod_{p\in\mathcal{P}\setminus S}\mathbf{f}_{1,0,p}(s)$.) □

The real number $C_{S,\xi,\tau}$ is nonnegative because of its combinatorial interpretation. However, at this point, we have not established that $C_{S,\xi,\tau}$ is nonzero: proving this fact (under the assumption that an extension indeed exists) is the focus of Subsection 2.6, and is the only piece of Theorem 2.16 (i) that is still missing.

Note that Equation (2.8) gives an expression for $\widetilde{f}_{S,\tau,k}(1)$ which can be used to compute $C_{S,\xi,\tau}$:

$$\widetilde{f}_{S,\tau,k}(1) = h_{\psi_{\tau,k}}(1) \left(\prod_{p \in S} \mathbf{h}_{\psi_{\tau,k},p}(1)^{-1} \right) \left(\prod_{p \in \mathcal{P} \setminus S} \mathbf{f}_{\tau,k,p}\left(\frac{1}{a}\right) \cdot \mathbf{h}_{\psi_{\tau,k},p}(1)^{-1} \right). \tag{2.11}$$

The value of $h_{\psi_{\tau,k}}(1)$ can itself be computed from the values (resp. residue for the trivial character) at $s = 1$ of the Artin L-functions associated to the irreducible characters of G, cf. Lemma 2.29 (iii).

Remark 2.35. An interesting special case arises when $\psi_{\tau,k} = \mathrm{avg}(\psi_{\tau,k}) \in \mathbb{C}$ is a constant class function (i.e., a multiple of the trivial character) — for example, if $F = Z$. In that case, we can use the expression for the residue $\mathrm{Res}_{s=1}\zeta_Z(s)$ of the Dedekind zeta function of Z at $s = 1$ given by the class number formula (for instance, it is 1 if $Z = \mathbb{Q}$) to get a more concrete expression for $\widetilde{f}_{S,\tau,k}(1)$ (and hence for the leading coefficient $C_{S,\xi,\tau}$):

$$\widetilde{f}_{S,\tau,k}(1) = \left((\mathrm{Res}_{s=1}\zeta_Z(s)) \cdot \prod_{p \in S} \left(1 - \frac{1}{\|p\|}\right) \right)^{\psi_{\tau,k}} \left(\prod_{p \in \mathcal{P} \setminus S} \mathbf{f}_{\tau,k,p}\left(\frac{1}{a}\right) \cdot \left(1 - \frac{1}{\|p\|}\right)^{\psi_{\tau,k}} \right).$$

2.6. Positivity of the leading coefficient

All notations are as in the previous subsection, and moreover we fix $\tau = 1$. We also assume that there exists an inner Galois extension L/K of degree n with $Z(L) = Z$ whose local invariants at places $v \in S$ are given by $\frac{\xi(v)}{M}$, and we denote by λ_0 the finitely supported map $\mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ corresponding to this extension. (We refer to Theorem 2.37 for criteria to check whether such an extension exists.) Our proof that the leading coefficient $C_{S,\xi,1}$ in Corollary 2.34 is nonzero relies on the following lemma:

Lemma 2.36. *If S' is a finite set of places containing S, and $\xi' : S' \to \mathbb{Z}/M\mathbb{Z}$ is a map extending ξ, then $C_{S',\xi',1} \leq C_{S,\xi,1}$. In particular, if $C_{S',\xi',1}$ is nonzero, then $C_{S,\xi,1}$ is nonzero.*

Proof. When we extend S and ξ, we are putting more constraints on the extensions we are counting and therefore there are fewer of them, i.e., $\Lambda_{S',\xi',1} \subseteq \Lambda_{S,\xi,1}$. This implies that:

$$\left|\{\lambda \in \Lambda_{S',\xi',1} \,|\, d(\lambda) \leq X\}\right| \leq \left|\{\lambda \in \Lambda_{S,\xi,1} \,|\, d(\lambda) \leq X\}\right|$$

and thus $C_{S',\xi',1} \leq C_{S,\xi,1}$ by Corollary 2.34. □

Instead of defining a new set S' and a map $\xi' : S' \to \mathbb{Z}/M\mathbb{Z}$, we use the notational shortcut of repeatedly adding places to S and extending ξ, until we can ensure that $C_{S,\xi,1}$ is positive. Recall from Equation (2.10) and Lemma 2.33 that:

$$C_{S,\xi,1} = \frac{1}{a^{(u-1)\beta-1} \cdot \Gamma((u-1)\beta)} \cdot \frac{d(\xi)^{-1/a}}{M} \sum_{\substack{0 \leq k \leq M-1 \\ u|k}} \mathrm{e}\left(\frac{k\sigma_\xi}{M}\right) \cdot \widetilde{f}_{S,1,k}(1).$$

Note also that, as soon as $u|k$, the class function $\psi_{1,k}$ defined in Equation (2.6) does not depend on k. For this reason, we simply let $\psi := \psi_{1,0}$. By Equation (2.8), we have for $u|k$:

$$\widetilde{f}_{S,1,k}(1) = h_\psi(1) \left(\prod_{p \in S} \mathbf{h}_{\psi,p}(1)^{-1} \right) \left(\prod_{p \in \mathcal{P} \setminus S} \mathbf{f}_{1,k,p}\left(\frac{1}{a}\right) \cdot \mathbf{h}_{\psi,p}(1)^{-1} \right).$$

Since the infinite product converges absolutely (Lemma 2.31), we have:

$$\prod_{\substack{p\in\mathcal{P}\setminus S\\ \|p\|>\kappa}} \left(\mathbf{f}_{1,k,p}\left(\frac{1}{a}\right)\cdot \mathbf{h}_{\psi,p}(1)^{-1}\right) \underset{\kappa\to\infty}{\longrightarrow} 1.$$

Fix any $\varepsilon\in(0,1)$, and choose κ such that, for all $0\le k\le M-1$ with $u\mid k$, we have:

$$\left|1-\prod_{\substack{p\in\mathcal{P}\setminus S\\ \|p\|>\kappa}} \mathbf{f}_{1,k,p}\left(\frac{1}{a}\right)\cdot \mathbf{h}_{\psi,p}(1)^{-1}\right|\le\varepsilon.$$

Add to S all the primes p with $\|p\|\le\kappa$ which are not already in S, extending ξ by setting $\xi(p)=\lambda_0(p)$. Now, define the nonzero number

$$c:=h_\psi(1)\left(\prod_{p\in S}\mathbf{h}_{\psi,p}(1)^{-1}\right)$$

so that, for some complex numbers $\widetilde{\varepsilon}_k$ of absolute value at most ε, we have $\widetilde{f}_{S,1,k}(1)=c\cdot(1+\widetilde{\varepsilon}_k)$ for all k divisible by u. We also let

$$c^+:=\frac{d(\xi)^{-1/a}\cdot c}{a^{(u-1)\beta-1}\cdot\Gamma\big((u-1)\beta\big)}$$

so that

$$C_{S,\xi,1}=\frac{c^+}{M}\sum_{\substack{0\le k<M\\ u\mid k}}\mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)(1+\widetilde{\varepsilon}_k).$$

Add to S the finitely many primes $p\in P\setminus S$ for which $\lambda_0(p)$ is nonzero, extending ξ by setting $\xi(p)=\lambda_0(p)$. Since λ_0 satisfies condition (IV) of Definition 2.23, we have $\sigma_\xi=\sum_{v\in S}\xi(v)=\sum_{v\in S}\lambda_0(v)=0$ in $\mathbb{Z}/M\mathbb{Z}$. Then,

$$\frac{c^+}{M}\sum_{\substack{0\le k<M\\ u\mid k}}\mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)=\frac{c^+}{M}\cdot\frac{M}{u}\cdot 1=\frac{c^+}{u}.$$

We now have:

$$\left|C_{S,\xi,1}-\frac{c^+}{u}\right|=\left|\frac{c^+}{M}\sum_{\substack{0\le k<M\\ u\mid k}}\mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)\widetilde{\varepsilon}_k\right|\le\frac{c^+}{M}\sum_{\substack{0\le k<M\\ u\mid k}}\left|\mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big)\widetilde{\varepsilon}_k\right|\le\frac{c^+}{M}\cdot\frac{M}{u}\cdot\varepsilon=\varepsilon\cdot\frac{c^+}{u}.$$

Since ε was chosen strictly smaller than 1, it follows that $C_{S,\xi,1}$ is nonzero. This concludes the proof of Theorem 2.16 (i).

2.7. Restriction to division algebras

All notations are as in Subsection 2.4. Recall that elements of $\Lambda_{S,\xi,\tau}$ correspond to extensions whose local invariants are all divisible by τ. Let $\Lambda'_{S,\xi}=\Lambda'\cap\Lambda_{S,\xi,1}$ be the set of maps corresponding to central simple Z-algebras of dimension M^2 in which K embeds, whose local invariants at places $v\in S$ are given by $\frac{\xi(S)}{M}$, and which are division algebras. Note that (cf. condition (V) in Definition 2.23):

$$\Lambda'_{S,\xi}=\Lambda_{S,\xi,1}\setminus\bigcup_{\substack{\tau\mid M\\ \tau>1}}\Lambda_{S,\xi,\tau}.$$

By the Möbius inversion formula, we get:

$$\left|\left\{\lambda \in \Lambda'_{S,\xi} \,\middle|\, d(\lambda) \leq X\right\}\right| = \sum_{\tau|M} \mu(\tau) \left|\{\lambda \in \Lambda_{S,\xi,\tau} \mid d(\lambda) \leq X\}\right|.$$

By Corollary 2.34, this implies:

$$\left|\left\{\lambda \in \Lambda'_{S,\xi} \,\middle|\, d(\lambda) \leq X\right\}\right| = C'_{S,\xi} X^{1/a} \log(X)^{(u-1)\beta-1} + o\Big(X^{1/a} \log(X)^{(u-1)\beta-1}\Big)$$

where

$$C'_{S,\xi} := \sum_{\tau|M} \mu(\tau) C_{S,\xi,\tau}.$$

All that is left is to show that $C'_{S,\xi}$ is positive when an extension exists. We assume that $\Lambda'_{S,\xi}$ is not empty, and we fix an element $\lambda_0 \in \Lambda'_{S,\xi}$ (see Theorem 2.37 to see what this hypothesis means in terms of S and ξ). Extend S by adding to it the finitely many primes p of Z not in S at which $\lambda_0(p)$ is nonzero, and set $\xi(p) = \lambda_0(p)$ at these primes. Since $\lambda_0 \in \Lambda'$, we now have $\gcd_{v \in S} \xi(v) = 1$. Therefore, all central simple algebras associated to maps agreeing with ξ on S are division algebras. This ensures that for all divisors τ of M besides 1, we have $C_{S,\xi,\tau} = 0$, and thus $C'_{S,\xi} = C_{S,\xi,1}$. Combined with Subsection 2.6, this implies the positivity of $C'_{S,\xi}$ (and this holds for the original "non-extended" S and ξ by a straightforward variant of Lemma 2.36).

We have now proved Theorem 2.16 (ii), completing the proof of Theorem 2.16.

2.8. Counting by product of ramified primes

We now explain how to adapt the proof of Theorem 2.16 in order to show Theorem 2.20. If L/K is an inner Galois extension of K with center Z corresponding to an element $\lambda \in \Lambda$, then the product $\mathrm{ram}(L)$ of the primes of Z ramified in L equals the following quantity $\mathrm{ram}(\lambda)$, computed in terms of the map λ alone:

$$\mathrm{ram}(\lambda) := \prod_{\substack{p \text{ prime of } Z \\ \lambda(p) \neq 0}} \|p\|.$$

Now, consider the Dirichlet series

$$f^*_{S,\xi,\tau}(s) := \sum_{\lambda \in \Lambda_{S,\xi,\tau}} \mathrm{ram}(\lambda)^{-s}.$$

As in Subsection 2.4, we rewrite the Dirichlet series as:

$$\begin{aligned} f^*_{S,\xi,\tau}(s) &= \mathrm{ram}(\xi)^{-s} \sum_{\text{(as in Eq. (2.2))}} \prod_{\substack{p \in \mathcal{P} \setminus S \\ \lambda(p) \neq 0}} \|p\|^{-s} \\ &= \frac{\mathrm{ram}(\xi)^{-s}}{M} \sum_{k=0}^{M-1} \mathrm{e}\Big(\frac{k\sigma_\xi}{M}\Big) \prod_{p \in \mathcal{P} \setminus S} \mathbf{f}^*_{\tau,k,p}(s), \end{aligned}$$

where we have defined:

$$\mathbf{f}^*_{\tau,k,p}(s) := 1 + \sum_{\substack{0 \neq \lambda \in \mathbb{Z}/M\mathbb{Z} \\ \eta_{\tau,p} | \lambda}} \mathrm{e}\Big(\frac{k\lambda}{M}\Big) \|p\|^{-s}.$$

The Euler factor $\mathbf{f}^*_{\tau,k,p}(s)$ also equals $1 + \psi^*_{\tau,k}(\mathrm{Frob}(p))\|p\|^{-s}$, where the class function $\psi^*_{\tau,k} : G \to \mathbb{Z}$ is defined as follows:

$$\psi^*_{\tau,k}(g) := \begin{cases} \gcd\Big(j \cdot \mathrm{cycgcd}(g),\, \frac{M}{\tau}\Big) - 1 & \text{if } \gcd\Big(j \cdot \mathrm{cycgcd}(g),\, \frac{M}{\tau}\Big) \text{ divides } k \\ -1 & \text{otherwise.} \end{cases}$$

The average of $\psi^*_{\tau,k}$ is largest for $\tau = 1$, $k = 0$, where it equals:

$$\operatorname{avg}\left(\psi^*_{1,0}(g)\right) = j\left(\frac{1}{|G|}\sum_{g\in G}\operatorname{cycgcd} g\right) - 1 = b^*.$$

The rest of the proof of Theorem 2.20 goes through exactly as in Subsections 2.5 to 2.7. In the argument, one uses the fact that $b^* > 0$ (shown in Remark 2.21) in order to see that $f_{S,\xi,\tau}(s)$ has a pole of positive order.

2.9. Criteria for existence of an extension

By Theorem 2.24, the existence of an inner Galois extension L/K of degree $n = dj^2$ with center $Z(L) = Z$ is equivalent to the existence of a map $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ in Λ, and the existence of such an extension which is a division algebra amounts to the existence of a map $\lambda \in \Lambda'$. The following lemma shows (when S is taken to be the empty set) that these conditions can be checked by considering only the finite set $\mathcal{P}^{\mathrm{ex}}$ of exceptional primes, and the finitely many maps $\mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$:

Theorem 2.37. *Let S be a finite set of places of Z and ξ be a map $S \to \mathbb{Z}/M\mathbb{Z}$ satisfying conditions (I)–(III) of Definition 2.23. The existence of an inner Galois extension L/K of degree $n = dj^2$ with center $Z(L) = Z$ and whose local invariants at places $v \in S$ are given by $\frac{\xi(v)}{M}$ is equivalent to the existence of a map $\lambda : \mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$ coinciding with ξ on $S \cap \mathcal{P}^{\mathrm{ex}}$, satisfying conditions (I)–(III) of Definition 2.23, and such that the following condition holds:*

(IV') $\frac{dm}{U} \mid \sum_{v\in\mathcal{P}^{\mathrm{ex}}} \lambda(v)$.

The existence of an extension as above which is also a division algebra is equivalent to the existence of a map $\lambda : \mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$ as above which moreover satisfies:

(V') $\gcd(\frac{dm}{U}, \gcd_{v\in\mathcal{P}^{\mathrm{ex}}} \lambda(v)) = 1$.

Proof.

($\Rightarrow$) We first assume that there is an inner Galois extension L/K as above. By Theorem 2.24, it corresponds to a map $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ in Λ, coinciding with ξ on S. Its restriction to $\mathcal{P}^{\mathrm{ex}}$ clearly still satisfies (I)–(III) at places $v \in \mathcal{P}^{\mathrm{ex}}$, and coincides with ξ on $S \cap \mathcal{P}^{\mathrm{ex}}$.

Let $v \in \mathcal{P} \setminus \mathcal{P}^{\mathrm{ex}}$. By the definition of U, $\frac{dm}{U} = \frac{dm}{\operatorname{lcm}_{g\in G} \operatorname{cycgcd} g}$ divides $\frac{dm}{\operatorname{cycgcd}(\mathrm{Frob}(v))}$, which in turn divides $\lambda(v)$ by Lemma 2.25. Hence, $\frac{dm}{U}$ divides $\sum_{p\in\mathcal{P}\setminus\mathcal{P}^{\mathrm{ex}}} \lambda(v)$.

By condition (IV) of Definition 2.23, we have $\sum_{v\in\mathcal{P}} \lambda(v) = 0$. It follows that $\frac{dm}{U} \mid \sum_{v\in\mathcal{P}^{\mathrm{ex}}} \lambda(v)$, so the restriction of λ to $\mathcal{P}^{\mathrm{ex}}$ satisfies (IV').

If L is a division algebra, then $\lambda \in \Lambda'$, so by condition (V) of Definition 2.23, we have $\gcd_{v\in\mathcal{P}} \lambda(v) = 1$. Since $\frac{dm}{U} \mid \lambda(v)$ for $v \in \mathcal{P} \setminus \mathcal{P}^{\mathrm{ex}}$, it follows that $\gcd(\frac{dm}{U}, \gcd_{v\in\mathcal{P}^{\mathrm{ex}}} \lambda(v)) = 1$, so the restriction of λ to $\mathcal{P}^{\mathrm{ex}}$ satisfies (V').

($\Leftarrow$) Conversely, assume that we have a map $\lambda\colon \mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$ as above, satisfying (I)–(III) and (IV') and coinciding with ξ on $S \cap \mathcal{P}^{\mathrm{ex}}$. We explain how to extend it to a map $\lambda\colon \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ satisfying (IV) and coinciding with ξ on S. First, by Chebotarëv's density theorem, the equality $\frac{dm}{U} = \gcd_{g\in G} \frac{dm}{\operatorname{cycgcd} g}$ implies

$$\frac{dm}{U} = \gcd_{p\notin S\cup\mathcal{P}^{\mathrm{ex}}} \frac{dm}{\operatorname{cycgcd}(\mathrm{Frob}(p))}. \tag{2.12}$$

By hypothesis, $\frac{dm}{U}$ divides $\sum_{v\in\mathcal{P}^{\mathrm{ex}}} \lambda(v)$. Moreover, $\frac{dm}{U}$ divides $\xi(v)$ for every $v \in S \setminus \mathcal{P}^{\mathrm{ex}}$ because ξ satisfies (III). Extend λ to a map $S \cup \mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$ by putting $\lambda(v) = \xi(v)$ if

$v \in S \setminus \mathcal{P}^{\mathrm{ex}}$. Then, $\frac{dm}{U}$ divides $\sum_{v \in S \cup \mathcal{P}^{\mathrm{ex}}} \lambda(v)$. By Equation (2.12) and Bézout's identity, there is a finite set S_1 of primes $p \notin S \cup \mathcal{P}^{\mathrm{ex}}$ and integers $\widetilde{\lambda}(p)$ for each $p \in S_1$, such that $\widetilde{\lambda}(p)$ is divisible by $\frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(p))}$ and such that

$$\sum_{v \in S \cup \mathcal{P}^{\mathrm{ex}}} \lambda(v) + \sum_{v \in S_1} \widetilde{\lambda}(v) = 0. \tag{2.13}$$

Extend λ to $\mathcal{P}$ by letting $\lambda(p) = \widetilde{\lambda}(p)$ if $p \in S_1$, and $\lambda(v) = 0$ for places $v \notin (S \cup \mathcal{P}^{\mathrm{ex}}) \sqcup S_1$. We have extended λ into a map $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ coinciding with ξ on S; by Lemma 2.25 and Equation (2.13), this map satisfies conditions (I)–(IV) and hence lies in Λ. This gives us an inner Galois extension L/K as needed.

Now assume also that the original map $\lambda : \mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$ satisfies (V'). It follows from Equation (2.12) that there is a finite set S_2 of places $p \notin S \cup \mathcal{P}^{\mathrm{ex}}$ such that $\frac{dm}{U} = \gcd_{p \in S_2} \frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(p))}$. Add these places to S and extend ξ by letting $\xi(p) = \frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(p))}$ if $p \in S_2$. Now, use the procedure from the previous paragraph to extend λ to a map $\mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ coinciding with ξ on S and satisfying (I)–(IV). Then $\gcd_{v \in \mathcal{P}} \lambda(v)$ divides $\gcd\big(\gcd_{v \in \mathcal{P}^{\mathrm{ex}}} \lambda(v), \gcd_{v \in S_2} \lambda(v)\big) = \gcd\big(\gcd_{v \in \mathcal{P}^{\mathrm{ex}}} \lambda(v), \frac{dm}{\mathrm{cycgcd}(\mathrm{Frob}(p))}\big) = \gcd\big(\gcd_{v \in \mathcal{P}^{\mathrm{ex}}} \lambda(v), \frac{dm}{U}\big)$, which is 1 by hypothesis (V'). This shows that the map $\lambda : \mathcal{P} \to \mathbb{Z}/M\mathbb{Z}$ satisfies (V). By Theorem 2.24, the corresponding extension L/K is therefore a division algebra as required. □

Remark 2.38. There are indeed situations where a map λ as in Theorem 2.37 does not exist, even when S is empty. For instance, assume that F/Z is a nontrivial Galois extension and that m does not divide j. Let v be a prime of Z completely split in F, so that condition (III) can be rewritten as "for all places $w|v$ of F, $\lambda(v) = dj\kappa_w \bmod dm$". It is then possible to construct the central simple F-algebra K of dimension m^2 so that the values of κ_w for different primes w above v force $\lambda(v)$ to take contradictory values modulo dm. For example, choose κ_w to be 0 for some place $w|v$, and 1 for some other place $w|v$. Then, $\lambda(v)$ must be congruent to both 0 and dj modulo dm, which is impossible as m does not divide j.

Note also the following corollary:

Corollary 2.39. *If there is an inner Galois extension of K of degree n with center Z which is a division algebra, then m and j are coprime.*

Proof. By Theorem 2.37, the hypothesis implies the existence of a map $\lambda : \mathcal{P}^{\mathrm{ex}} \to \mathbb{Z}/M\mathbb{Z}$ satisfying conditions (I)–(III) of Definition 2.23 as well as condition (V'). The integer $d\gcd(m, j)$ divides both dm and dj. Since λ satisfies condition (III) of Definition 2.23, this implies that $d\gcd(m, j)$ divides $d_w\lambda(v)$ for all places w of F lying above a place $v \in \mathcal{P}^{\mathrm{ex}}$. Summing over all places w above a fixed place $v \in \mathcal{P}^{\mathrm{ex}}$, we get $d\gcd(m, j) \mid d\lambda(v)$, i.e., $\gcd(m, j) \mid \lambda(v)$. This holds for all places $v \in \mathcal{P}^{\mathrm{ex}}$, and thus $\gcd(m, j)$ divides $\gcd_{v \in \mathcal{P}^{\mathrm{ex}}} \lambda(v)$. On the other hand, $\gcd(m, j) \mid m \mid \frac{dm}{U}$. Hence, $\gcd(m, j)$ divides $\gcd\Big(\frac{dm}{U}, \gcd_{v \in \mathcal{P}^{\mathrm{ex}}} \lambda(v)\Big)$, which equals 1 by condition (V'). We conclude that $\gcd(m, j) = 1$ as claimed. □

3. Outer extensions

In this section, we study the distribution of outer extensions L of a given (finite-dimensional) simple $\mathbb{Q}$-algebra K. We also discuss more specific questions, considering the case of outer Galois extensions with a given finite Galois group or restricting our attention to division algebras. In all cases, our main results relate these problems to questions concerning the distribution of ordinary commutative field extensions. Those questions are open in most cases.

In Subsection 3.1, we prove general facts concerning outer extensions, notably Theorem 3.3 which states that every outer extension of K is the tensor product of K with a field extension of its

center $Z(K)$. In Subsection 3.2, we give criteria for such a tensor product to be a division algebra and express $d(L/K)$ in terms of the relative discriminant of the field extension $Z(L)/Z(K)$. Finally, in Subsection 3.3, we use these descriptions to relate the problem of counting outer extensions of K with that of counting field extensions of $Z(K)$.

3.1. General facts about outer extensions

3.1.1. Groups of inner automorphisms are either trivial or infinite. We first prove Proposition 3.1 and Corollary 3.2, which imply that every extension whose automorphism group is finite is an outer extension, assuming that its center is infinite. For division algebras, this is well-known (see [Des18, Théorème]). Proposition 3.1 is also used in our proof of the characterization Theorem 3.3.

Proposition 3.1. *Let A be a finite-dimensional algebra over an infinite field F. If the group $A^\times/F^\times$ is finite, then $A = F$.*

Proof. Write $A^\times = a_1F^\times \sqcup \cdots \sqcup a_rF^\times$. Then, A is covered by the subsets $A \setminus A^\times$ and $a_1F, \dots, a_rF$. Each of these is an algebraic subset of the F-vector space A: The set $A\setminus A^\times$ is defined by the equation $\mathrm{Nm}_{A/F}(x) = 0$, which is polynomial in the coordinates of x, and the sets $a_1F, \dots, a_rF$ are linear subspaces. If $A \neq F$, then the F-vector space A is at least two-dimensional, so $A \setminus A^\times, a_1F, \dots, a_rF$ are properly contained in A. However, it is well-known that a finite-dimensional vector space over an infinite field cannot be covered by finitely many algebraic proper subsets. (See [Coh03, p. 228].) □

Corollary 3.2. *Let L/K be an extension of simple algebras. Assume that the inner automorphism group of L/K is finite and that the field $Z(L)$ is infinite. Then, L/K is an outer extension.*

Proof. By Proposition 3.1, the finiteness of $\mathrm{Inn}(L/K) \simeq \mathrm{Cent}_L(K)^\times/Z(L)^\times$ implies that $\mathrm{Cent}_L(K) = Z(L)$ and thus $\mathrm{Inn}(L/K) = 1$. Therefore, the extension L/K is outer. □

(The assumption that $Z(L)$ be infinite is crucial, as the example $L = \mathfrak{M}_d(\mathbb{F}_q)$, $K = \mathbb{F}_q$ shows.)

3.1.2. The Deschamps-Legrand descent theorem. We state and prove a generalized version of a theorem of Deschamps and Legrand [DL20, Corollaire 2], which is an "outer equivalent" of Corollary 2.7. The original result does not deal with the non-Galois case, and only treats the case of division algebras. This theorem gives a concrete description of extensions of K, allowing to parametrize them in terms of field extensions of $Z(K)$ (see Corollary 3.4).

Theorem 3.3. *Let L/K be an extension of simple $\mathbb{Q}$-algebras. The following are equivalent:*

(i) *L/K is outer.*

(ii) $\mathrm{Cent}_L(K) = Z(L)$.

(iii) *$Z(K)$ is contained in $Z(L)$, and L is generated by K and $Z(L)$.*

(iv) *$Z(K)$ is contained in $Z(L)$, and L is isomorphic to the tensor product $Z(L) \otimes_{Z(K)} K$ as an extension of K.*

(v) *$Z(K)$ is contained in $Z(L)$, and the restriction map $\mathrm{Aut}(L/K) \to \mathrm{Aut}(Z(L)/Z(K))$ is bijective.*

Proof.

(i) ⇒ (ii) Since L/K is outer, the group $\mathrm{Inn}(L/K) \simeq \mathrm{Cent}_L(K)^\times/Z(L)^\times$ is trivial and thus $\mathrm{Cent}_L(K)^\times = Z(L)^\times$. Now, Proposition 3.1 directly implies that $\mathrm{Cent}_L(K) = Z(L)$.

(ii) ⇒ (iii) We have $Z(K) = K \cap \mathrm{Cent}_L(K) \overset{\text{(ii)}}{=} K \cap Z(L)$, so $Z(K)$ is contained in $Z(L)$. Let L^Δ be the subalgebra of L generated jointly by $Z(L)$ and K. We have:

$$\begin{aligned}
L^\Delta &= \mathrm{Cent}_L\Big(\mathrm{Cent}_L(L^\Delta)\Big) && \text{by [Stacks, Theorem 074T (3)]}\\
&= \mathrm{Cent}_L\Big(\mathrm{Cent}_L(Z(L)) \cap \mathrm{Cent}_L(K)\Big) && \text{because } L^\Delta \text{ is generated by } Z(L) \text{ and } K\\
&= \mathrm{Cent}_L\Big(L \cap \mathrm{Cent}_L(K)\Big)\\
&= \mathrm{Cent}_L(Z(L)) && \text{by (ii)}\\
&= L.
\end{aligned}$$

Therefore, L is generated jointly by $Z(L)$ and K.

(iii) ⇒ (iv) By (iii), the algebras $Z(L)$ and K generate L, and thus the tensor product $Z(L) \otimes_{Z(K)} K$ surjects onto L via $x \otimes y \mapsto xy$. Since $L \neq 1$ and the algebra $Z(L) \otimes_{Z(K)} K$ is simple by [Stacks, Lemma 074F], this surjection is an isomorphism. Therefore, $L \simeq Z(L) \otimes_{Z(K)} K$ as claimed.

(iv) ⇒ (v) The restriction map is well-defined because automorphisms of L preserve the center. By functoriality of the tensor product, we obtain a map $\mathrm{Aut}(Z(L)/Z(K)) \to \mathrm{Aut}(Z(L) \otimes_{Z(K)} K/K) \overset{\text{(iv)}}{\simeq} \mathrm{Aut}(L/K)$. That map is an inverse of the restriction map, proving its bijectivity.

(v) ⇒ (i) By (v), automorphisms of L/K are determined by their restriction to $Z(L)$. However, inner automorphisms of L act trivially on $Z(L)$. Therefore, the extension L/K has no nontrivial inner automorphisms and thus is outer. □

We rephrase Theorem 3.3 to emphasize its importance for parametrizing outer extensions of K:

Corollary 3.4. *Let F be a number field and let K be a central simple F-algebra.*
There is a bijective correspondence:

$$\{\textit{outer extensions } L/K\}\,/\cong \quad \overset{\sim}{\longleftrightarrow} \quad \{\textit{field extensions } F'/F\}\,/\cong$$

given by:

$$\begin{aligned}
L &\mapsto Z(L)\\
F' \otimes_F K &\hookleftarrow F'
\end{aligned}$$

Moreover, via this correspondence:

$$\begin{aligned}
[L:K] &= [F':F]\\
\mathrm{Aut}(L/K) &\simeq \mathrm{Aut}(F'/F)\\
L/K \textit{ is Galois} &\Leftrightarrow F'/F \textit{ is Galois.}
\end{aligned}$$

Proof. Everything follows directly from Theorem 3.3 apart from the last equivalence. By Theorem 3.3 [(i) ⇒ (iv), (v)], we have:

$$L^{\mathrm{Aut}(L/K)} = (Z(L) \otimes_{Z(K)} K)^{\mathrm{Aut}(Z(L)/Z(K))}$$

where $\mathrm{Aut}(Z(L)/Z(K))$ only acts on the factor $Z(L)$, so that:

$$L^{\mathrm{Aut}(L/K)} = Z(L)^{\mathrm{Aut}(Z(L)/Z(K))} \otimes_{Z(K)} K. \tag{3.1}$$

Thus, $L^{\mathrm{Aut}(L/K)} = K$ is equivalent to $Z(L)^{\mathrm{Aut}(Z(L)/Z(K))} = Z(K)$. □

Remark 3.5. Corollary 3.4 implies a "noncommutative Hilbert theorem 90" as in [Des23, Proposition 26.2]. Indeed, consider an outer Galois extension L/K of simple algebras. Combining Corollary 3.4 with the result of [Ser62, Chap. X, §1, Exercise 2], we obtain:

$$H^1\Big(\mathrm{Gal}(L/K), L^\times\Big) = H^1\Big(\mathrm{Gal}(Z(L)/Z(K)), (K \otimes_{Z(K)} Z(L))^\times\Big) = 1.$$

3.2. Computing relative discriminants of outer extensions

Let F be a number field and K be a central division F-algebra of dimension m^2. If v is a place of F, let κ_v be the element of $\mathbb{Z}/m\mathbb{Z}$ such that the local invariant of K at v is given by $\frac{\kappa_v}{m}$. We denote by S the finite set of places v of F for which $\kappa_v \neq 0$.

In this section, we take a closer look at tensor products of K with field extensions F'/F, which by Corollary 3.4 are all the outer extensions of K. The main result is Theorem 3.6, which relates the "generalized relative discriminant" $d(L/K)$ when $L = K \otimes_F F'$ to the relative discriminant $d(F'/F)$, and characterizes situations where L is a division algebra.

Let $d \in \mathbb{N}$. We introduce the set $\mathcal{E}_d$ of tuples $(E(v))_{v\in S}$ where $E(v)$ is an étale F_v-algebra of dimension d for all $v \in S$. This set $\mathcal{E}_d$ is finite.[3] To each field extension F'/F of degree d corresponds a tuple $(F' \otimes_F F_v)_{v\in S} \in \mathcal{E}_d$. For $E \in \mathcal{E}_d$, we define:

$$\delta(E) := \prod_{\substack{p\in S \\ \text{prime of } F}} \|p\|^{\delta_p(E)} \tag{3.2}$$

where

$$\delta_p(E) := md(m - \gcd(m, \kappa_p)) - m \sum_{\substack{\text{field } E' \\ \text{factor of } E(p)}} f(E'/F_v)(m - \gcd(m, [E' : F_v]\kappa_p)). \tag{3.3}$$

We also define the following subset of $\mathcal{E}_d$:

$$\mathcal{E}'_d := \left\{ (E(v))_{v\in S} \in \mathcal{E}_d \;\middle|\; \text{the elements } \Big([E' : F_v]\kappa_v\Big)_{\substack{v\in S \\ E' \text{ factor of } E(v)}} \text{ generate } \mathbb{Z}/m\mathbb{Z} \right\}.$$

Theorem 3.6. *Let F'/F be a field extension of degree d and let L/K be an outer extension, associated to each other via the bijection of Corollary 3.4 (i.e., $F' = Z(L)$ and $L = F' \otimes_F K$). Let $E = (F' \otimes_F F_v)_{v\in S} \in \mathcal{E}_d$. Then:*

(i) The number $d(L/K)$ introduced in Definition 1.3 satisfies $d(L/K) = \delta(E)^{-1} \cdot d(F'/F)^{m^2}$;

(ii) L is a division algebra if and only if $E \in \mathcal{E}'_d$.

Proof. By [Rei03, (31.9)], the local invariant of L at a place w of F', lying above a place v of F, is given by:

$$\operatorname{inv}(L_w) = \operatorname{inv}((K \otimes_F F')_w) = [F'_w : F_v] \cdot \operatorname{inv}(K_v) = \frac{[F'_w : F_v]\kappa_v}{m}. \tag{3.4}$$

(i) Letting $f(q|p)$ denote the inertia degree of a prime q of F' lying above a prime p of F, we have

$$\begin{aligned} d(L/F') &= \prod_{p \text{ prime of } F} \prod_{q|p \text{ prime of } F'} \|q\|^{m\left(m - \gcd(m, [F'_q:F_p]\kappa_p)\right)} && \text{by Equations (1.2) and (3.4)} \\ &= \prod_{p \text{ prime of } F} \prod_{q|p \text{ prime of } F'} \|p\|^{mf(q|p)\left(m - \gcd(m, [F'_q:F_p]\kappa_p)\right)} \\ &= \prod_{\substack{p\in S \\ \text{prime of } F}} \|p\|^{m\sum_{q|p} f(q|p)\left(m - \gcd(m, [F'_q:F_p]\kappa_p)\right)} \end{aligned}$$

[3] Here, complications arise if the base field is a function field over a finite field instead of a number field, as its completions may have infinitely many extensions of a given degree and thus the naive analogue of $\mathcal{E}_d$ is not always finite. Then, when taking cardinalities in Equation (3.5), the sum on the right is not finite.

$$= \prod_{\substack{p\in S\\ \text{prime of } F}} \|p\|^{md\left(m-\gcd(m,\kappa_p)\right)-\delta_p(E)} \qquad \text{by Equation (3.3)}$$

$$= d(K/F)^d \cdot \delta(E)^{-1}. \qquad \text{by Equations (1.2) and (3.2)}$$

Finally, using Proposition 1.4:

$$d(L/K) = \frac{d(L/F') \cdot d(F'/F)^{m^2}}{d(K/F)^d} = \delta(E)^{-1} \cdot d(F'/F)^{m^2}.$$

(ii) By definition, L is a division algebra if and only if its index is m. Since index and exponent coincide for central simple algebras over number fields, this is equivalent to the condition that the invariants $\mathrm{inv}(L_w) = \frac{[F'_w:F_v]\kappa_v}{m}$ have least common denominator m, which amounts to the numerators $[F'_w : F_v]\kappa_v$ generating $\mathbb{Z}/m\mathbb{Z}$. The places $v \notin S$, with $\kappa_v = 0$, do not contribute. For $v \in S$, the fields F'_w with $w \mid v$ are exactly the factors E' of $E(v) = F' \otimes_F F_v$. Thus, L is a division algebra if and only if $E \in \mathcal{E}'_d$. □

Remark 3.7. The number $\delta(E)$ is the m-th power of an integer and divides $d(K/F)^d$. Indeed, for all primes $p \in S$, we have:

$$\begin{aligned}
\delta_p(E) &= m \sum_{\substack{\text{field } E'\\ \text{factor of } E(p)}} f(E'/F_v)\left[e(E'/F_v)(m-\gcd(m,\kappa_p)) - (m-\gcd(m,[E':F_v]\kappa_p))\right]\\
&\geq m \sum_{\substack{\text{field } E'\\ \text{factor of } E(p)}} f(E'/F_v)\left[e(E'/F_v)(m-\gcd(m,\kappa_p)) - (m-\gcd(m,\kappa_p))\right]\\
&= m \sum_{\substack{\text{field } E'\\ \text{factor of } E(p)}} f(E'/F_v)(e(E'/F_v)-1)(m-\gcd(m,\kappa_p))\\
&\geq 0
\end{aligned}$$

and thus $\delta(E)$ is an integer. Since the integers $\delta_p(E)$ are multiples of m, $\delta(E)$ is an m-th power. Finally, $\delta_p(E) \leq md(m-\gcd(m,\kappa_p))$ so $\delta(E)$ divides $d(K/F)^d$ (compare with Equation (1.2)).

Remark 3.8. Assume that K is a division algebra and that d is coprime to m. Then, $\mathcal{E}_d = \mathcal{E}'_d$ (i.e., $K \otimes_F F'$ is a division algebra for all field extensions F'/F of degree d). Indeed, consider an element $E \in \mathcal{E}_d$. For each place $v \in S$, $\gcd_{E' \text{ factor of } E(v)}[E' : F_v]$ divides $\sum_{E' \text{ factor of } E(v)}[E' : F_v] = [E(v) : F_v] = d$. Since d and m are coprime, this implies $\gcd_{v\in S}\gcd_{E' \text{ factor of } E(v)}[E' : F_v]\kappa_v = \gcd_{v\in S}\kappa_v$, which equals 1 because K is a division algebra unramified outside S. We have shown $E \in \mathcal{E}'_d$.

3.3. Counting outer extensions.

All notations are as in Subsection 3.2. By Theorem 3.6, the bijection of Corollary 3.4 restricts to a bijection:

$$\left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{outer extensions } L/K\\ \text{such that } d(L/K) \leq X\end{array}\right\} \xleftrightarrow{\sim} \bigsqcup_{E\in\mathcal{E}_d} \left\{\begin{array}{c}\text{isomorphism classes of}\\ \text{field extensions } F'/F\\ \text{such that } d(F'/F) \leq (\delta(E)X)^{1/m^2}\\ \text{and } F' \otimes_F F_v \simeq E(v) \text{ for all } v \in S\end{array}\right\}. \tag{3.5}$$

This bijection can be restricted to outer extensions which are division algebras by considering only tuples $E \in \mathcal{E}'_d$ on the right-hand side. We can therefore relate the counting function for outer extensions of K to a finite sum of counting functions for field extensions of F with fixed local behaviors above S.

For example, the results of [Woo10, Sections 2.4 and 2.5] on Malle's conjecture for abelian groups imply:

Corollary 3.9. *Let G be a finite abelian group. Let u be the smallest prime divisor of $|G|$ and let r be the number of elements of order u in G.*

(i) There is a real number $C > 0$ such that the number $N(X)$ of isomorphism classes of Galois extensions L/K with Galois group isomorphic to G (necessarily outer by Corollary 3.2) and $d(L/K) \leq X$ satisfies

$$N(X) \underset{X\to\infty}{\sim} CX^{1/a}(\log X)^{b-1}$$

where $a = m^2\,|G|\left(1-\frac{1}{u}\right)$ and $b = \frac{r}{[F(\zeta_u):F]}$.

(ii) Assuming that K is a division algebra, the same holds if we restrict to extensions L/K which are division algebras (with a possibly smaller constant C).

Similarly, [BSW15, Theorem 3] implies:

Corollary 3.10. *Let $n \in \{2,3,4,5\}$.*

(i) There is a real number $C > 0$ such that the number $N(X)$ of isomorphism classes of outer extensions L/K of degree n with $d(L/K) \leq X$ satisfies

$$N(X) \underset{X\to\infty}{\sim} CX^{1/m^2}.$$

(ii) Assuming that K is a division algebra, the same holds if we restrict to extensions L/K which are division algebras (with a possibly smaller constant C).

4. General extensions

In this section, we briefly discuss the possibility of combining the methods of Section 3 with the methods of Section 2 in order to parametrize or count general extensions which are neither inner nor outer. We focus exclusively on extensions L/K which are division algebras. The main result is Theorem 4.2, which explains how to uniquely decompose such an extension L/K into an outer extension $F' \otimes_F K/K$ and an inner Galois extension $L/F' \otimes_F K$. This decomposition can be used "backwards" to parametrize extensions L/K. Moreover, we relate the outer automorphism group of L/K and the Galois group of F'/F.

In the proof of Theorem 4.2, we make use of Lemma 4.1 below, which lets one extend automorphisms of a field into automorphisms of simple central algebras over that field. A proof is given in [Han06, Proposition 5.8], where the result is attributed to Deuring.

Lemma 4.1. *Let Z be a number field and let L be a central simple Z-algebra. Then, an automorphism $\sigma \in \mathrm{Aut}(Z)$ extends into an automorphism $\widetilde{\sigma} \in \mathrm{Aut}(L)$ if and only if $\mathrm{inv}(L_v) = \mathrm{inv}\left(L_{\sigma(v)}\right)$ for every place v of L. We say that an automorphism of Z* preserves *L if it satisfies that property.*

Finally, we state and prove Theorem 4.2:

Theorem 4.2. *Let K be a division $\mathbb{Q}$-algebra with center F.*

(i) We have a bijection between the set of isomorphism classes of extensions L/K that are division algebras and the set of equivalence classes of triples (F', Z, L), where:

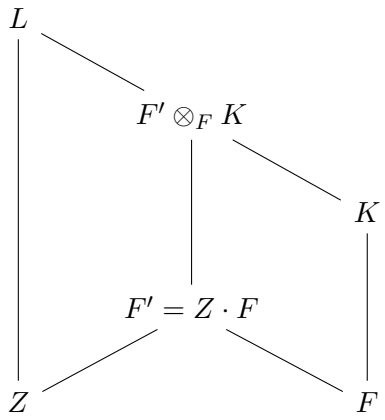
- *F'/F is a finite field extension,*
- *Z is a subfield of F' satisfying $F' = Z \cdot F$,*
- *L is an extension with center Z of the central simple F'-algebra $F' \otimes_F K$ such that L is a division algebra. (By Lemma 2.3, such an extension is inner Galois.)*

Here, two triples (F_1', Z_1, L_1) and (F_2', Z_2, L_2) are considered equivalent if there is an F-algebra isomorphism $f : F_1' \to F_2'$ with $f(Z_1) = Z_2$ and a ring isomorphism $g : L_1 \to L_2$ such that $g(x \otimes y) = f(x) \otimes y$ for all $x \in F_1'$ and $y \in K$.

Moreover, if an extension L/K corresponds to a triple (F', Z, L) via this bijection, then:

(ii) The outer automorphism group $\mathrm{Out}(L/K) := \mathrm{Aut}(L/K)/\mathrm{Inn}(L/K)$ of L/K is isomorphic to the group of automorphisms of F'/F sending Z to Z and whose restriction to Z preserves L.

(iii) The extension L/K is Galois if and only if the field extension F'/F is Galois and every automorphism of F'/F restricts to a well-defined automorphism of Z preserving L.



Proof. Any triple (F', Z, L) as above naturally gives rise to an extension L/K which is a division algebra, as L is an extension of $F' \otimes_F K$ and hence of K. Equivalent triples by definition give rise to isomorphic extensions of K.

Conversely, consider any extension L/K that is a division algebra. To construct the triple (F', Z, L), we first let $Z := Z(L)$, and we let $F' := Z \cdot F$ be the smallest subring of L containing Z and F. As a commutative finite-dimensional $\mathbb{Q}$-algebra without zero divisors, F' is a field. Since elements of F' commute with those of K, we have a Z-algebra homomorphism $F' \otimes_F K \to L$ sending $f \otimes k$ to fk, which is injective since $F' \otimes_F K$ is a simple ring by [Stacks, Lemma 074F]. Using this embedding, we can interpret L as an extension of $F' \otimes_F K$. This concludes the construction of (F', Z, L).

Consider any isomorphism $g : L_1 \to L_2$ between extensions of K which are division algebras. It restricts to an isomorphism $Z(L_1) \to Z(L_2)$ and fixes $F \subseteq K$. Hence, it restricts to an isomorphism $f : Z(L_1) \cdot F \to Z(L_2) \cdot F$ with $f(Z(L_1)) = Z(L_2)$. Moreover, $g(xy) = f(x)y$ for all $x \in Z(L_1) \cdot F$ and $y \in K$. This implies that isomorphic extensions give rise to equivalent tuples, completing the proof of (i). We leave it to the reader to verify that the maps are inverse to each other.

Let (F', Z, L) be a triple as above. Reasoning as in the previous paragraph, we see that we have a group homomorphism:

$$\varphi : \mathrm{Aut}(L/K) \longrightarrow \Big\{\sigma \in \mathrm{Aut}(F'/F) \,\Big|\, \sigma(Z) = Z\Big\}.$$

Any element of the kernel of φ is an automorphism of L/Z and hence an inner automorphism by the Skolem–Noether theorem. Conversely, any inner automorphism of L/K fixes all elements of $Z = Z(L)$ and of $F \subseteq K$ and hence fixes all elements of F'. Therefore, the group homomorphism φ has kernel $\mathrm{Inn}(L/K)$ and thus induces an injective homomorphism:

$$\widetilde{\varphi} : \mathrm{Out}(L/K) \hookrightarrow \Big\{\sigma \in \mathrm{Aut}(F'/F) \,\Big|\, \sigma(Z) = Z\Big\}.$$

Finally, Lemma 4.1 lets us describe the image of that map, proving (ii):

$$\mathrm{Out}(L/K) \simeq H := \left\{ \sigma \in \mathrm{Aut}(F'/F) \;\middle|\; \begin{array}{c} \sigma(Z) = Z \\ \sigma|_Z \text{ preserves } L \end{array} \right\}.$$

It remains to prove (iii). We have seen that the restrictions to F' of automorphisms of L/K are exactly the elements of $H \subseteq \mathrm{Aut}(F'/F)$. If F'/F is not a Galois extension or if H is a proper subgroup of $\mathrm{Aut}(F'/F)$, then $F'^H \supsetneq F$. But then $L^{\mathrm{Aut}(L/K)} \supseteq (F' \otimes_F K)^{\mathrm{Aut}(L/K)} = F'^H \otimes_F K \supsetneq K$, so L/K is not Galois.

Conversely, if F'/F is Galois extension and every automorphism of F'/F belongs to H, then $F'^H = F'^{\mathrm{Gal}(F'/F)} = F$. Hence, $(F' \otimes_F K)^{\mathrm{Aut}(L/K)} = F'^H \otimes_F K = F \otimes_F K = K$. According to Lemma 2.3, the extension $L/F' \otimes_F K$ is Galois, so in particular $L^{\mathrm{Aut}(L/K)} \subseteq L^{\mathrm{Aut}(L/F' \otimes_F K)} = F' \otimes_F K$. Together, we conclude that $L^{\mathrm{Aut}(L/K)} = K$, so L/K is Galois. □

Remark 4.3. Without the assumption that L is a division algebra, the compositum $F' = Z \cdot F$ might not be a field. For example, let $L = \mathfrak{M}_2(\mathbb{Q}(i))$ and let $K \subseteq L$ be the $\mathbb{Q}$-algebra generated by the rotation matrix $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, whose minimal polynomial is $X^2 + 1$. Note that K is a commutative algebra, abstractly isomorphic to $\mathbb{Q}[X]/(X^2+1) \simeq \mathbb{Q}(i)$. We have $Z = Z(L) = \mathbb{Q}(i)$ and $F = Z(K) = K$. The compositum $F' = Z \cdot F = \mathbb{Q}(i)[M]$ is then isomorphic to $\mathbb{Q}(i)[X]/(X^2 + 1) = \mathbb{Q}(i) \times \mathbb{Q}(i)$ which is not a field.

Remark 4.4. In the proof of Theorem 4.2, we constructed an embedding of $F' \otimes_F K$ into L. Since $F' = Z \cdot F$, the image A of this embedding is the compositum $Z \cdot K$. In particular, $Z \cdot K \cong F' \otimes_F K$ is a simple Z-algebra. By [Stacks, Theorem 074T], we have $Z \cdot K = \mathrm{Cent}_L(\mathrm{Cent}_L(Z \cdot K))$. Moreover, $\mathrm{Cent}_L(Z \cdot K) = \mathrm{Cent}_L(K)$. Thus, the image A can also be constructed as the double centralizer $\mathrm{Cent}_L(\mathrm{Cent}_L(K))$, and the field F' as the center of $A \simeq F' \otimes_F K$.

In principle, Theorem 4.2 suggests an approach for enumerating or counting extensions L/K: parametrize number fields F'/F (say, with fixed Galois group G), subfields Z of F', and then inner Galois extensions $L/F' \otimes_F K$. An enumeration of inner Galois extensions $L/F' \otimes_F K$ is obtained by adapting the methods of Section 2 to account for the condition that certain local invariants must coincide (see Lemma 4.1 and points (ii), (iii) of Theorem 4.2). The question of the enumeration of number fields F'/F is essentially Malle's conjecture [Mal02, Mal04]. However, even in situations where Malle's conjecture has a known answer (for example the case $G = \mathbb{Z}/2\mathbb{Z}$ where F'/F is a quadratic extension), one is left with nontrivial analytic problems (uniformity estimates in constant factors and error terms) that require future research.

References

[ALP20] Gil Alon, François Legrand, and Elad Paran. Galois groups over rational function fields over skew fields. *Comptes Rendus. Mathématique*. 358(7), pp. 785–790. 2020. DOI: 1010.5802/crmath.20.

[BDL22] Angelot Behajaina, Bruno Deschamps, and François Legrand. Problèmes de plongement finis sur les corps non commutatifs. *Israel Journal of Mathematics*. 249(2), pp. 617–650. 2022. DOI: 10.1007/s11856-022-2321-7.

[Beh21] Angelot Behajaina. Théorie inverse de Galois sur les corps des fractions rationnelles tordus. *Journal of Pure and Applied Algebra*. 225(4), pp. 106549. 2021. DOI: 10.1016/j.jpaa.2020.106549.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*. 162(2), pp. 1031–1063. 2005. DOI: 10.4007/annals.2005.162.1031. URL: http://www.jstor.org/stable/20159935.

[Bha10] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Annals of Mathematics*. 172(3), pp. 1559–1591. 2010. DOI: 10.4007/annals.2010.172.1559. URL: http://www.jstor.org/stable/29764652.

[BSW15] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Geometry-of-numbers methods over global fields i: Prehomogeneous vector spaces. 2015. URL: https://arxiv.org/abs/1512.03035. arXiv: 1512.03035.

[BSW22] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. An improvement on Schmidt's bound on the number of number fields of bounded discriminant and small degree. *Forum of Mathematics, Sigma*. 10, pp. e86. 2022. DOI: 10.1017/fms.2022.71.

[Car47] Henri Cartan. Théorie de Galois pour les corps non commutatifs. *Annales scientifiques de l'École Normale Supérieure*. 3^{e} série, 64, pp. 59–77. 1947. DOI: 10.24033/asens.942. URL: http://www.numdam.org/articles/10.24033/asens.942/.

[Coh54] Harvey Cohn. The density of abelian cubic fields. *Proceedings of the American Mathematical Society*. 5, pp. 476–477. 1954. DOI: 10.1090/S0002-9939-1954-0064076-8.

[Coh95] Paul Moritz Cohn. *Skew Fields: Theory of General Division Rings*. Encyclopedia of Mathematics and its Applications. Cambridge University Press. 1995. DOI: 10.1017/CBO9781139087193.

[Coh03] Paul Moritz Cohn. *Basic algebra*. Springer-Verlag London, Ltd., London. 2003. Groups, rings and fields. DOI: 10.1007/978-0-85729-428-9. ISBN: 1-85233-587-4.

[Cou20] Jean-Marc Couveignes. Enumerating number fields. *Annals of Mathematics*. 192(2), pp. 487–497. 2020. DOI: 10.4007/annals.2020.192.2.4.

[Del54] Hubert Delange. Généralisation du théorème de Ikehara. *Annales scientifiques de l'École Normale Supérieure*. 71(3), pp. 213–242. 1954. DOI: 10.24033/asens.1023.

[Des18] Bruno Deschamps. Des extensions plus petites que leurs groupes de Galois. *Communications in Algebra*. 46(10), pp. 4555–4560. 2018. DOI: 10.1080/00927872.2018.1448844.

[Des21] Bruno Deschamps. La méthode Behajaina appliquée aux corps de fractions tordus par une dérivation. *Research in Number Theory*. 7(39), pp. 106549. 2021. DOI: 10.1007/s40993-021-00263-z.

[Des23] Bruno Deschamps. Arithmétique des extensions intérieures. *Journal of Algebra*. 620, pp. 50–88. 2023. DOI: 10.1016/j.jalgebra.2022.12.020.

[DesInd] Bruno Deschamps. Indices dans $\mathrm{Br}(\mathbb{R}(\!(x)\!)(\!(y)\!))$. URL: http://perso.univ-lemans.fr/~bdesch/Brauerdeg.pdf.

[DH71] Harold Davenport and Hans Heilbronn. On the Density of Discriminants of Cubic Fields. II. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*. 322(1551), pp. 405–420. 1971. DOI: 10.1098/rspa.1971.0075. URL: http://www.jstor.org/stable/77760.

[DL20] Bruno Deschamps and François Legrand. Le Problème Inverse de Galois sur les corps des fractions tordus à indéterminée centrale. *Journal of Pure and Applied Algebra*. 224(5), pp. 106–240. 2020. DOI: 10.1016/j.jpaa.2019.106240.

[ESZB23] Jordan S. Ellenberg, Matthew Satriano, and David Zureick-Brown. Heights on stacks and a generalized Batyrev–Manin–Malle conjecture. *Forum of Mathematics, Sigma*. 11, pp. e14. 2023. DOI: 10.1017/fms.2023.5.

[ETW23] Jordan S. Ellenberg, TriThang Tran, and Craig Westerland. Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields. 2023. arXiv: 1701.04541.

[EV06] Jordan S. Ellenberg and Akshay Venkatesh. The Number of Extensions of a Number Field with Fixed Degree and Bounded Discriminant. *Annals of Mathematics*. 163(2), pp. 723–741. 2006. DOI: 10.4007/annals.2006.163.723. URL: http://www.jstor.org/stable/20159972.

[FKS81] Burton Fein, William M. Kantor, and Murray Schacher. Relative Brauer groups II. *Journal für die reine und angewandte Mathematik*. 328, pp. 39–57. 1981. DOI: 10.1515/crll.1981.328.39. URL: https://pages.uoregon.edu/kantor/PAPERS/BrauerGroups.pdf.

[FLN22] Christopher Frei, Daniel Loughran, and Rachel Newton. Number fields with prescribed norms. *Commentarii Mathematici Helvetici. A Journal of the Swiss Mathematical Society*. 97(1), pp. 133–181. 2022. With an appendix by Yonatan Harpaz and Olivier Wittenberg. DOI: 10.4171/cmh/528.

[Han06] Timo Hanke. Computation of outer automorphisms of central-simple algebras. In Jan Draisma and Hanspeter Kraft, editors, *Proceedings of the Rhine Workshop on Computer Algebra*. 2006. URL: http://www.math.rwth-aachen.de/~Timo.Hanke/thanke_outer-automorphisms.pdf.

[Hei67] Hans Heilbronn. Zeta-Functions and L-Functions. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*. pages 204–230. Academic Press. 1967. ISBN: 978-0-9502-7342-6.

[HHK11] David Harbater, Julia Hartmann, and Daniel Krashen. Patching subfields of division algebras. *Transactions of the American Mathematical Society*. 363(6), pp. 3335–3349. 2011. DOI: 10.1090/S0002-9947-2010-05229-8.

[Jac40] Nathan Jacobson. The Fundamental Theorem of the Galois Theory for Quasi-Fields. *Annals of Mathematics*. Second Series, Vol. 41(1), pp. 1–7. 1940. DOI: 10.2307/1968817.

[Jac47] Nathan Jacobson. A Note on Division Rings. *American Journal of Mathematics*. 69(1), pp. 27–36. 1947. DOI: 10.2307/2371651.

[Jac56] Nathan Jacobson. *Structure of Rings*. volume 37 of *Colloquium Publications*. American Mathematical Society. 1956. DOI: 10.1090/coll/037. ISBN: 978-0-8218-1037-8.

[Klü22] Jürgen Klüners. The asymptotics of nilpotent Galois groups. *Acta Arithmetica*. 204, pp. 165–184. 2022. DOI: 10.4064/aa211207-16-5.

[KP23] Peter Koymans and Carlo Pagano. On Malle's conjecture for nilpotent groups. *Trans. Amer. Math. Soc. Ser. B*. 10, pp. 310–354. 2023. DOI: 10.1090/btran/140.

[Leg22a] François Legrand. On a variant of the Beckmann–Black problem. *Proceedings of the American Mathematical Society*. 150, pp. 3267–3281. 2022. DOI: 10.1090/proc/15909.

[Leg22b] François Legrand. On finite embedding problems with abelian kernels. *Journal of Algebra*. 595, pp. 633–659. 2022. DOI: 10.1016/j.jalgebra.2021.12.026.

[Leg24] François Legrand. On Galois extensions of division rings of Laurent series. *Journal of Pure and Applied Algebra*. 228(2), pp. 107466. 2024. DOI: 10.1016/j.jpaa.2023.107466.

[LMPT18] Benjamin Linowitz, David Ben McReynolds, Paul Pollack, and Lola Thompson. Counting and effective rigidity in algebra and geometry. *Inventiones mathematicae*. 213, pp. 697–758. 2018. DOI: 10.1007/s00222-018-0796-y.

[LT22] Robert J. Lemke Oliver and Frank Thorne. Upper bounds on number fields of given degree and bounded discriminant. *Duke Mathematical Journal*. 171(15), pp. 3077 – 3087. 2022. DOI: 10.1215/00127094-2022-0046.

[Mäk85] Sirpa Mäki. *On the Density of Abelian Number Fields*. PhD thesis. Turun yliopisto. 1985. ISBN: 978-951-41-0507-4.

[Mal02] Gunter Malle. On the Distribution of Galois Groups. *Journal of Number Theory*. 92(2), pp. 315–329. 2002. DOI: 10.1006/jnth.2001.2713.

[Mal04] Gunter Malle. On the Distribution of Galois Groups. II. *Experimental Mathematics*. 13(2), pp. 129–135. 2004. DOI: 10.1080/10586458.2004.10504527. URL: http://eudml.org/doc/52777.

[Mot23] François Motte. Hilbert irreducibility, the Malle conjecture and the Grunwald problem. *Annales de l'Institut Fourier*. 73(5), pp. 2099–2134. 2023. DOI: 10.5802/aif.3567.

[Neu13] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg. 2013. DOI: 10.1007/978-3-662-03983-0.

[Rei03] Irving Reiner. *Maximal Orders*. London Mathematical Society Monographs. Oxford University Press. 2003. DOI: 10.1093/oso/9780198526735.001.0001. ISBN: 978-0-1985-2673-5.

[Sch68] Murray M. Schacher. Subfields of division rings, I. *Journal of Algebra*. 9, pp. 451–477. 1968. DOI: 10.1016/0021-8693(68)90015-X.

[Sch95] Wolfgang M. Schmidt. Number fields of given degree and bounded discriminant. In *Columbia university number theory seminar - New York, 1992*. number 228 in Astérisque. pages 189–195. Société mathématique de France, Paris. 1995. URL: http://www.numdam.org/item/AST_1995___228___189_0/.

[Ser62] Jean-Pierre Serre. *Corps Locaux*. Hermann, Paris. 1962. ISBN: 978-2-7056-1296-2.

[Stacks] The Stacks project authors. The Stacks project. URL: https://stacks.math.columbia.edu.

[Wan21] Jiuya Wang. Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$. *Compos. Math.*. 157(1), pp. 83–121. 2021. DOI: 10.1112/s0010437x20007587.

[Woo10] Melanie Matchett Wood. On the probabilities of local behaviors in abelian field extensions. *Compositio Mathematica*. 146(1), pp. 102–128. 2010. DOI: 10.1112/S0010437X0900431X.

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. *Proceedings of the London Mathematical Society*. s3-58(1), pp. 17–50. 1989. DOI: 10.1112/plms/s3-58.1.17.