Low-degree extensions of number fields and local fields

by

Sebastian Monnet

This thesis is submitted for the degree of
Doctor of Philosophy

to the

Department of Mathematics
University College London (UCL)

February 2025

Contents

Declaration

I, Sebastian Monnet, confirm that the work presented in my thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

We present new results in arithmetic statistics, particularly in the statistics of number fields and p-adic fields. For $n \leq 5$, and conjecturally for $n \geq 6$, the asymptotic counting of so-called "S_n-n-ic" extensions of number fields amounts to computing the "masses" of certain sets of étale extensions. This notion of mass was studied by Serre in his famous "Serre's mass formula", and subsequently by Bhargava and others. By counting various families of étale extensions of p-adic fields, we obtain novel refinements of Serre's formula and apply them to prove results about counting S_n-n-ic extensions of number fields with certain prescribed norm elements. Our results are divided into two categories: a "pure" study of masses for wildly ramified extensions of 2-adic fields, and a more "applied" study of S_n-n-ic extensions, where we use our techniques to deduce results about counting number fields.

The upshot of our pure study of masses is as follows. Given a 2-adic field F, a finite group G, and a positive integer m, we obtain a formula for the number of isomorphism classes of totally ramified quartic field extensions L/F with Galois closure group G and discriminant valuation m. As a corollary, we then use these counts to deduce our refinements of Serre's mass formula.

As for the applied study of S_n-n-ic extensions, let k be a number field and let $\mathcal{A} \subseteq k^\times$ be a finitely generated subgroup. For a positive integer n and a real number X, let $N_{k,n}(X; \mathcal{A})$ be the number of S_n-n-ic extensions K/k with $\mathcal{A} \subseteq N_{K/k}K^\times$ and $\mathrm{Nm}(\mathrm{disc}(K/k)) \leq X$. For $n \leq 5$, and conjecturally for $n \geq 6$, we express the limit

$$\lim_{X \to \infty} \frac{N_{k,n}(X; \mathcal{A})}{X}$$

as an Euler product, whose term at each prime $\mathfrak{p}$ of k is the mass of a certain set of étale algebras over the completion $k_\mathfrak{p}$. Using, among other things, the techniques from our pure study of masses, we evaluate almost all of these local factors explicitly and give an efficient algorithm for computing the rest.

Impact statement

This thesis is largely concerned with mass computations involving p-adic fields. Such computations appear often when studying the statistics of number fields. Indeed, we use our mass formulae to prove results about the distribution of so-called "S_n-n-ic" extensions with prescribed norm elements. Outside our own work, methods in this thesis have already found application in upcoming work of Newton–Varma, in which the authors count certain families of S_4-quartic extensions. More generally, we expect our methods and results to be useful for a variety of counting problems involving S_n-n-ics, especially in the quartic case.

Acknowledgements

Of course, everybody thanks their supervisor in their thesis, but I would like to emphasise that Rachel Newton has really been a phenomenal supervisor, and my gratitude extends far beyond the obligatory acknowledgement. She takes her role extremely seriously, and has worked much harder than was required by the job. Aside from the obvious - that this mathematical work would not have been possible without her guidance - I am grateful that I had a supervisor who really cared about the wellbeing of her students as people, and not just about their research output.

During the PhD, I have had many helpful conversations with many people! I can't possibly hope to list all of their names here, but I will mention a few. I particularly remember a series of conversations in which Ross Paterson and Tim Santens made some crucial suggestions that helped me put a key puzzle piece into place. I'm also very much indebted to Jiuya Wang for making me aware of the result [BSW15, Theorem 3], which became a major workhorse in my thesis. Brandon Alberts helped me understand some of the context for my work, telling me about the Malle–Bhargava heuristics, and Jordan Ellenberg helped me appreciate the beauty of Serre's mass formula. More recently, Christopher Keyes and Lazar Radicevic have both been very generous, helping me work out quite a few details during the preparation of this thesis.

Aside from the mathematical conversations (of which there have been many besides those listed), I am grateful for the friends I have made at conferences and within my own university. Not only is it intrinsically good that people are friendly, constructive, and kind, but feeling part of the community has motivated me tremendously and been a great aide to my research. I am especially grateful to Ross Paterson, who has been very supportive and encouraged my research throughout the PhD. I really appreciate Ross's mentorship and how generous he has been with his time. To list just a few others, I am thankful to Lee Berry, Christopher Keyes, Giorgio Navone, Dan Loughran, Jesse Pajwani, Lazar Radicevic, Tim Santens, Harmeet Singh, and Happy Uppal for being all-round nice people and making me feel at home in academia.

Important credit goes to my parents for all their hard work raising me, especially for teaching me to try to understand things, which was hugely important in my journey to become a mathematician. Thanks also to my brother, Dominic, and my girlfriend, Nera, for being my best friends. I am very grateful to them both for being in my life, and for reminding me that sometimes it's also fun to do things that aren't maths.

Finally, thank you to both examiners, Vladimir Dokchitser and Adam Morgan, for reading the whole thesis very carefully and making some excellent suggestions to improve it!

UCL Research Paper Declaration Form

First paper:

(1) **For a research manuscript that has already been published.**
  (a) **What is the title of the manuscript?** Counting wild quartics with prescribed discriminant and Galois closure group.
  (b) **Please include a link to or doi for the work:** `https://doi.org/10.1016/j.jnt.2024.10.008`.
  (c) **Where was the work published?** Journal of Number Theory.
  (d) **Who published the work?** Elsevier.
  (e) **When was the work published?** November 2024.
  (f) **List hte manuscript's authors in the order they appear on the publication:** Sebastian Monnet.
  (g) **Was the work peer-reviewed?** Yes.
  (h) **Have you retained the copyright?** Yes.
  (i) **Was an earlier form of the manuscript uploaded to a preprint server? If 'Yes', please give a link or doi.** Yes: `https://doi.org/10.48550/arXiv.2304.03154`

(2) **In which chapters of your thesis can this material be found?** Part 3.

Second paper:

(1) **For a research manuscript prepared for publication that has not yet been published.**
  (a) **What is the current title of the manuscript?** S_n-extensions with prescribed norms.
  (b) **Has the manuscript been uploaded to a preprint server? If 'Yes', please give a link or doi.** Yes: `https://doi.org/10.48550/arXiv.2405.02740`.
  (c) **Where is the work intended to be published?** A pure mathematics journal.
  (d) **List the manuscript's authors in the order they appear on the publication:** Sebastian Monnet.
  (e) **Stage of publication:** Submitted.

(2) **In which chapters of your thesis can this material be found?** Part 4.

Part 1. Introduction

This thesis has two aims. The first is to introduce the uninitiated to the highly active field of arithmetic statistics, and more specifically to the subdiscipline of field counting. The second is to present original research in these areas.

Excluding this introduction, the thesis is divided into three parts: Part 2, Part 3, and Part 4.

The first of these, Part 2, contains background. It introduces the reader to arithmetic statistics in general, before specialising to the statistics of number fields by introducing the Malle–Bhargava heuristics and sketching their proof in low degree. Before stating the Malle–Bhargava heuristics, we establish the notion of “mass” of étale algebras. We explore some well-known properties of this mass, including the famous “Serre’s mass formula” and Bhargava’s generalisations thereof. We then state the Malle–Bhargava heuristics, and the major conjectures that they motivate. Some of these conjectures have been proved for low-degree number fields, and the final section of Part 2 is devoted to the key ideas in their proof.

The aim of Part 3 is to present several refinements of Serre’s mass formula in the case of wildly ramified quartic extensions of p-adic fields. For a rational prime p, let F be a finite extension of the p-adic numbers $\mathbb{Q}_p$, and let S be a set of degree n field extensions of F. The *pre-mass*[1] of S is defined to be

$$\widetilde{m}(S) = \sum_{L \in S} \frac{1}{\# \operatorname{Aut}(L/F)} \cdot q^{-v_F(d_{L/F})},$$

where $d_{L/F}$ is the discriminant of the extension, q is the size $\#\mathbb{F}_F$ of the residue field, and $\operatorname{Aut}(L/F)$ is the set of F-algebra automorphisms of L. Then Serre’s mass formula states that

$$\widetilde{m}\big(\{\text{all totally ramified degree } n \text{ extensions } L/F\}\big) = \frac{1}{q^{n-1}}.$$

When $p \nmid n$, so that all ramification is tame, it is easy to classify such extensions and thus prove the result. On the other hand, when $p \mid n$, there is no straightforward classification of degree n extensions of F. Even with modern algorithms, computing all such extensions becomes prohibitively expensive for all but the smallest values of n and $[F : \mathbb{Q}_p]$. The remarkable thing about Serre’s result is that the same formula holds in the wild case as the tame. This is really amazing; when $p \nmid n$, the mass is distributed among a few, well-behaved pieces. On the other hand, when $p \mid n$, there are very many tiny, messy fragments, and yet somehow they still fit together into the same simple shape.

Serre’s formula states the mass of all totally ramified field extensions of a given degree. One might naturally ask similar questions about the masses of other sets of extensions. For example, Dalawat [Dal10, Propositions 15-16] finds the mass of ramified *cyclic* extensions of *prime* degree. Thus, in the case of prime degree, Dalawat proves a *refinement* of Serre’s formula. In general, proving generalised and refined mass formulae is a popular pastime in the arithmetic statistics community. Of particular relevance to our work, Bhargava generalises Serre’s formula in [Bha07, Propositions 2.1-2.2], to compute the mass of certain sets of *étale algebras*, rather than fields (we state his results concisely in Theorem 3.9). There is also much interest (for example [Ked07] and [WY15]) in the masses of Galois representations, which are closely related to étale algebras, as we will see in Section 3.2. Let F be a 2-adic field, so that totally ramified quartic extensions of F are wildly ramified. The main result of Part 3 is to find the mass of all totally ramified

[1] This is the quantity Serre refers to as mass. We call it pre-mass because “mass” will refer to a closely related but slightly different quantity.

quartic extensions with each possible *Galois closure group*. Our formulae are stated fully in Section 5.

In fact, our results are somewhat stronger than just stating masses. Rather, we compute the *number* of totally ramified quartic field extensions L/F with each possible discriminant *and* Galois closure group, from which it is easy to deduce the masses. In order to do this, we use a variety of techniques, depending on the Galois closure group. For Galois closure groups S_4 and A_4, we adapt Serre's original proof of his mass formula. Serre's work allows us to reduce our problem to the study of certain sets of Eisenstein polynomials. We establish congruence conditions for these sets and use them to count the corresponding fields. The case V_4 is already available in the literature. Cyclic extensions are the most difficult to deal with, and we devote significant effort to them. We adapt techniques of [CDO05], decomposing C_4-extensions as towers of quadratics, and counting the top and bottom halves separately. Finally, we count D_4-extensions by characterising them as the towers of quadratics that are neither C_4 nor V_4. This allows us to relate their quantity to those we have already computed, and hence state it explicitly.

In Part 4, we count so-called "S_n-n-ic[1] extensions" with prescribed norms. Our choice of problem is inspired by [FLN22], at the suggestion of our supervisor, Rachel Newton. In [FLN22], given a number field k, a finite abelian group G, and a finitely generated subgroup $\mathcal{A} \subseteq k^\times$, the authors count Galois extensions K/k with

$$\mathrm{Gal}(K/k) \cong G \quad \text{and} \quad \mathcal{A} \subseteq N_{K/k}K^\times.$$

We consider the same problem for degree n extensions K/k with Galois closure group S_n (these are the aforementioned S_n-n-ic extensions). These are in some sense the furthest extensions from being abelian, so that our work and [FLN22] constitute two extremes of a spectrum. Frei, Loughran, and Newton prove their results by parametrising their extensions using class field theory. Since our extensions are not abelian, these methods are inaccessible to us. Instead, we use the famous *Malle–Bhargava heuristics*, which give a conjectural framework for understanding the distribution of S_n-n-ic extensions. Write $N_{k,n}(X;\mathcal{A})$ for the number of S_n-n-ic extensions K/k with $\mathrm{Nm}(\mathrm{disc}(K/k)) \leq X$ and $\mathcal{A} \subseteq N_{K/k}K^\times$. Also write $N_{k,n}(X)$ as shorthand for $N_{k,n}(X;\{1\})$, which counts S_n-n-ics without any constraints on the norm group. Contingent on the Malle–Bhargava heuristics, we show that

$$\lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{X} = \frac{1}{2} \cdot \mathrm{Res}_{s=1}\left(\zeta_k(s)\right) \cdot \prod_{\mathfrak{p}\in\Pi_k} m_{\mathcal{A},\mathfrak{p}},$$

where the product is over prime ideals of k, both finite and infinite, and the quantities $m_{\mathcal{A},\mathfrak{p}}$ are certain local factors (depending implicitly on n) called "masses". The eagle-eyed reader might notice that this is not the first time we have used the word "mass". Indeed, the masses $m_{\mathcal{A},\mathfrak{p}}$ are none other than the masses of certain sets of étale algebras, in the sense of Serre's and Bhargava's mass formulae. Thus, once again, we are essentially proving generalisations and refinements of Serre's mass formula. The flavour is different in this case, though; in Part 3, our study is "pure", in the sense that we ask questions primarily because they are natural and interesting in their own right. On the other hand, Part 4 is more applied, because we are using mass as a means to the end of counting number fields.

[1] Despite some aesthetic misgivings about the term "S_n-n-ic", we find it to be concise and unambiguous, so we have opted to use it.

For general n, contingent on the Malle–Bhargava heuristics, we prove some qualitative results about the proportion

$$\lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{N_{k,n}(X)}$$

of S_n-n-ics with $\mathcal{A}$ in their norm group. In particular, we show that (assuming the Malle–Bhargava heuristics hold) this proportion is always positive, but can only be 100% in certain trivial cases. In contrast to these qualitative statements, we also prove explicit, quantitative results whenever n is an odd prime or $n = 4$. In the prime case, we give formulae for the local masses $m_{\mathcal{A},\mathfrak{p}}$, allowing us to express the density

$$\lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{X}$$

as an explicit Euler product. In the quartic case, we give a formula for $m_{\mathcal{A},\mathfrak{p}}$ whenever $\mathfrak{p}$ is not a finite prime lying over 2. For the finitely many such exceptional primes $\mathfrak{p}$, we give algorithms for computing $m_{\mathcal{A},\mathfrak{p}}$, in principle allowing one to find the same explicit Euler product as in the prime case. As we mentioned earlier, in general the Malle–Bhargava heuristics are conjectural, but in fact they are theorems for $n \leq 5$. Since each of $n = 3, 4, 5$ is either an odd prime or equal to 4, our explicit Euler product is unconditionally true in those cases.

Part 2. Context and motivation

The aim of Part 2 is to set the scene for our work by giving exposition and historical context. Most of this context is not essential for understanding the original results in Parts 3 and 4. The only strict prerequisites are Section 3.1, and the statement of Theorem 3.53.

1. Arithmetic statistics is not statistics!

On multiple occasions, actual number theory graduate students have told me things like "I will not go to the arithmetic statistics course at this summer school because *I don't like statistics*". This is sad to hear, because arithmetic statistics has very little to do with statistics. The word "statistics" just refers to the fact that we are counting arithmetic objects. For example, the Prime Number Theorem[1] is a result in arithmetic statistics, because we are counting prime numbers.

1.1. **A motivating example.** Now that we know what arithmetic statistics is not (statistics), we will start thinking about what it is. Consider the following question:

Question 1.1. What is the probability that a randomly selected integer is even?

It is obvious that the answer should be half. Unfortunately, there are a few obstacles to making the question precise.

First of all, we haven't specified the method of "random selection", i.e. our probability distribution. Naïvely, we would like a uniform distribution, but this is impossible for a countably infinite set. Instead, we might think about truncating the integers by some large real number. For any positive real number X, define

$$\mathbb{Z}_{\leq X} = \{n \in \mathbb{Z} : |n| \leq X\}.$$

Since $\mathbb{Z}_{\leq X}$ is finite, we can actually define a uniform distribution on it. Write

$$N(X) = \#\mathbb{Z}_{\leq X},$$

and

$$N(X; \text{even}) = \#\{n \in \mathbb{Z}_{\leq X} : n \text{ is even}\}.$$

Then we have

$$N(X) = 1 + 2\lfloor X \rfloor$$

and

$$N(X; \text{even}) = 1 + 2\left\lfloor \frac{X}{2} \right\rfloor,$$

and it follows that the probability is given by

$$\mathbb{P}_{n \in \mathbb{Z}_{\leq X}}\big(\{n \text{ is even}\}\big) = \frac{1 + 2\lfloor \frac{X}{2} \rfloor}{1 + 2\lfloor X \rfloor}.$$

It is easy to see that this probability converges to $\frac{1}{2}$, as one would expect. Since the quantities $N(X)$ and $N(X; \text{even})$ contain strictly more information than the probability alone, we might be interested in them for their own sake. More likely, we might be interested in their asymptotics, noting that

$$N(X) = X + O(1)$$

[1] We will see in Example 2.2 how the PNT fits into our framework of arithmetic statistics.

and

$$N(X;\text{even}) = \frac{1}{2}\cdot X + O(1).$$

It follows from these asymptotics that

$$\lim_{X\to\infty} \mathbb{P}_{n\in\mathbb{Z}_{\leq X}}\big(\{n \text{ is even}\}\big) = \frac{1}{2}.$$

An important point is that all of the above depends on how we order the integers. For example, we could order them as follows:

$$0, -2, 2, -1, -4, 4, 1, -6, 6, -3, -8, 8, 3, \ldots.$$

We could then define

$$\mathbb{Z}_{\leq X} = \{\text{The first } \lfloor X \rfloor \text{ integers with respect to this other ordering}\},$$

and we would obtain

$$N(X) = X + O(1)$$

and

$$N(X;\text{even}) = \frac{2}{3}\cdot X + O(1),$$

resulting in

$$\lim_{X\to\infty} \mathbb{P}_{n\in\mathbb{Z}_{\leq X}}\big(\{n \text{ is even}\}\big) = \frac{2}{3}.$$

So the asymptotics of $N(X)$ and $N(X;\text{even})$, and the resulting probabilities, depend meaningfully on how we order our objects. In the case of $\mathbb{Z}$, this seems facetious, since there really is an obvious way of ordering them. However, for other families of objects, there might be more than one sensible ordering, and different ways might yield different results.

2. Examples of asymptotic counting problems

Many problems in arithmetic statistics concern the kind of "asymptotic counting" that we saw in Section 1. In Section 2.1, we will make precise what we mean by asymptotic counting. Subsequently, in Sections 2.2, 2.4, and 2.5, we give three famous examples of such problems.

2.1. **Setup.**

Suppose that we have the following data:

(1) A countably infinite set $\mathcal{C}$.
(2) A map $f : \mathcal{C} \to \mathbb{R}_{>0}$ such that for each $X \in \mathbb{R}_{>0}$, the set $\{c \in \mathcal{C} : f(c) \leq X\}$ is finite.
(3) A property $\mathcal{P}$ that each element of $\mathcal{C}$ either satisfies or does not satisfy. We view this property as a function $\mathcal{P} : \mathcal{C} \to \{0, 1\}$, where $\mathcal{P}(c) = 1$ if and only if c has the property.

We refer to the function f as an *ordering* on $\mathcal{C}$. Given such an ordering, define the set

$$\mathcal{C}_{f\leq X} = \{c \in \mathcal{C} : f(c) \leq X\}$$

and the count

$$N_{\mathcal{C},f}(X;\mathcal{P}) = \#\{c \in \mathcal{C}_{f\leq X} : \mathcal{P}(c) = 1\}.$$

Write $N_{\mathcal{C},f}(X)$ for $N_{\mathcal{C},f}(X;\mathcal{P})$ in the case where $\mathcal{P}$ is the trivial property that is always true. That is, we define

$$N_{\mathcal{C},f}(X) = \#\mathcal{C}_{f\leq X}.$$

In general, we will use the term *asymptotic counting problem* to mean finding asymptotics of $N_{\mathcal{C},f}(X;\mathcal{P})$, for some choice of data $(\mathcal{C}, f, \mathcal{P})$.

Example 2.1 (Even integers)**.** Taking

$$(\mathcal{C}, f, \mathcal{P}) = (\mathbb{Z}, n \mapsto |n|, \text{“n is even”}),$$

we recover our motivating example, for which we obtained

$$N_{\mathcal{C},f}(X) = X + O(1)$$

and

$$N_{\mathcal{C},f}(X; \mathcal{P}) = \frac{1}{2}X + O(1).$$

Example 2.2 (Prime Number Theorem)**.** Taking

$$(\mathcal{C}, f, \mathcal{P}) = \{\mathbb{Z}_{>0}, n \mapsto n, \text{“}n\text{ is prime”}\},$$

the Prime Number Theorem is precisely that

$$N_{\mathcal{C},f}(X; \mathcal{P}) \sim \frac{X}{\log X},$$

as $X \to \infty$.

In the remainder of Section 2, we give some examples of prominent asymptotic counting problems. These examples are well-known, even outside specialist arithmetic statistics circles. The most relevant example for this thesis, Malle's conjecture, is postponed until Section 3.

2.2. **Manin's conjecture.** This example involves some terminology from algebraic geometry. If a word is unfamiliar, it can generally be replaced with “nice” or “suitable”.

Let V/k be a Fano (suitable) variety over a number field k, and let $\mathcal{L}$ be an adelically metrised ample (suitable) line bundle on V. The line bundle induces a *height* on V, which is a function $H_{\mathcal{L}} : V(k) \to \mathbb{R}_{\geq 0}$ with the property that $H_{\mathcal{L}}^{-1}([0, X])$ is finite for all real numbers X.

Given a subset $U \subseteq V(k)$ and a real number X, define

$$N_{U,\mathcal{L}}(X) = \#\{p \in U : H_{\mathcal{L}}(p) \leq X\}.$$

Then Manin's conjecture states that there exists a “thin” set $T \subseteq V(k)$ and real constants a, b, and C, such that

$$N_{V(k)\setminus T,\mathcal{L}}(X) \sim CX^a(\log X)^{b-1}.$$

This fits into our framework from before by taking

$$(\mathcal{C}, f, \mathcal{P}) = (V(k), H_{\mathcal{L}}, \text{“}p \notin T\text{”}).$$

Manin's conjecture is a very active open problem in arithmetic geometry (see e.g. [J F89], [Pey95], [Bro05]).

2.3. **Goldfeld's conjecture.** Let E be an elliptic curve defined over $\mathbb{Q}$. Then there are integers A and B such that E is isomorphic to the curve defined over $\mathbb{Q}$ by $y^2 = x^3 + Ax + B$. For a squarefree integer D, define the *quadratic twist of E by D* to be the elliptic curve E_D with equation $Dy^2 = x^3+Ax+B$. The twisting operation $E \mapsto E_D$ is well-defined up to isomorphism, and the curves E and E_D are usually[1] nonisomorphic over $\mathbb{Q}$.

There is a famous conjecture, called Goldfeld's conjecture ([Gol79, Page 113, Conjecture B]), concerning the statistical behaviour of these quadratic twists. The conjecture states that, when

[1] This is not always the case. For example, the curve $E : y^2 = x^3 - x$ is isomorphic to its twist E_{-1} by -1.

ordered by the size of D, the average (analytic) rank of the quadratic twists E_D is equal to $\frac{1}{2}$. A natural refinement, often also called Goldfeld's conjecture (see e.g. [BT22, Conjecture 2.4]), is that 50% of quadratic twists have rank 0, 50% have rank 1, and 0% have any other rank. This refined conjecture fits into our definition for an asymptotic counting problem, taking

$$(\mathcal{C}, f, \mathcal{P}_r) = (\{\text{squarefree integers } D\}, D \mapsto |D|, \text{“}E_D \text{ has rank } r\text{”}),$$

for each nonnegative integer r. Then the conjecture is that

$$\lim_{X\to\infty} \frac{N_{\mathcal{C},f}(X;\mathcal{P}_r)}{N_{\mathcal{C},f}(X)} = \begin{cases} \frac{1}{2} & \text{if } r = 0 \text{ or } r = 1, \\ 0 & \text{otherwise.} \end{cases}$$

2.4. **Elliptic curves ordered by height.** Let $\mathcal{E}$ be the set of isomorphism classes of elliptic curves over $\mathbb{Q}$. For each curve $E \in \mathcal{E}$, there is a unique pair of integers (A, B) such that the following two statements are true:

(1) The elliptic curve E is isomorphic over $\mathbb{Q}$ to the elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$.
(2) For every prime p with $p^4 \mid A$, we have $p^6 \nmid B$.

For $E \in \mathcal{E}$, define the *height* $H(E)$ of E to be the quantity

$$H(E) = \max\{4|A|^3, 27B^2\},$$

where the pair (A, B) is as above. For real numbers X, define

$$\mathcal{E}_{H\leq X} = \{E \in \mathcal{E} : H(E) \leq X\}.$$

Given a property $\mathcal{P}$ of elliptic curves, write

$$N_{\mathcal{E},H}(X;\mathcal{P}) = \#\{E \in \mathcal{E}_{H\leq X} : \text{“}E \text{ satisfies } \mathcal{P}\text{”}\}.$$

Similarly to the refinement of Goldfeld's conjecture stated above, it is also conjectured ([BS13a, Corollary 6]) that, for nonnegative integers r, we have

$$\lim_{X\to\infty} \frac{N_{\mathcal{E},H}(X;\operatorname{rank} E = r)}{N_{\mathcal{E},H}(X)} = \begin{cases} \frac{1}{2} & \text{if } r = 0 \text{ or } r = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

In other words, when elliptic curves over $\mathbb{Q}$ are ordered by height, 50% of them have rank 0, 50% have rank 1, and 0% of them have any other rank. In fact, Bhargava and Shankar show that Equation 1 is implied by a stronger set of conjectures, including[1] [BS13a, Conjecture 4], which states that, for all n, the average size of the n-Selmer group $\operatorname{Sel}_n(E)$ is equal to $\sigma(n)$, which is defined to be the sum of the divisors of n. That is, they conjecture that

$$\lim_{X\to\infty} \frac{\sum_{E\in\mathcal{E}_{H\leq X}} \# \operatorname{Sel}_n(E)}{N_{\mathcal{E},H}(X)} = \sum_{d\mid n} d,$$

for all n.

Bhargava and Shankar are able to prove this conjecture for $n = 2, 3, 4$, and 5, in [BS10, Theorem 1.1], [BS15, Theorem 1.1], [BS13a, Theorem 1], and [BS13b, Theorem 1], respectively. They use a powerful collection of techniques, referred to colloquially as “Bhargavology”, which involves parametrising families of arithmetic objects by so-called “coregular representations”, and then counting “integral points” of those representations. We will see much more Bhargavology in Section 3, in the context of counting number fields rather than elliptic curves.

[1] The other conditions are that the root numbers of elliptic curves are equidistributed and that the parity conjecture holds. See [BS13a, Corollary 6].

2.5. **Cohen–Lenstra heuristics.** Write Cl_K for the class group of a number field K. The Cohen–Lenstra heuristics are conjectural heuristics for understanding the distribution of the p-part $\mathrm{Cl}_K[p^\infty]$ of Cl_K, as K ranges over either imaginary quadratic fields or abelian totally real fields of a given degree. For non-quadratic fields, the original conjectures are known to be false in some cases; see [BJ20] for a detailed discussion. Nevertheless, the Cohen–Lenstra heuristics remain some of the best-known conjectures in arithmetic statistics. For simplicity, we will restrict our attention to the imaginary quadratic case, noting that the full conjectures are stated in [CL84, Fundamental Assumptions 8.1, Page 54]. For a real number X, write

$$\underline{\mathrm{IQ}}_{\leq X} = \{K \in \underline{\mathrm{IQ}} : |\mathrm{disc}(K/\mathbb{Q})| \leq X\}.$$

The Cohen–Lenstra heuristics essentially say that, as K varies over $\underline{\mathrm{IQ}}$, the finite p-group $\mathrm{Cl}_K[p^\infty]$ behaves like a "random finite abelian p-group", in a sense we will now make precise. Write $[n]$ as shorthand for the set $\{1, \dots, n\}$. Define a *group law on n symbols* to be an associative binary operation $f : [n] \times [n] \to [n]$ with identity, and write $\mathbf{GrpLaw}(n)$ for the set of group laws on n symbols. For $f \in \mathbf{GrpLaw}(n)$, write $([n], f)$ for the group defined by f.

Lemma 2.3. *Let G be a finite group of size n. We have*

$$\#\{f \in \mathbf{GrpLaw}(n) : ([n], f) \cong G\} = \frac{n!}{\#\,\mathrm{Aut}(G)}.$$

Proof. There is a well-defined, transitive right-action of $\mathrm{Aut}_{\mathbf{Set}}([n])$ on

$$\{f \in \mathbf{GrpLaw}(n) : ([n], f) \cong G\},$$

given by $f^\sigma(i, j) = \sigma^{-1} f(\sigma i, \sigma j)$. For a given group law $f \in \mathbf{GrpLaw}(n)$ with $([n], f) \cong G$, this action has

$$\mathrm{Stab}(f) = \mathrm{Aut}_{\mathbf{Grp}}(([n], f)),$$

and the result follows by the Orbit-Stabiliser Theorem. □

For each positive integer i, we define a *random p-group of size p^i* to be the group $([p^i], f)$, where f is selected uniformly at random from $\mathbf{GrpLaw}(p^i)$. Let $\mathcal{G}$ be a random p-group of size p^i, and let G be a specific p-group of size p^i. Then we have just shown that

$$\mathbb{P}(\mathcal{G} \cong G) = \frac{1}{c_i \cdot \#\,\mathrm{Aut}(G)},$$

where, writing $\mathbf{Grp}(p^i)$ for the set of isomorphism classes of groups of size p^i, we have

$$c_i = \sum_{G \in \mathbf{Grp}(p^i)} \frac{1}{\#\,\mathrm{Aut}(G)}.$$

It turns out (see [Woo16, Proposition 5.7]) that $\sum_i c_i < \infty$, so we can allow $\mathcal{G}$ to vary over the set $\mathbf{Grp}_p$ of p-groups of *any size*, by insisting that

$$\mathbb{P}(\#\mathcal{G} = p^i) = \frac{c_i}{\sum_j c_j}.$$

By the law of total probability, it follows that for any p-group G, we have

$$\mathbb{P}(\mathcal{G} = G) = \frac{\kappa_p}{\#\,\mathrm{Aut}(G)},$$

for a constant κ_p depending only on p. We call a group $\mathcal{G}$ distributed in this way a *random p-group*, with no size prescribed. From here, it is straightforward to define a "random abelian p-group" to come from the same distribution, conditional on $\mathcal{G}$ being an abelian group. Letting

$\mathcal{G}'$ be a random abelian p-group, we then have

$$\mathbb{P}(\mathcal{G}' \cong G) = \frac{\kappa_p'}{\#\operatorname{Aut}(G)},$$

for a different constant κ_p'. The Cohen–Lenstra heuristics for imaginary quadratic fields essentially conjecture that, for odd p, the p-part of the class group of a "randomly selected" $K \in \underline{\mathrm{IQ}}$ is a random abelian p-group. That is, for any finite abelian p-group G, the conjecture is that

$$\lim_{X \to \infty} \frac{\#\{K \in \underline{\mathrm{IQ}}_{\leq X} : \mathrm{Cl}_K[p^\infty] \cong G\}}{\#\underline{\mathrm{IQ}}_{\leq X}} = \frac{\kappa_p'}{\#\operatorname{Aut}(G)}.$$

This conjecture was originally made in [CL84, Fundamental Assumption 2, Page 54]. Our formulation looks slightly different from Cohen and Lenstra's formal statement, but resembles more closely their informal explanation in the final paragraph of [CL84, Page 54].

The Cohen–Lenstra heuristics illustrate a common pattern in arithmetic statistics, namely that an object's prevalence is inversely proportional to its "complexity", which in this case means the number of automorphisms. We will see more examples of this idea later.

3. Background on counting rings of low rank

In Section 3, we explore the asymptotic counting problems most relevant to our work, namely those involving number fields ordered by discriminant. We will try to understand the asymptotics of a certain function $N_{k,G}(X;\Sigma)$, where k is a number field, G is a "permutation group", and Σ is a "collection of local conditions". In order to define $N_{k,G}(X;\Sigma)$ properly, we will need more theory, so we postpone the full definition until Section 3.4. In the meantime, we will give an imprecise definition, so that we can roughly explain the Malle–Bhargava heuristics.

Given a subgroup $G \subseteq S_n$, we will define $N_{k,G}(X)$ to be the number of degree n extensions K/k with $\operatorname{Nm}(\operatorname{disc}(K/k)) \leq X$, such that the Galois closure group $\operatorname{Gal}(\widetilde{K}/k)$ acts on the embeddings $\operatorname{Hom}(K, \overline{k})$ in the same way that G acts on $[n]$, via the inclusion $G \subseteq S_n$. Taking $G = S_n$, we recover the count $N_{k,n}(X)$ of S_n-n-ic extensions from Part 1. Moreover, we can insist that the extensions K/k satisfy a "family of local conditions" Σ, which means that K has certain prescribed behaviour "at each place" of the base field k. We write $N_{k,G}(X;\Sigma)$ for the modified count of extensions K/k satisfying the local conditions Σ. In keeping with our earlier notation, we write $N_{k,n}(X;\Sigma)$ for the special case where G is the whole group S_n. There is a set of conjectures, called the "Malle–Bhargava heuristics", which assume that the count $N_{k,G}(X;\Sigma)$ behaves in certain simple, intuitive ways, leading to conjectures about its asymptotics.

The Malle–Bhargava heuristics depend heavily on a notion called the *mass* of a collection of étale algebras, which we discuss in Section 3.1. It turns out that there is a correspondence between étale algebras and Galois representations. We explain this correspondence in Section 3.2, translating the masses of Section 3.1 into quantities related to Galois representations. Having developed the prerequisite theory, in Sections 3.3 and 3.4 we present two different versions of the Malle–Bhargava heuristics, which we call the "algebraic" and "analytic" MBH, respectively.

The algebraic MBH is quite intuitive, but it only addresses the special case $G = S_n$, giving conjectural asymptotics for the count $N_{k,n}(X;\Sigma)$. The analytic MBH is theoretically deeper, but much more general, extending the conjectures to $N_{k,G}(X;\Sigma)$ for any subgroup G of S_n.

3.1. **Étale algebras and their masses.** In this subsection, we introduce étale algebras and the notion of mass. We develop some theory concerning these concepts, mostly following [Bha07].

By a *p-adic field*, we mean a finite field extension of $\mathbb{Q}_p$, for some rational prime p. By a *local field*, we mean a field that is either p-adic or isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

Definition 3.1 (Étale algebras)**.** Let $\mathcal{E}$ be a field.

1. An *étale algebra over* $\mathcal{E}$ is an $\mathcal{E}$-algebra $\mathcal{M}$ that is isomorphic to a finite product $\mathcal{M}_1 \times \ldots \times \mathcal{M}_r$ of separable field extensions $\mathcal{M}_i/\mathcal{E}$.
2. The *degree* of an étale algebra over $\mathcal{E}$ is its dimension as an $\mathcal{E}$-vector space.
3. Write $\text{Ét}_{n/\mathcal{E}}$ for the set of isomorphism classes of degree n étale algebras over $\mathcal{E}$.
4. Assume that $\mathcal{E}$ is a number field or a local field, and let $\mathcal{M}$ be a finite degree étale algebra over $\mathcal{E}$, isomorphic to the product of fields $\mathcal{M}_1 \times \ldots \times \mathcal{M}_r$. The fields $\mathcal{M}_i$ correspond to the maximal ideals of the algebra $\mathcal{M}$, so they are unique up to reordering, and therefore the following notions are well-defined. The *norm map* of the étale algebra is the map
$$N_{\mathcal{M}/\mathcal{E}} : \mathcal{M} \to \mathcal{E}, \quad (x_1, \ldots, x_r) \mapsto \prod_{i=1}^{r} N_{\mathcal{M}_i/\mathcal{E}}(x_i).$$
If $\mathcal{E}$ is a number field or a p-adic field, then the *discriminant* of $\mathcal{M}/\mathcal{E}$ is
$$\text{disc}(\mathcal{M}/\mathcal{E}) = \prod_{i=1}^{r} \text{disc}(\mathcal{M}_i/\mathcal{E}).$$

For finite degree (étale or field) extensions $\mathcal{M}/\mathcal{E}$, we will often write $d_{\mathcal{M}/\mathcal{E}}$ as shorthand for the discriminant $\text{disc}(\mathcal{M}/\mathcal{E})$.

Definition 3.2 (Mass)**.** Let n be an integer, let F be a local field, and let $\Sigma \subseteq \text{Ét}_{n/F}$. We define a few related notions of "mass" of Σ as follows:

1. The *pre-mass* of Σ is the quantity
$$\widetilde{m}(\Sigma) = \begin{cases} \sum_{L \in \Sigma} \frac{1}{\#\operatorname{Aut}(L/F)} \cdot q_F^{-v_F(d_{L/F})} & \text{if } F \text{ is } p\text{-adic}, \\ \sum_{L \in \Sigma} \frac{1}{\#\operatorname{Aut}(L/F)} & \text{if } F \text{ is isomorphic to } \mathbb{R} \text{ or } \mathbb{C}, \end{cases}$$
where q_F is the size of the residue field $\mathbb{F}_F$ of F.
2. The *mass* of Σ is the quantity
$$m(\Sigma) = \begin{cases} \frac{q_F - 1}{q_F} \cdot \widetilde{m}(\Sigma) & \text{if } F \text{ is } p\text{-adic}, \\ \widetilde{m}(\Sigma) & \text{if } F \text{ is isomorphic to } \mathbb{R} \text{ or } \mathbb{C}. \end{cases}$$
3. For p-adic F, the *generalised pre-mass* of Σ is the rational function
$$\widetilde{m}(t; \Sigma) = \sum_{L \in \Sigma} \frac{1}{\#\operatorname{Aut}(L/F)} \cdot t^{-v_F(d_{L/F})}.$$

The notion of mass was first studied by Serre in the 1970s. Given a p-adic field F, he asked for the mass (or, in our language, the pre-mass) of the set of all totally ramified field extensions L/F of a given degree. In the tamely ramified case, it is easy to write down all such extensions (see [PR01, Theorem 7.2]), and hence compute the mass, which turns out to be described by a simple formula. In the wildly ramified case, there are very many more extensions, and they have no known classification. Remarkably, Serre proved that in the wild case, the mass is given by *exactly the same formula* as in the tame case. His famous result, called "Serre's mass formula" is the following:

Theorem 3.3 (Serre's mass formula)**.** *Let n be an integer, let F be a p-adic field with residue field of size q_F, and let Σ be the set of all totally ramified degree n field extensions of F. Then*

$$\widetilde{m}(\Sigma) = \frac{1}{q_F^{n-1}}.$$

Proof. This is essentially [Ser78, Theorem 2]. □

In [Bha07], Bhargava extends Serre's work in two directions:

(1) Bhargava defines and studies the mass of étale algebras, rather than just field extensions.
(2) He also considers different ramification behaviours, rather than just totally ramified extensions.

In order to understand ramification behaviours of étale algebras, Bhargava defines the notion of a "splitting symbol" as follows:

Definition 3.4 (Splitting symbols)**.** Let n be a positive integer. A *degree n splitting symbol* is a symbol $(f_1^{e_1} \dots f_r^{e_r})$, where the f_i and e_i are positive integers with $\sum_i f_i e_i = n$. We identify splitting symbols that are permutations of each other, i.e. $(1^2 2^3) = (2^3 1^2)$. The superscripts are purely symbolic, and do not represent exponentiation, so for example (1^2) and (1^3) are different splitting symbols. Finally, we suppress exponents with value 1, writing e.g. (2) instead of (2^1). Write Split_n for the set of degree n splitting symbols.

Definition 3.5 (Splitting symbols)**.** Let F be a local field and let $L \in \text{Ét}_{n/F}$. Then we have

$$L = L_1 \times \ldots \times L_r,$$

for field extensions L_i/F with inertia degree f_i and ramification index e_i. We adopt the convention that the extension $\mathbb{C}/\mathbb{R}$ has ramification index 2 and inertia degree 1. The *splitting symbol* (L, F) *of L over F* is defined to be the symbol

$$(L, F) = (f_1^{e_1} \dots f_r^{e_r}).$$

For a splitting symbol $\sigma \in \mathrm{Split}_n$, write $\text{Ét}_{\sigma/F}$ for the set of $L \in \text{Ét}_{n/F}$ with $(L, F) = \sigma$.

Example 3.6. For a p-adic field F and an integer n, the set $\text{Ét}_{(1^n)/F}$ consists of all totally ramified field extensions L/F of degree n, so Serre's mass formula says precisely that

$$\widetilde{m}(\text{Ét}_{(1^n)/F}) = \frac{1}{q_F^{n-1}}.$$

Bhargava gives two different generalisations of Serre's mass formula. One of them gives the mass of $\text{Ét}_{\sigma/F}$ for an arbitrary splitting symbol σ, and the other involves something called a "ramification partition", which we will define shortly.

Definition 3.7 (Partitions)**.** Let d be a nonnegative integer and let m be a positive integer. The symmetric group S_m acts by permutation of coordinates on the set $\mathbb{Z}_{\geq 0}^m$ of nonnegative integers. We make the following definitions:

(1) We define a *partition of d into m parts* to be an equivalence class

$$[(a_i)] \in \mathbb{Z}_{\geq 0}^m / S_m$$

such that $\sum_i a_i = d$. This is often referred to as a partition into "at most" m parts, but for our purposes it is more convenient to allow parts to be zero.

(2) Write $\mathrm{Part}(d, m)$ for the number of partitions of d into m parts.

Definition 3.8 (Invariants of splitting symbols)**.** Let $\sigma = (f_1^{e_1} \dots f_r^{e_r})$ be a degree n splitting symbol.

(1) The *ramification partition of* σ is the partition

$$\pi(\sigma) := (e_1 - 1, \dots, e_1 - 1, e_2 - 1, \dots, e_2 - 1, \dots, e_r - 1, \dots, e_r - 1),$$

where each term $e_i - 1$ appears f_i times.

(2) The *discriminant of* σ is the integer

$$d_\sigma = \sum_i f_i(e_i - 1).$$

(3) The *automorphism count of* σ is the integer

$$\#\,\mathrm{Aut}(\sigma) = \Big(\prod_i f_i\Big) \cdot \#\big\{\tau \in S_r : (e_{\tau(i)}, f_{\tau(i)}) = (e_i, f_i) \text{ for all } i\big\}.$$

Note that $\pi(\sigma)$ is a partition of d_σ into $n - d_\sigma$ parts. We are now ready to state Bhargava's generalisations of Serre's mass formula:

Theorem 3.9 (Bhargava's mass formulae)**.** *Let n be a positive integer and let F be a p-adic field with residue field of size q. The following two statements are true:*

(1) For each $\sigma \in \mathrm{Split}_n$, we have

$$\widetilde{m}(\mathrm{\acute{E}t}_{\sigma/F}) = \frac{1}{q^{d_\sigma}} \cdot \frac{1}{\#\,\mathrm{Aut}(\sigma)}.$$

(2) Let d be an integer with $0 \le d \le n - 1$, and let π_0 be any partition of d into $n - d$ parts. Then

$$\widetilde{m}\big(\{L \in \mathrm{\acute{E}t}_{n/F} : \pi((L, F)) = \pi_0\}\big) = \frac{1}{q^d}.$$

Proof. These are essentially [Bha07, Propositions 2.1 and 2.2]. Bhargava states the results for $F = \mathbb{Q}_p$, but the appendix of [Bha07] explains how to extend the proof to arbitrary F. □

We record the following corollary:

Corollary 3.10. *Let F be a p-adic field for some rational prime p. Let n and d be integers with $0 \le d \le n - 1$. Then*

$$\widetilde{m}\big(\{L \in \mathrm{\acute{E}t}_{n/F} : d_{(L,F)} = d\}\big) = \frac{\mathrm{Part}(d, n - d)}{q^d}.$$

Proof. This follows easily from Theorem 3.9(2). □

Lemma 3.11. *Let E/F be a tamely ramified extension of p-adic fields, with ramification index e and inertia degree f. Then*

$$v_F(d_{E/F}) = f(e - 1).$$

Proof. This follows easily from [NS13, Page 199, Theorem 2.6] and [NS13, Page 201, Theorem 2.9]. □

In the tamely ramified case, we can extend Bhargava's formula for $\widetilde{m}(\text{Ét}_{\sigma/F})$ to a statement about the generalised pre-mass, which will be useful when we consider the analytic Malle–Bhargava heuristics.

Lemma 3.12 (Generalised Bhargava mass formula)**.** *Let F be a p-adic field, let n be a positive integer, and let $\sigma \in \operatorname{Split}_n$. Write $\sigma = (f_1^{e_1} \dots f_r^{e_r})$, and assume that $p \nmid e_i$ for all i. The following three statements are true:*

(1) We have

$$\widetilde{m}\big(t; \text{Ét}_{\sigma/F}\big) = \frac{1}{t^{d_\sigma}} \cdot \frac{1}{\# \operatorname{Aut}(\sigma)}.$$

(2) We have

$$\widetilde{m}\big(t; \big\{L \in \text{Ét}_{n/F} : \pi((L,F)) = \pi(\sigma)\big\}\big) = \frac{1}{t^{d_\sigma}}.$$

(3) For each integer d with $0 \leq d \leq n-1$, we have

$$\widetilde{m}\big(t; \big\{L \in \text{Ét}_{n/F} : d_{L/F} = d\big\}\big) = \frac{\operatorname{Part}(d, n-d)}{t^d}.$$

Proof. Since $p \nmid e_i$ for each i, Lemma 3.11 tells us that every $L \in \text{Ét}_{n/F}$ with $\pi((L,F)) = \pi(\sigma)$ has

$$v_F(d_{L/F}) = d_\sigma.$$

This has two consequences:

(a) We have

$$\widetilde{m}(t; \text{Ét}_{\sigma/F}) = \frac{1}{t^{d_\sigma}} \cdot \sum_{L \in \text{Ét}_{\sigma/F}} \frac{1}{\# \operatorname{Aut}(L/F)}$$

and

$$\widetilde{m}(t; \{L \in \text{Ét}_{n/F} : \pi((L,F)) = \pi(\sigma)\}) = \frac{1}{t^{d_\sigma}} \cdot \sum_{\substack{L \in \text{Ét}_{n/F} \\ \pi((L,F)) = \pi(\sigma)}} \frac{1}{\# \operatorname{Aut}(L/F)}.$$

(b) By Theorem 3.9, we have

$$\sum_{L \in \text{Ét}_{\sigma/F}} \frac{1}{\# \operatorname{Aut}(L/F)} = \frac{1}{\# \operatorname{Aut}(\sigma)}$$

and

$$\sum_{\substack{L \in \text{Ét}_{n/F} \\ \pi((L,F)) = \pi(\sigma)}} \frac{1}{\# \operatorname{Aut}(L/F)} = 1.$$

The result follows from Statements (a) and (b). □

3.2. **Equivalence of étale algebras and Galois representations.** The theory in this section is well-known, and is often used without reference in the arithmetic statistics literature. It is essentially what is known as "Grothendieck's Galois theory" (see e.g. [Mil22, Chapter 8]). We were unable to find a reference that uses the same language as Bhargava, so we have included the proofs here to aid the coherence of the thesis.

Let F be a field and let $\overline{F}$ be an algebraic closure of F. Write G_F for the absolute Galois group $\operatorname{Gal}(\overline{F}/F)$.

Definition 3.13. A *permutation group* is a triple (G, ι, X), where G is a finite group, X is a finite set, and ι is an injective group homomorphism $\iota : G \hookrightarrow \mathrm{Aut}(X)$. A *morphism of permutation groups* $(G_1, \iota_1, X_1) \to (G_2, \iota_2, X_2)$ is a pair (φ, f), where $\varphi : G_1 \to G_2$ is a group homomorphism and $f : X_1 \to X_2$ is a bijection, such that the following diagram commutes:

$$\begin{tikzcd}
G_1 \arrow[r, hook, "\iota_1"] \arrow[d, "\varphi"'] & \mathrm{Aut}(X_1) \arrow[d, "f_*"] \\
G_2 \arrow[r, hook, "\iota_2"'] & \mathrm{Aut}(X_2),
\end{tikzcd}$$

where $f_* : \mathrm{Aut}(X_1) \to \mathrm{Aut}(X_2)$ is defined by

$$f_*(\sigma)(y) = f(\sigma(f^{-1}(y)))$$

for all $y \in X_2$. Composition of morphisms is defined by

$$(\varphi, f) \circ (\psi, g) = (\varphi \circ \psi, f \circ g).$$

The *degree* of a permutation group (G, ι, X) is the size of X. Given a permutation group (G, ι, X), a *permutation subgroup* of (G, ι, X) is a permutation group (H, ι_H, X), where H is a subgroup of G and ι_H is the composition $H \hookrightarrow G \overset{\iota}{\hookrightarrow} \mathrm{Aut}(X)$.

It is clear that permutation groups form a category, where a morphism (φ, f) is an isomorphism if and only if φ is a group isomorphism.

Definition 3.14 (G-sets)**.** Let G be a topological group. A *G-set* is a pair (ρ, X), where X is a set and $\rho : G \to \mathrm{Aut}(X)$ is a continuous[1] group homomorphism. A *morphism of G-sets* $(\rho_1, X_1) \to (\rho_2, X_2)$ is a function $f : X_1 \to X_2$ such that for all $g \in G$, the following diagram commutes:

$$\begin{tikzcd}
X_1 \arrow[r, "\rho_1(g)"] \arrow[d, "f"'] & X_1 \arrow[d, "f"] \\
X_2 \arrow[r, "\rho_2(g)"'] & X_2
\end{tikzcd}$$

Call a G-set (ρ, X) *finite* if the set X is finite.

For any choice of G, it is clear that G-sets form a category, which we denote by G-**Set**.

Definition 3.15. Let G be any topological group and let (ρ, X) be a finite G-set. The *permutation group induced by* (ρ, X) is the permutation group

$$\big(\operatorname{im}\rho, \iota, X\big),$$

where ι is the natural inclusion $\operatorname{im}\rho \hookrightarrow \mathrm{Aut}(X)$.

Definition 3.16 (Galois permutation groups)**.** Let L be a degree n étale algebra over F. We have a natural G_F-set

$$\rho : G_F \to \mathrm{Aut}(\mathrm{Hom}_F(L, \overline{F})),$$

where $\sigma \in G_F$ acts by $\sigma \cdot \varphi = \sigma \circ \varphi$. The *Galois permutation group of L over F* is the permutation group

$$\mathrm{Gal}(L/F) = \big(\operatorname{im}\rho, \iota, \mathrm{Hom}_F(L, \overline{F})\big),$$

where ι is the natural inclusion.

The definition of the Galois permutation group is quite abstract, but it is in fact closely related to the Galois groups of the component field extensions. When these field extensions are

[1] With respect to the discrete topology on $\mathrm{Aut}(X)$.

linearly disjoint, in a sense we will make precise, the Galois permutation group admits a particularly simple description, which we will give in Lemma 3.20. In order to motivate the proof of Lemma 3.20, we first study the special case in which L is a field:

Example 3.17 (Galois group of a field extension)**.** Let L/F be a finite separable field extension, not necessarily Galois. The homomorphism

$$\rho : G_F \to \mathrm{Aut}(\mathrm{Hom}_F(L, \overline{F}))$$

factors through

$$G_F \to \mathrm{Gal}(\widetilde{L}/F) \overset{\iota}{\hookrightarrow} \mathrm{Aut}(\mathrm{Hom}_F(L, \overline{F})),$$

where $\widetilde{L}$ is the normal closure of L in $\overline{F}$ and, for all $\sigma \in \mathrm{Gal}(\widetilde{L}/F)$, we define $\iota(\sigma)$ to be the postcomposition map $\sigma \circ -$. It follows that $\mathrm{im}\,\rho \cong \mathrm{Gal}(\widetilde{L}/F)$, and the Galois permutation group of L over F is isomorphic to

$$\big(\mathrm{Gal}(\widetilde{L}/F), \iota, \mathrm{Hom}_F(L, \overline{F})\big).$$

In other words, the Galois permutation group $\mathrm{Gal}(L/F)$ is the group $\mathrm{Gal}(\widetilde{L}/F)$ together with its natural action on the embeddings of L. Thus, our étale algebra notion of Galois permutation groups strictly generalises the traditional notion of Galois groups of finite Galois field extensions.

Lemma 3.18. *Let F be a field and let $L_1, \ldots, L_r$ be field extensions of F, and let $L = L_1 \times \ldots \times L_r$. Let M be another field extension of F. There is a natural bijection*

$$f : \bigsqcup_{i=1}^{r} \mathrm{Hom}_F(L_i, M) \to \mathrm{Hom}_F(L, M),$$

where for each $\varphi \in \mathrm{Hom}_F(L_i, M)$, we have

$$f(\varphi)(x_1, \ldots, x_r) = \varphi(x_i).$$

Proof. It is easy to see that the map f is well-defined and injective, so we only need to show surjectivity. Let $\psi \in \mathrm{Hom}_F(L, M)$. For each i, write e_i for the element

$$(0, \ldots, 0, 1, 0, \ldots, 0) \in L,$$

where the 1 is in the i^{th} entry, and define the map $\varphi_i : L_i \to M$ by

$$\varphi_i(\lambda_i) = \psi(\lambda_i e_i).$$

It is easy to see that

$$\psi(x_1, \ldots, x_r) = \sum_{i=1}^{r} \varphi(x_i),$$

so there is some i such that $\varphi_i \neq 0$. There exists an element $\lambda_i \in L_i$ with $\varphi_i(\lambda_i) \neq 0$. For all $j \neq i$ and all $\lambda_j \in L_j$, we have

$$\varphi_i(\lambda_i)\varphi_j(\lambda_j) = \psi(\lambda_i \lambda_j e_i e_j) = \psi(0) = 0,$$

so $\varphi_j = 0$ for all $j \neq i$. Since ψ is an F-algebra homomorphism, it is easy to see that φ_i is too, and hence that $\psi = f(\varphi_i)$, as required. □

In the case where the component field extensions of an étale algebra are linearly disjoint, the Galois permutation group has a particularly nice description in terms of the Galois groups of those field extensions. We isolate this description in Lemma 3.20, whose proof is a natural extension of Example 3.17.

Definition 3.19. Let F be a field and let $L_1, L_2, \ldots, L_r$ be finite-degree field extensions of F. For each i, let $f_i(X) \in F[X]$ be a polynomial such that

$$L_i \cong \frac{F[X]}{(f_i(X))}.$$

We say that the extensions $L_1, \ldots, L_r$ are *mutually linearly disjoint* if, for each i, the splitting fields of f_i and $\prod_{j \neq i} f_j$ over F are linearly disjoint.

Note that in the case $r = 2$, extensions L_1 and L_2 are mutually linearly disjoint if and only if they are linearly disjoint.

Lemma 3.20. *Let F be a field with algebraic closure $\overline{F}$, and let $L_1, \ldots, L_r$ be mutually linearly disjoint finite field extensions of F. Let $m_1, \ldots, m_r$ be positive integers, and let L be the étale algebra*

$$L = \prod_{i=1}^{r} L_i^{m_i}$$

over F. For each i, let $\widetilde{L}_i \subseteq \overline{F}$ be a normal closure of L_i over F. Then the Galois permutation group of L/F is isomorphic to the permutation group

$$\Big(\prod_{i=1}^{r} \mathrm{Gal}(\widetilde{L}_i/F), \iota, \bigsqcup_{i=1}^{r} \bigsqcup_{j=1}^{m_i} \mathrm{Hom}_F(L_i, \overline{F}) \Big),$$

where ι is the natural inclusion

$$\iota : \prod_{i=1}^{r} \mathrm{Gal}(\widetilde{L}_i/F) \to \mathrm{Aut}\, \Big(\bigsqcup_{i=1}^{r} \bigsqcup_{j=1}^{m_i} \mathrm{Hom}_F(L_i, \overline{F}) \Big),$$

corresponding to the postcomposition action of $\mathrm{Gal}(\widetilde{L}_i/F)$ *on each copy of* $\mathrm{Hom}_F(L_i, \overline{F})$.

Proof. By Lemma 3.18, there is a natural bijection

$$f : \bigsqcup_{i=1}^{r} \bigsqcup_{j=1}^{m_i} \mathrm{Hom}_F(L_i, \overline{F}) \to \mathrm{Hom}_F(L, \overline{F}).$$

Since each $\widetilde{L}_i$ is a subfield of $\overline{F}$. We have a commutative diagram,

$$\begin{tikzcd}
G_F \arrow[r] \arrow[d] & \mathrm{Aut}(\mathrm{Hom}_F(L, \overline{F})) \\
\prod_{i=1}^{r} \mathrm{Gal}(\widetilde{L}_i/F) \arrow[r] & \mathrm{Aut}(\bigsqcup_i \bigsqcup_j \mathrm{Hom}_F(L_i, \overline{F})) \arrow[u, "f_*"']
\end{tikzcd}$$

where the horizontal maps come from the natural postcomposition actions, the map f_* is the same as in Definition 3.13, and the left-hand vertical map is the restriction map. We claim that the left-hand vertical map is surjective. This is clear in the case $r = 2$, and for $r \geq 2$ it follows by induction on r. The result then follows from commutativity of the diagram and surjectivity of the left-hand vertical map. □

Lemma 3.21. *Let (G, ρ, X) be a permutation group, and let $n = \#X$. There exists a subgroup $H \subseteq S_n$ and an isomorphism of permutation groups*

$$(G, \rho, X) \cong (H, \iota, [n]),$$

where ι is the inclusion $H \hookrightarrow S_n$. Moreover, if H' is another such subgroup of S_n, then there is an element $\sigma \in S_n$ such that $H' = \sigma H \sigma^{-1}$.

Proof. Label the elements of X by $\{x_1, \dots, x_n\}$. Define the bijection $f : [n] \to X$ by $f(i) = x_i$. The isomorphism $f_* : S_n \to \mathrm{Aut}(X)$ from Definition 3.13 simplifies to

$$S_n \overset{f_*}{\to} \mathrm{Aut}(X), \quad \sigma \mapsto (x_i \mapsto x_{\sigma i}).$$

Let H be the image of the composition

$$G \overset{\rho}{\hookrightarrow} \mathrm{Aut}(X) \overset{f_*^{-1}}{\to} S_n.$$

Then we have a commutative diagram

$$\begin{tikzcd}
G \arrow[r, "\rho"] \arrow[d, "f_*^{-1}\circ\rho"'] & \mathrm{Aut}(X) \arrow[d, "f_*^{-1}"] \\
H \arrow[r, "\iota"'] & S_n,
\end{tikzcd}$$

which tells us precisely that the permutation group $(H, \iota, [n])$ is isomorphic to (G, ρ, X). Now suppose that $H' \subseteq S_n$ is another subgroup with inclusion $\iota' : H' \hookrightarrow S_n$. The definition of morphisms of permutation groups tells us that

$$(H', \iota', [n]) \cong (H, \iota, [n])$$

if and only if $H' = \sigma H \sigma^{-1}$ for some $\sigma \in S_n$. □

In light of Lemma 3.21, we can specify a permutation group up to isomorphism by giving a subgroup of S_n. Given such a subgroup $G \subseteq S_n$, we will often just write G to refer to the permutation group $(G, \iota, [n])$, leaving the embedding of G into S_n implicit. As illustrated by the following example, this embedding really matters, so it is important to understand that writing G by itself is an abuse of notation. We will sometimes also write $G \subseteq S_n$ as abuse of notation for the same permutation group, $(G, \iota, [n])$.

Example 3.22 (Choice of embedding matters)**.** Let G_1 and G_2 be the permutation groups

$$G_1 = (\langle (12)(34), (13)(24) \rangle, \iota_1, [4])$$

and

$$G_2 = (\langle (12), (34) \rangle, \iota_2, [4]),$$

where ι_1 and ι_2 are the natural inclusions. In each case, the underlying group is isomorphic to V_4, but the embeddings into S_4 give nonisomorphic permutation groups. A quartic étale algebra always satisfies the hypotheses of Lemma 3.20, so we obtain the following two observations:

(1) An étale algebra has Galois permutation group G_1 if and only if it is a Galois field extension with Galois group V_4.
(2) An étale algebra has Galois permutation group G_2 if and only if it is a product of two nonisomorphic quadratic field extensions.

Lemma 3.23. *Let F be a field with algebraic closure $\overline{F}$, and let G_F be the absolute Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$. The following three statements are true:*

(1) There is a natural bijection

$$(\rho : G_F \to \mathrm{Aut}(X)) \mapsto L_\rho$$

between isomorphism classes of G_F-sets of size n and isomorphism classes of degree n étale algebras over F.

(2) Given a G_F-set $\rho : G_F \to \mathrm{Aut}(X)$ of size n and associated étale algebra L_ρ, the G_F-set $\mathrm{Hom}_F(L_\rho, \overline{F})$ is isomorphic to (ρ, X).

(3) *Given a G_F-set $\rho : G_F \to \mathrm{Aut}(X)$ of size n, the Galois permutation group of the étale algebra L_ρ is isomorphic to the permutation group induced by ρ.*

Proof. Let $\rho : G_F \to \mathrm{Aut}(X)$ be a continuous homomorphism, where X is a set of size n. Let $X_1, \ldots, X_r$ be the orbits of the corresponding action. For each i, choose some element $x_i \in X_i$, let $H_i = \mathrm{Stab}_{G_F}(x_i)$, and set $L_i = \overline{F}^{H_i}$. The subextensions of $\overline{F}/F$ isomorphic to L_i correspond to the conjugate subgroups of H_i in G_F. Changing choice of $x_i \in X_i$ would give a conjugate subgroup of H_i, so the field extension L_i/F is well-defined up to isomorphism. Reordering the sets X_i corresponds to reordering the L_i, so we have a well-defined étale algebra up to isomorphism, given by

$$L_\rho = L_1 \times \ldots L_r.$$

Conversely, let $L = L_1 \times \ldots \times L_r$ be a degree n étale algebra over F. For each i, the isomorphism class of the field extension L_i/F corresponds to a conjugacy class of subgroup $H_i \subseteq G_F$, with $L_i \cong \overline{F}^{H_i}$. Given such a subgroup H_i, let X_i be the set of left cosets G_F/H_i. Then there is a natural action of G_F on X_i, given by $g \cdot [f] = [g \circ f]$. Given a conjugate $\sigma H_i \sigma^{-1}$ of H_i, the G_F-sets G_F/H_i and $G_F/\sigma H_i \sigma^{-1}$ are isomorphic via the map

$$G_F/H_i \to G_F/(\sigma H_i \sigma^{-1}), \quad [f] \mapsto [f \circ \sigma^{-1}].$$

Thus, each G_F-set X_i is well-defined up to isomorphism. Changing the ordering of the L_i corresponds to changing the ordering of the X_i, so the G_F-set

$$X = \bigsqcup_i X_i$$

is well-defined up to isomorphism of G_F-sets. It is clear that these two constructions are mutual inverses, so we obtain the first statement. The second and third statements are immediate from the construction. □

Definition 3.24. Let $G = (G, \iota, X)$ be a permutation group and let F be a field. A *G-extension of F* is an étale algebra L/F with Galois permutation group isomorphic to G. Write $(G\text{−}\mathbf{Ext})_F$ for the set of isomorphism classes of G-extensions of F.

Let $G \subseteq S_n$ be a permutation group. We say that two homomorphisms $\rho, \rho' : G_F \to G$ are *S_n-conjugate* if there is some $f \in S_n$ such that $fGf^{-1} = G$ and the diagram

$$\begin{tikzcd}
 & G \arrow[dd, "f_*"] \\
G_F \arrow[ur, "\rho"] \arrow[dr, "\rho'"'] & \\
 & G
\end{tikzcd}$$

commutes, where f_* is the map $f_*(\sigma) = f\sigma f^{-1}$.

Lemma 3.25. *Let $G \subseteq S_n$ be a permutation group. There is a natural bijection between S_n-conjugacy classes of surjective group homomorphisms $\rho : G_F \to G$ and isomorphism classes of étale algebras with Galois permutation group isomorphic to G.*

Proof. This follows easily from Lemma 3.23. □

Example 3.26 (S_3-cubics)**.** Cubic étale algebras over $\mathbb{Q}$ correspond to isomorphism classes of $G_{\mathbb{Q}}$-sets of size 3. Let $\rho : G_F \to \mathrm{Aut}(X)$ be such a $G_{\mathbb{Q}}$-set. Since we only care about our $G_{\mathbb{Q}}$-set up to isomorphism, we may assume that $X = \{1, 2, 3\}$, so that we have $\rho : G_F \to S_3$.

Then the étale algebra L_ρ is a field if and only if ρ is transitive, in which case

$$L_\rho \cong \overline{\mathbb{Q}}^{\mathrm{Stab}_{G_\mathbb{Q}}(1)}.$$

Since ρ is transitive, its image is either S_3 or $A_3 = \langle(123)\rangle$. If $\operatorname{im}\rho = A_3$, then $\mathrm{Stab}_{G_F}(1) = \ker\rho$, so L_ρ is a Galois extension with Galois group C_3.

Suppose instead that $\operatorname{im}\rho = S_3$. Then

$$\mathrm{Stab}_{G_F}(1) = \rho^{-1}(\{\mathrm{id}, (23)\}),$$

which cuts out a non-Galois cubic extension $L_\rho/\mathbb{Q}$. Thus, isomorphism classes of S_3-cubic extensions correspond to equivalence classes of surjections $\rho : G_F \to S_3$, where two such surjections ρ_1, ρ_2 are equivalent if and only if there is some $\sigma \in S_3$ such that

$$\rho_2(f) = \sigma\rho_1(f)\sigma^{-1},$$

for all $f \in G_\mathbb{Q}$.

Example 3.27 (D_4-quartics)**.** By Lemma 3.23, quartic étale algebras over $\mathbb{Q}$ correspond to isomorphism classes of $G_\mathbb{Q}$-sets of size 4. Let $\rho : G_\mathbb{Q} \to \mathrm{Aut}(X)$ be such a $G_\mathbb{Q}$-set. We may assume that $X = \{1, 2, 3, 4\}$, so that $\rho : G_\mathbb{Q} \to S_4$. The étale algebra L_ρ is a field if and only if ρ is transitive, in which case we have

$$L_\rho \cong \overline{\mathbb{Q}}^{\mathrm{Stab}_{G_\mathbb{Q}}(1)}.$$

The extension L_ρ/F has Galois permutation group D_4 if and only if the permutation group induced by ρ is isomorphic to D_4. Since there is only one copy of D_4 in S_4, this is the case if and only if $\operatorname{im}\rho = D_4$. Thus, counting D_4-quartics is equivalent to counting S_4-equivalence classes of surjections $\rho : G_\mathbb{Q} \to D_4$, where two such surjections ρ_1, ρ_2 are equivalent if and only if there is some $\sigma \in S_4$ such that

$$\rho_2(f) = \sigma\rho_1(f)\sigma^{-1},$$

for all $f \in G_\mathbb{Q}$. Since the subgroup $D_4 \subseteq S_4$ is self-normalising, such a σ must in fact be in D_4, so we can forget about the embedding into S_4 and just count surjections $\rho : G_\mathbb{Q} \to D_4$, where we identify surjections that are related by conjugation by D_4.

Definition 3.28. Let k be a number field and let v be a place of k. Fix algebraic closures $\overline{k}$ and $\overline{k}_v$ of k and k_v, respectively. Also fix an embedding $\overline{k} \hookrightarrow \overline{k}_v$. There is a natural inclusion $G_{k_v} \to G_k$ given by restriction of maps. For any group homomorphism $\rho : G_k \to G$, write ρ_v for the composition

$$\rho_v : G_{k_v} \hookrightarrow G_k \xrightarrow{\rho} G.$$

Definition 3.29. Let K/k be a degree n extension of number fields, and let v be a place of k. The *completion of K over v* is the étale algebra K_v over k_v, given by

$$K_v = K \otimes_k k_v.$$

Let K/k be a degree n extension of number fields with Galois permutation group $G \subseteq S_n$. Let $\rho : G_k \to G$ be the surjective homomorphism corresponding to K (defined up to S_n-conjugation).

Lemma 3.30. *With notation as above, the following three étale algebras over k_v are isomorphic:*

1. *The completion K_v of K over v.*
2. *The product $\prod_{w|v} K_w$, where w ranges over the places of K lying over v.*
3. *The étale algebra L_{ρ_v} associated to the G_{k_v}-set $\rho_v : G_{k_v} \to S_n$.*

Proof. The equivalence of (1) and (2) is well-known; see e.g. [NS13, Chapter II, Proposition 8.3]. We now prove the equivalence of (2) and (3). For each $w \mid v$, we have a natural morphism of G_{k_v}-sets given by the restriction map

$$\mathrm{Hom}_{k_v}(K_w, \overline{k}_v) \to \mathrm{Hom}_k(K, \overline{k}).$$

This map is injective, and its image consists precisely of the embeddings $K \hookrightarrow \overline{k}$ that correspond to the place w of K. Thus, we can glue such maps to obtain an isomorphism of G_{k_v}-sets

$$\bigsqcup_{w \mid v} \mathrm{Hom}_{k_v}(K_w, \overline{k}_v) \to \mathrm{Hom}_k(K, \overline{k}).$$

The result follows from the natural isomorphism of G_{k_v}-sets

$$\mathrm{Hom}_{k_v}\Big(\prod_{w \mid v} K_w, \overline{k}_v\Big) \cong \bigsqcup_{w \mid v} \mathrm{Hom}_{k_v}(K_w, \overline{k}_v).$$

□

The reason we care about completions of K over places of k is that they give us the natural language for talking about local conditions. This is made precise in the following definition:

Definition 3.31. Let k be a number field. We define the key terminology for local conditions as follows:

(1) For a place v of k, a *degree n local condition at v* is a subset $\Sigma_v \subseteq \acute{\mathrm{E}}\mathrm{t}_{n/k_v}$.
(2) A *degree n collection of local conditions on k* is a collection $(\Sigma_v)_v$, where v ranges over the places of k.
(3) For a place v and a local condition Σ_v at v, a degree n field extension K/k *satisfies* the local condition Σ_v if the completion K_v is in Σ_v.
(4) A degree n extension K/k *satisfies* the collection $(\Sigma_v)_v$ of local conditions if it satisfies Σ_v for every place v of k.
(5) We call a collection of local conditions $(\Sigma_v)_v$ *acceptable* if, for all but finitely many (finite) v, the set Σ_v contains every $L \in \acute{\mathrm{E}}\mathrm{t}_{n/k_v}$ with $v(d_{L/k_v}) \leq 1$.
(6) Let $G = (G, \iota, X)$ be a permutation group. A collection Σ of local conditions is *G-compatible* if for each place v of k and each $L \in \Sigma_v$, the Galois permutation group $\mathrm{Gal}(L/k_v)$ is isomorphic to a sub-permutation group of G.

By Lemma 3.23, a degree n local condition at v is equivalent to a set Σ_v of S_n-conjugacy classes of homomorphisms $G_{k_v} \to S_n$. Given a group G and a subgroup $H \subseteq G$, write $Z_G(H)$ for the centraliser of H in G, defined to be

$$Z_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

Lemma 3.32. *Let N/F be a (possibly infinite) Galois extension of fields with Galois group G, and let $H \leq G$ be a (closed) subgroup. Let $L = N^H$. Let $X = G/H$ be the set of left cosets of H in G. Let ρ be the natural group homomorphism $\rho : G \to \mathrm{Aut}(X)$, associated to the left-action $g \cdot (aH) = (ga)H$. There is a natural bijection*

$$\Phi : \mathrm{Aut}(L/F) \to Z_{\mathrm{Aut}(X)}(\mathrm{im}\, \rho),$$

given by

$$\varphi \mapsto \big(aH \mapsto a\widetilde{\varphi}H\big),$$

where $\widetilde{\varphi}$ is an arbitrary lift of φ to $G = \mathrm{Gal}(N/F)$.

Proof. Our proof is a simplified version of [AMS15, Proof of Theorem 3.6]. Our rewritten version is considerably shorter, so we include it here.

It is easy to see that the map Φ is well-defined and injective. Let $f \in Z_{\mathrm{Aut}(X)}(\operatorname{im}\rho)$. By definition of the centraliser, for all g and a in G, we have

$$f(gaH) = gf(aH).$$

Let $n \in G$ be an element such that $f(gH) = nH$. Then, taking $a = 1$ in the above equation, we have

$$f(gH) = gnH$$

for all $g \in H$. It follows that for $h \in H$, we have

$$f(nhn^{-1}H) = f(H),$$

so $nhn^{-1} \in H$, since f is injective. Therefore, $nHn^{-1} = H$, so $n(L) = L$, and therefore $n|_L \in \mathrm{Aut}(L/F)$, and we have

$$\Phi(n|_L) = f$$

by definition of n. Therefore, Φ is surjective, so we are done. □

Lemma 3.33. *Let (ρ, X) be a transitive G_F-set of size n, and let L be the corresponding field extension. Then*

$$\#\,\mathrm{Aut}_{G_F\textbf{-Set}}((\rho, X)) = \#\,\mathrm{Aut}(L/F).$$

Proof. Write G_L for the subgroup $\mathrm{Gal}(\overline{F}/L)$ of G_F. Up to isomorphism of G_F-sets, we may assume that $X = G_F/G_L$, with the natural left-multiplication action. Let $\rho : G_F \to \mathrm{Aut}(X)$ be the group homomorphism associated to this action. By definition of morphisms in G_F**-Set**, we have

$$\mathrm{Aut}_{G_F\textbf{-Set}}((\rho, X)) = Z_{\mathrm{Aut}(X)}(\operatorname{im}\rho),$$

and the result follows from Lemma 3.32. □

3.3. **The algebraic Malle–Bhargava heuristics.** Throughout this thesis, we will always write Π_k to denote the set of places of a number field k. Moreover, we will write Π_k^{fin} and Π_k^{∞} for the nonarchimedean and archimedean places (i.e. finite and infinite), respectively. We start with the following elementary observation:

Lemma 3.34. *Let k be a number field or a p-adic field, let $\overline{k}$ be an algebraic closure of k, and let K/k be a finite field extension. Then*

$$\#\{L \subseteq \overline{k} : L \cong_k K\} = \frac{[K : k]}{\#\,\mathrm{Aut}(K/k)}.$$

Proof. Let $\widetilde{K} \subseteq \overline{k}$ be a normal closure of K over k. There is a natural, transitive left-action of $\mathrm{Gal}(\widetilde{K}/k)$ on the set

$$\{L \subseteq \overline{k} : L \cong_k K\},$$

where σ takes L to its set-theoretic image $\sigma(L)$. It is clear that, under this action,

$$\mathrm{Stab}(K) = \{\sigma \in \mathrm{Gal}(\widetilde{K}/k) : \sigma|_K \in \mathrm{Aut}(K/k)\}.$$

By Galois theory, each element of $\mathrm{Aut}(K/k)$ lifts to precisely $[\widetilde{K} : K]$ elements of $\mathrm{Aut}(\widetilde{K}/k)$, so

$$\#\,\mathrm{Stab}(K) = [\widetilde{K} : K] \cdot \#\,\mathrm{Aut}(K/k),$$

and the result follows by the Orbit-Stabiliser Theorem. □

Our proof of Lemma 3.34 is very similar to our proof of Lemma 2.3. In both cases, we find that the prevalence of an object is inversely proportional to its number of automorphisms. This motif appears often in arithmetic statistics. In [Bha07, Page 9], Bhargava writes “It is a common philosophy in number theory [...] that isomorphism classes of algebraic objects tend to occur [...] by weights that are inversely proportional to the cardinalities of their respective automorphism groups”. Inspired by this observation, Bhargava formulates the “Malle–Bhargava heuristics”, which underpin much of our work. We will state the most basic version of these heuristics in Heuristic 3.35, but first we need some notation.

Given a p-adic field F and a positive integer m, define

$$\text{Ét}_{n/F,m} = \{L \in \text{Ét}_{n/F} : v_F(d_{L/F}) = m\}.$$

Let D be an integer, let v be a place of $\mathbb{Q}$, and let $L \in \text{Ét}_{n/\mathbb{Q}_v}$. Call L *discriminant-compatible with* D if

$$\begin{cases} v(d_{L/\mathbb{Q}_v}) = v(D) & \text{if } v \text{ is finite,} \\ \operatorname{sign}(d_{L/\mathbb{R}}) = \operatorname{sign}(D) & \text{if } v \text{ is infinite.} \end{cases}$$

When v is infinite, this just means that

$$\operatorname{sign}(D) = (-1)^s,$$

where $L = \mathbb{R}^r \times \mathbb{C}^s$. Bhargava imagines that number fields occur randomly, so that the number of S_n-n-ics with a given discriminant is a random variable. Viewing the situation through this lens, he writes $E_n(D)$ for the expected number of S_n-n-ic number fields with discriminant equal to D. For a randomly selected such number field K, and for each place v of $\mathbb{Q}$, we expect the completion $K \otimes_{\mathbb{Q}} \mathbb{Q}_v$ to be a “random element” of

$$\{L \in \text{Ét}_{n/\mathbb{Q}_v} : \ L \text{ is discriminant-compatible with } D\},$$

where, in line with the philosophy above, the probability distribution is given by

$$\mathbb{P}(K \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong L) \propto \frac{1}{\# \operatorname{Aut}(L/\mathbb{Q}_v)}.$$

Thus, we expect $E_n(D)$ to be proportional to the sum

$$\sum_{\substack{L \in \text{Ét}_{n/\mathbb{Q}_v} \\ L \text{ discriminant-compatible} \\ \text{with } D}} \frac{1}{\# \operatorname{Aut}(L/\mathbb{Q}_v)}.$$

Moreover, we expect the completions $K \otimes_{\mathbb{Q}} \mathbb{Q}_v$ to be independent random variables for different places v. These assumptions lead us to the following heuristic:

Heuristic 3.35 (Algebraic Malle–Bhargava heuristics for $\mathbb{Q}$)**.** Let D be an integer. If $D \equiv 0, 1 \pmod 4$, then

$$E_n(D) = \Big(\sum_{\substack{L \in \text{Ét}_{n/\mathbb{R}} \\ \operatorname{sign}(D) = \operatorname{sign}(d_{L/\mathbb{R}})}} \frac{1}{\# \operatorname{Aut}(L/\mathbb{R})} \Big) \cdot \prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} \Big(\sum_{L \in \text{Ét}_{n/\mathbb{Q}_p, v_p(D)}} \frac{1}{\# \operatorname{Aut}(L/\mathbb{Q}_p)} \Big),$$

where the product is over finite primes. If $D \equiv 2, 3 \pmod 4$, then

$$E_n(D) = 0.$$

Define the functions $\overline{E}_n$ and $\overline{E}_{n,\infty}$ by

$$\overline{E}_n(D) = \prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} \Big(\sum_{L \in \text{Ét}_{n/\mathbb{Q}_p, v_p(D)}} \frac{1}{\# \operatorname{Aut}(L/\mathbb{Q}_p)} \Big)$$

and

$$\overline{E}_{n,\infty}(D) = m\big(\{L \in \text{Ét}_{n/\mathbb{R}} : \operatorname{sign}(D) = \operatorname{sign}(d_{L/\mathbb{R}})\}\big),$$

so that Heuristic 3.35 implies that

$$E_n(D) = \overline{E}_{n,\infty}(D) \cdot \overline{E}_n(D),$$

whenever $D \equiv 0, 1 \pmod 4$. Using Corollary 3.10, it is easy to see that $\overline{E}_n$ is multiplicative, in the sense that $\overline{E}_n(DD') = \overline{E}_n(D)\overline{E}_n(D')$ for coprime integers D and D'. Assume that X is some large positive real number. Let D be a randomly selected integer in $(-X, X)$. Since

$$\mathbb{P}_D\big(D \equiv 0, 1 \pmod 4\big) = \frac{1}{2},$$

the expectation of $E_n(D)$ is given by

$$\begin{aligned}
\mathbb{E}_D[E_n(D)] &= \frac{1}{2} \cdot \mathbb{E}_D[\overline{E}_{n,\infty}(D) \cdot \overline{E}_n(D)] \\
&= \frac{1}{2} \cdot \mathbb{E}_D\Big[\overline{E}_{n,\infty}(D) \cdot \prod_p \overline{E}_n(p^{v_p(D)})\Big] \\
&\approx \frac{1}{2} \cdot \mathbb{E}_D[\overline{E}_{n,\infty}(D)] \cdot \prod_p \mathbb{E}_D\Big[\overline{E}_n(p^{v_p(D)})\Big],
\end{aligned}$$

where the second equality comes form multiplicativity of $\overline{E}_n$, and the approximate equalities come from from approximate independence of the random variables $v_p(D)$ for different p. We have

$$\begin{aligned}
\mathbb{E}_D\Big[\overline{E}_n\Big(p^{v_p(D)}\Big)\Big] &= \sum_{a=0}^{\infty} \overline{E}_n(p^a) \cdot \mathbb{P}(v_p(D) = a) \\
&\approx \sum_{a=0}^{\infty} \Big(\Big(\frac{1}{p^a} - \frac{1}{p^{a+1}}\Big) \cdot \sum_{L \in \text{Ét}_{n/\mathbb{Q}_p,a}} \frac{1}{\#\operatorname{Aut}(L/\mathbb{Q}_p)}\Big) \\
&= \frac{p-1}{p} \cdot \sum_{L \in \text{Ét}_{n/\mathbb{Q}_p}} \frac{1}{\#\operatorname{Aut}(L/\mathbb{Q}_p) \cdot p^{v_p(d_{L/\mathbb{Q}_p})}} \\
&= m\big(\text{Ét}_{n/\mathbb{Q}_p}\big).
\end{aligned}$$

Similarly, we have

$$\mathbb{E}_D\Big[\overline{E}_{n,\infty}(D)\Big] = \frac{1}{2} \cdot m\big(\text{Ét}_{n/\mathbb{R}}\big).$$

Putting the above together, we have

$$\mathbb{E}_D[E_n(D)] = \frac{1}{4} \cdot \prod_{v \in \Pi_{\mathbb{Q}}} m\big(\text{Ét}_{n/\mathbb{Q}_v}\big).$$

The vague definition of $E_n(D)$ suggests that we should have approximate equality

$$N_{\mathbb{Q},n}(X) \approx \sum_{D \in (-X,X)} E_n(D) \approx 2X \cdot \mathbb{E}_D[E_n(D)],$$

so we obtain the following conjecture:

Conjecture 3.36. *For all n, we have*

$$\lim_{X \to \infty} \frac{N_{\mathbb{Q},n}(X)}{X} = \frac{1}{2} \cdot \prod_{v \in \Pi_{\mathbb{Q}}} m\big(\text{Ét}_{n/\mathbb{Q}_v}\big).$$

We can actually go much further than Conjecture 3.36, extending the base field to an arbitrary number field k and counting S_n-n-ics with local conditions. To that end, let k be a number field and let $\Sigma = (\Sigma_v)_v$ be an acceptable degree n collection of local conditions on k, in the sense of Definition 3.31.

Let D be an ideal of $\mathcal{O}_k$. Again taking the view that number fields occur randomly, define $E_{k,n}(D;\Sigma)$ to be the expected number of S_n-n-ic extensions K/k such that K satisfies Σ and $\operatorname{disc}(K/k) = D$. By the same reasoning we used to justify Heuristic 3.35, we obtain the following heuristic:

Heuristic 3.37 (Algebraic Malle–Bhargava heuristics for arbitrary base number field)**.** Let Σ be an acceptable degree n collection of local conditions on k, and let D be an ideal of $\mathcal{O}_k$. Then $E_{k,n}(D;\Sigma)$ is the product of the following two quantities:

(1)
$$\frac{1}{2}\cdot \prod_{v\in\Pi_k^\infty}\Big(\sum_{L\in\Sigma_v}\frac{1}{\#\operatorname{Aut}(L/k_{\mathfrak{p}})}\Big).$$

(2)
$$\prod_{\mathfrak{p}\in\Pi_k^{\mathrm{fin}}}\Big(\sum_{\substack{L\in\Sigma_{\mathfrak{p}}\\ v_{\mathfrak{p}}(d_{L/k_{\mathfrak{p}}})=v_{\mathfrak{p}}(D)}}\frac{1}{\#\operatorname{Aut}(L/k_{\mathfrak{p}})}\Big).$$

The first quantity in Heuristic 3.37 is just
$$\frac{1}{2}\cdot\prod_{v\in\Pi_k^\infty} m(\Sigma_v).$$

As before, write $\overline{E}_{k,n}(D;\Sigma)$ for the product
$$\prod_{\mathfrak{p}\in\Pi_k^{\mathrm{fin}}}\Big(\sum_{\substack{L\in\Sigma_{\mathfrak{p}}\\ v_{\mathfrak{p}}(d_{L/k_{\mathfrak{p}}})=v_{\mathfrak{p}}(D)}}\frac{1}{\#\operatorname{Aut}(L/k_{\mathfrak{p}})}\Big).$$

Again, we may use Corollary 3.10 to see that
$$\overline{E}_{k,n}(DD';\Sigma) = \overline{E}_{k,n}(D;\Sigma)\cdot\overline{E}_{k,n}(D';\Sigma)$$
for any pair of coprime ideals D and D'.

Lemma 3.38. *Let k be a number field, let X be a large positive real number, and let D be a uniformly randomly selected ideal of $\mathcal{O}_k$ with $\operatorname{Nm}(D)\le X$. For each nonzero ideal I of $\mathcal{O}_k$, we have*
$$\lim_{X\to\infty}\mathbb{P}(D\subseteq I) = \frac{1}{\operatorname{Nm}(I)}.$$

Proof. Let S be the set of all ideals of $\mathcal{O}_k$, let I be a nonzero ideal, and let
$$S_I = \{J\in S : J\subseteq I\}.$$

For each positive real number T, define
$$S_{\le T} = \{J\in S : \operatorname{Nm}(J)\le T\},$$
and define $S_{I,\le T} = S_I\cap S_{\le T}$. It is well-known that

$$\lim_{T\to\infty}\frac{\#S_{\le T}}{T} = \operatorname{Res}_{s=1}\zeta_k(s). \tag{2}$$

There is a bijection
$$\varphi : S\to S_I,\quad J\mapsto JI,$$

It is easy to see that $\mathrm{Nm}(\varphi(J)) \leq X$ if and only if $\mathrm{Nm}(J) \leq \frac{X}{\mathrm{Nm}(I)}$, so

$$\#S_{I,\leq X} = \#S_{\leq \frac{X}{\mathrm{Nm}(I)}}. \tag{3}$$

We have

$$\mathbb{P}(D \subseteq I) = \frac{\#S_{I,\leq X}}{\#S_{\leq X}},$$

and the result follows from Equations (2) and (3). □

Corollary 3.39. *Let k be a number field, let I and J be coprime ideals of $\mathcal{O}_k$, let X be a positive real number, and let D be a uniformly randomly selected ideal of $\mathcal{O}_k$ with* $\mathrm{Nm}(D) \leq X$*. The events $\{D \subseteq I\}$ and $\{D \subseteq J\}$ are "approximately independent", in the sense that*

$$\lim_{X\to\infty} \frac{\mathbb{P}(\{D \subseteq I\} \cap \{D \subseteq J\})}{\mathbb{P}(D \subseteq I) \cdot \mathbb{P}(D \subseteq J)} = 1.$$

Proof. This follows easily from Lemma 3.38. □

Let k be a number field, let X be a large positive real number, and let D be a uniformly randomly selected ideal of $\mathcal{O}_k$ with $\mathrm{Nm}(D) \leq X$. It follows from Corollary 3.39 that the valuations $v_\mathfrak{p}(D)$ are approximately independent for different primes $\mathfrak{p}$, so Heuristic 3.37 implies

$$\begin{aligned}\mathbb{E}_D[E_{k,n}(D;\Sigma)] &= \mathbb{E}_D\Big[\frac{1}{2} \cdot \prod_{v\in\Pi_k^\infty} m(\Sigma_v) \cdot \prod_{\mathfrak{p}\in\Pi_k^{\mathrm{fin}}} \overline{E}_{k,n}(\mathfrak{p}^{v_\mathfrak{p}(D)};\Sigma)\Big] \\ &\approx \frac{1}{2} \cdot \prod_{v\in\Pi_k^\infty} m(\Sigma_v) \cdot \prod_{\mathfrak{p}\in\Pi_k^{\mathrm{fin}}} \mathbb{E}_D\Big[\overline{E}_{k,n}(\mathfrak{p}^{v_\mathfrak{p}(D)};\Sigma)\Big].\end{aligned}$$

Moreover, for each finite prime $\mathfrak{p}$ of k, Lemma 3.38 implies that

$$\begin{aligned}\mathbb{E}_D[\overline{E}_{k,n}(\mathfrak{p}^{v_\mathfrak{p}(D)};\Sigma)] &= \sum_{a=0}^{\infty} \overline{E}_{k,n}(\mathfrak{p}^a;\Sigma) \cdot \mathbb{P}(v_\mathfrak{p}(D) = a) \\ &= \frac{\mathrm{Nm}\,\mathfrak{p} - 1}{\mathrm{Nm}\,\mathfrak{p}} \cdot \sum_{a=0}^{\infty} \sum_{\substack{L\in\Sigma_\mathfrak{p} \\ v_\mathfrak{p}(d_{L/k_\mathfrak{p}})=a}} \frac{1}{\#\,\mathrm{Aut}(L/k_\mathfrak{p}) \cdot (\mathrm{Nm}\,\mathfrak{p})^a} \\ &= \frac{\mathrm{Nm}\,\mathfrak{p} - 1}{\mathrm{Nm}\,\mathfrak{p}} \cdot \sum_{L\in\Sigma_\mathfrak{p}} \frac{1}{\#\,\mathrm{Aut}(L/k_\mathfrak{p}) \cdot (\mathrm{Nm}\,\mathfrak{p})^{v_\mathfrak{p}(d_{L/k_\mathfrak{p}})}} \\ &= m(\Sigma_\mathfrak{p}).\end{aligned}$$

Write $N_{k,n}(X;\Sigma)$ for the number of S_n-n-ic extensions K/k such that $\mathrm{Nm}(\mathrm{disc}(K/k)) \leq X$ and K satisfies Σ. Then

$$\begin{aligned}N_{k,n}(X;\Sigma) &\sim \sum_{D:\mathrm{Nm}(D)\leq X} E_{k,n}(D;\Sigma) \\ &\sim \#\{D : \mathrm{Nm}(D) \leq X\} \cdot \mathbb{E}_D[E_{k,n}(D;\Sigma)] \\ &\sim \#\{D : \mathrm{Nm}(D) \leq X\} \cdot \frac{1}{2} \cdot \prod_{v\in\Pi_k} m(\Sigma_v).\end{aligned}$$

Since

$$\lim_{X\to\infty} \frac{\#\{D : \mathrm{Nm}(D) \leq X\}}{X} = \mathrm{Res}_{s=1}\,\zeta_k(s),$$

we obtain the following conjecture:

Conjecture 3.40. *Let n be an integer, let k be a number field, and let Σ be an acceptable degree n collection of local conditions on k. Then we have*

$$\lim_{X\to\infty} \frac{N_{k,n}(X;\Sigma)}{X} = \frac{1}{2}\cdot \operatorname{Res}_{s=1}\zeta_k(s)\cdot \prod_{v\in\Pi_k} m(\Sigma_v).$$

3.4. **The analytic Malle–Bhargava heuristics.** The analytic MBH is a more general set of conjectures, from which Conjecture 3.40 arises as a special case. Let $G = (G, \iota, [n])$ be a transitive permutation group, and let Σ be a G-compatible collection of local conditions on k. Recall from Definition 3.24 that a G-extension of k is an étale algebra K/k whose Galois permutation group is isomorphic to G, and that we write $(G{-}\mathbf{Ext})_k$ for the set of isomorphism classes of such extensions. Define

$$N_{k,G}(X;\Sigma) = \sum_{\substack{K\in(G-\mathbf{Ext})_k\\ K \text{ satisfies } \Sigma\\ \operatorname{Nm}(\operatorname{disc}(K/k))\le X}} \frac{1}{\#\operatorname{Aut}(K/k)}.$$

Remark 3.41. If the action of G on $[n]$ is transitive, then $N_{k,G}(X;\Sigma)$ counts field extensions with Galois closure group G. Otherwise, it counts étale algebras. Thus, for arbitrary permutation groups G, the counting function $N_{k,G}(X;\Sigma)$ is very general.

For each ideal D of $\mathcal{O}_k$, write

$$n_{k,G}(D;\Sigma) = \sum_{\substack{K\in(G-\mathbf{Ext})_k\\ K \text{ satisfies } \Sigma\\ \operatorname{disc}(K/k)=D}} \frac{1}{\#\operatorname{Aut}(K/k)}.$$

Let $\xi_k(G,\Sigma,s)$ be the Dirichlet series

$$\xi_k(G,\Sigma,s) = \sum_D \frac{n_{k,G}(D;\Sigma)}{\operatorname{Nm}(D)^s}.$$

For each place v of k, define

$$M_v(s;\Sigma_v) = \begin{cases} \sum_{L\in\Sigma_\mathfrak{p}} \frac{1}{\#\operatorname{Aut}(L/k_\mathfrak{p})\cdot(\operatorname{Nm}\mathfrak{p})^{v_\mathfrak{p}(d_{L/k_\mathfrak{p}})s}} & \text{if } v=\mathfrak{p} \text{ is finite,}\\ \sum_{L\in\Sigma_v} \frac{1}{\#\operatorname{Aut}(L/k_v)} & \text{if } v \text{ is infinite.}\end{cases}$$

Remark 3.42. Bhargava defines $M_v(s;\Sigma_v)$ in the context where Σ_v is a set of S_n-conjugacy classes of homomorphisms $\rho : G_{k_v} \to G$. By the work in Section 3.2, our definition is equivalent to Bhargava's.

For an as yet unspecified constant $C(k,G)$, define

$$M_k(s;\Sigma) = C(k,G)\cdot \prod_v M_v(s;\Sigma_v),$$

where the product is over all places of k, both finite and infinite.

Definition 3.43. We define the following two terms:

(1) A *special Dirichlet series* is a Dirichlet series $f(s)$, such that the following three statements are true:
- All coefficients of $f(s)$ are nonnegative.
- There is some $s_0 > 0$ such that f converges in the open right-half plane $\operatorname{Re}(s) > s_0$.
- For the same s_0, the function f has a meromorphic continuation to the closed right-half plane $\operatorname{Re}(s) \ge s_0$.

(2) Let f and g be special Dirichlet series. We say that f and g are *asymptotically equivalent* if they have the same rightmost pole $s_0 \in \mathbb{R}$, and the order of the pole of $f - g$ at $s = s_0$ is strictly lower than the order of the pole of f or g at $s = s_0$.

Theorem 3.44 (Tauberian Theorem). *Let $f(s) = \sum_n a_n n^{-s}$ be a special Dirichlet series with rightmost pole of order k at $s = s_0$, for some $s_0 \in \mathbb{R}$ with $s_0 > 0$. Then*

$$\sum_{n \leq X} a_n \sim \frac{\lim_{s \to s_0}((s - s_0)^k f(s))}{s_0(k-1)!} X^{s_0} (\log X)^{k-1}.$$

Proof. This is [Woo16, Theorem 7.1]. □

Corollary 3.45. *Let $f(s) = \sum_n a_n n^{-s}$ and $g(s) = \sum_n b_n n^{-s}$ be asymptotically equivalent special Dirichlet series. Then*

$$\sum_{n \leq X} a_n \sim \sum_{n \leq X} b_n.$$

Proof. This follows easily from Theorem 3.44. □

Heuristic 3.46 (Analytic Malle–Bhargava heuristics). Given a positive integer n, a finite permutation group $G \subseteq S_n$, and a base field k, there exists a value of $C(k, G)$ such that, for all suitably nice collections Σ of G-compatible local conditions, the functions $M_k(s; \Sigma)$ and $\xi_k(G, \Sigma, s)$ are asymptotically equivalent special Dirichlet series.

Combining the analytic Malle–Bhargava heuristics with Theorem 3.44, we obtain the following conjecture:

Conjecture 3.47 (Essentially Malle's conjecture). *Let k be a number field and let G be a finite permutation group. There exist constants $a(k, G), b(k, G)$, and $c(k, G)$, with $c(k, G) > 0$ and $b(k, G) \geq 1$, such that*

$$N_{k,G}(X) \sim c(k, G) \cdot X^{1/a(k,G)} \cdot (\log X)^{b(k,G)-1}.$$

Lemma 3.48. *Let k be a number field and let $M(s)$ be a Dirichlet series with an Euler product $M(s) = \prod_{\mathfrak{p}} M_{\mathfrak{p}}(s)$, indexed by finite primes of k. Suppose that $M_{\mathfrak{p}}(s) > 0$ for all $\mathfrak{p}$ and for all s with $\mathrm{Re}(s) > 0$, and that there is a positive real number A such that*

$$1 + \frac{1}{\mathrm{Nm}(\mathfrak{p})^s} \leq M_{\mathfrak{p}}(s) \leq 1 + \frac{1}{\mathrm{Nm}(\mathfrak{p})^s} + \frac{A}{\mathrm{Nm}(\mathfrak{p})^{2s}},$$

for all real $s > 0$ and all but finitely many primes $\mathfrak{p}$. Then $M(s)$ has a simple pole at $s = 1$.

Proof. Without loss of generality, we may assume that the inequality

$$1 + \frac{1}{\mathrm{Nm}(\mathfrak{p})^s} \leq M_{\mathfrak{p}}(s) \leq 1 + \frac{1}{\mathrm{Nm}(\mathfrak{p})^s} + \frac{A}{\mathrm{Nm}(\mathfrak{p})^{2s}},$$

holds for all primes $\mathfrak{p}$. Since we have

$$\zeta_k(s) = \prod_{\mathfrak{p}} (1 + \mathrm{Nm}(\mathfrak{p})^{-s} + \mathrm{Nm}(\mathfrak{p})^{-2s} + \ldots),$$

it is easy to see that

$$\prod_{\mathfrak{p}} (1 - \mathrm{Nm}(\mathfrak{p})^{-2s}) \leq \frac{M(s)}{\zeta_k(s)} \leq \prod_{\mathfrak{p}} (1 + A\,\mathrm{Nm}(\mathfrak{p})^{-2s}). \tag{4}$$

We have

$$\begin{aligned}\prod_{\mathfrak{p}}(1+A\,\mathrm{Nm}(\mathfrak{p})^{-2}) &\leq \prod_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}\prod_{\mathfrak{p}\mid p}(1+Ap^{-2})\\ &\leq \Big(\prod_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}(1+Ap^{-2})\Big)^{[k:\mathbb{Q}]},\end{aligned}$$

and similarly

$$\prod_{\mathfrak{p}}(1-\mathrm{Nm}(\mathfrak{p})^{-2}) \geq \Big(\prod_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}(1-p^{-2})\Big)^{[k:\mathbb{Q}]}.$$

We also have

$$\log\prod_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}(1+Ap^{-2}) \leq \sum_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}\frac{A}{p^2} < \infty$$

and

$$\log\prod_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}(1-p^{-2}) \geq -\sum_{p\in\Pi_{\mathbb{Q}}^{\mathrm{fin}}}\frac{1}{p^2} > -\infty,$$

so both products in Equation (4) converge to positive values when $s=1$. Therefore, the ratio $\frac{M(s)}{\zeta_k(s)}$ converges to a finite, nonzero value as $s\to 1$, and the result follows. □

Let Σ be an acceptable collection of local conditions on k. It follows from Lemma 3.12 that there is a positive real number A such that, for all but finitely many primes $\mathfrak{p}$ of k, we have

$$1+\frac{1}{\mathrm{Nm}(\mathfrak{p})^s} \leq M_{\mathfrak{p}}(s;\Sigma) \leq 1+\frac{1}{\mathrm{Nm}(\mathfrak{p})^s}+\frac{A}{\mathrm{Nm}(\mathfrak{p})^{2s}}.$$

Lemma 3.48 tells us that $M_k(s;\Sigma)$ has a simple pole at $s=1$. Moreover, Part (3) of Lemma 3.12 tells us that

$$\begin{aligned}\mathrm{Res}_{s=1}M_k(s;\Sigma) &= C(k,G)\cdot\prod_{v\in\Pi_k^{\infty}}m(\Sigma_v)\cdot\lim_{s\to 1}\Big((s-1)\prod_{\mathfrak{p}\in\Pi_k^{\mathrm{fin}}}\widetilde{m}(\mathrm{Nm}(\mathfrak{p})^s;\Sigma_v)\Big)\\ &= C(k,G)\cdot\prod_{v\in\Pi_k}m(\Sigma_v)\cdot\lim_{s\to 1}\Big((s-1)\prod_{\mathfrak{p}\in\Pi_k^{\mathrm{fin}}}\frac{1}{1-\mathrm{Nm}(\mathfrak{p})^{-s}}\Big)\\ &= C(k,G)\cdot\mathrm{Res}_{s=1}\zeta_k(s)\cdot\prod_{v\in\Pi_k}m(\Sigma_v).\end{aligned}$$

If Heuristic 3.46 is true, then Theorem 3.44 implies the following conjecture:

Conjecture 3.49. *Let $G\subseteq S_n$ be a permutation group and let Σ be degree n collection of local conditions, such that Σ is both G-compatible and acceptable. There is a constant $C(k,G)$, determined by k and G, such that*

$$N_{k,G}(X;\Sigma)\sim C(k,G)\cdot\mathrm{Res}_{s=1}\zeta_k(s)\cdot\prod_{v\in\Pi_k}m(\Sigma_v)\cdot X.$$

Lemma 3.50. *Let $G\subseteq S_n$ be a permutation group. For each v, let Σ_v be the set of étale algebras $L\in\acute{\mathrm{E}}\mathrm{t}_{n/k_v}$ such that $\mathrm{Gal}(L/k_v)$ is isomorphic to a sub-permutation group of G. Then Σ is acceptable if and only if G contains a transposition.*

Proof. Let $\mathfrak{p}$ be a finite prime of k. Without loss of generality, we may assume that $\mathfrak{p}$ does not divide any integer e with $e\leq n$, so that any degree n étale algebra over $k_{\mathfrak{p}}$ is tamely ramified. By Lemma 3.11, the degree n étale algebras $L/k_{\mathfrak{p}}$ with $v(d_{L/k_{\mathfrak{p}}})\leq 1$ are precisely those with splitting symbols $(11\dots11)$ and $(1^21\dots11)$, whose Galois permutation groups are respectively trivial and generated by a single transposition. □

We obtain the following consequence of Conjecture 3.49 and Lemma 3.50:

Conjecture 3.51. *Let $G \subseteq S_n$ be a permutation group containing a transposition. Then there is a constant $c(k,G)$, determined by k and G, with*

$$N_{k,G}(X) \sim c(k,G) \cdot X.$$

The following result, which is [BW07, Theorem 2], shows that we really need the transposition in G:

Theorem 3.52 (Bhargava–Wood)**.** *Let $S_3 \subseteq S_6$ be the permutation group where S_3 acts on itself by left-multiplication. There is a positive constant c such that*

$$N_{k,S_3\subseteq S_6}(X) \sim cX^{1/3}.$$

Recall that, given a collection Σ of local conditions on k, the special case $G = (S_n \subseteq S_n)$ recovers the notion of an S_n-n-ic extension, and we write $N_{k,n}(X;\Sigma)$ as shorthand for $N_{k,S_n\subseteq S_n}(X;\Sigma)$. The following result is a special case of [BSW15, Theorem 3]:

Theorem 3.53 (Bhargava–Shankar–Wang)**.** *Let n be a positive integer with $n \leq 5$. In the case $G = S_n$, Conjecture 3.49 is true with $C(k,G) = \frac{1}{2}$. That is, for any acceptable degree n collection of local conditions Σ, we have*

$$N_{k,n}(X;\Sigma) \sim \frac{1}{2} \cdot \operatorname{Res}_{s=1} \zeta_k(s) \cdot \prod_{v\in\Pi_k} m(\Sigma_v) \cdot X.$$

More generally, we have the following conjecture:

Conjecture 3.54 (Bhargava)**.** *Let n be any positive integer with $n \geq 2$, and let Σ be an acceptable degree n family of local conditions. Then we have*

$$N_{k,n}(X;\Sigma) \sim \frac{1}{2} \cdot \operatorname{Res}_{s=1} \zeta_k(s) \cdot \prod_{v\in\Pi_k} m(\Sigma_v) \cdot X.$$

4. Parametrising rings and counting integral points

According to Wikipedia, Bhargava's 2014 Fields Medal was for "developing powerful new methods in the geometry of numbers, which he applied to count rings of small rank and to bound the average rank of elliptic curves". These powerful methods are known colloquially as "Bhargavology", and they form the crux of the proof of Theorem 3.53. The remainder of Section 3 is devoted to a high-level sketch of the key ideas in the proof. Most writing about a difficult topic will exist somewhere on the following spectrum:

$$\{\text{Easy to understand but missing details}\} \longleftrightarrow \{\text{Hard but including all details}\}.$$

Of course, the right-hand limit of this spectrum exists in the original paper [BSW15], as well as in Bhargava's earlier work in [Bha04], [Bha05], [Bha08], and [Bha10]. On the other hand, there are several excellent expositions more in the middle/middle-left of the spectrum, such as [BST13, Sections 2-5 and Section 8] and [Woo16, Section 11]. The latter two references explain the case of cubic number fields over $\mathbb{Q}$.

We endeavour to push a little further to the left of this spectrum, including fewer details and emphasising the big picture. We do not claim that our exposition is in any way better than that in [BST13] or [Woo16]. Both references are really excellent, and we merely hope that it is useful to have an additional viewpoint with slightly different emphasis. We especially recommend Pages 323-334 of [Woo16], which give an exceptionally clear explanation of the lattice point counting techniques. In addition to the two references we have given, the reader may wish to attempt Problems 47-80 of the 2014 Arizona Winter School, which walk through the same special case in an exercise-driven manner.

Final appeal: This stuff is just hard! Most people will probably need to try to read Bhargava, then try to read several different expository works, then try to read Bhargava again, and flit about chaotically for a while before it starts to make sense.

4.1. **Parametrising cubic rings: Delone–Fadeev and Davenport–Heilbronn.** By an *integral binary cubic form* we mean a homogeneous cubic polynomial $f(x,y) \in \mathbb{Z}[x,y]$. Write $\mathrm{Sym}^3(\mathbb{Z}^2)$ for the set of integral binary cubic forms.

Definition 4.1. A *cubic ring* is a ring R that is a free $\mathbb{Z}$-module of rank 3. The *discriminant* $\mathrm{disc}(R)$ of a cubic ring R is the determinant of the bilinear form $t_R : R \times R \to \mathbb{Z}$, where $t_R(\alpha, \beta)$ is the trace of the $\mathbb{Z}$-linear map $\alpha\beta : R \to R$. The discriminant and trace and both integers.

Write $\mathbf{CubRing}(\mathbb{Z})$ for the category of cubic rings over $\mathbb{Z}$. We will occasionally make reference to the categories of cubic rings over other base rings, such as $\mathbf{CubRing}(\mathbb{Z}_p)$ and $\mathbf{CubRing}(\mathbb{F}_p)$. These are defined analogously, as full subcategories of $\mathbb{Z}_p$-algebras and $\mathbb{F}_p$-algebras, respectively.

For a matrix $g \in \mathrm{GL}_2(\mathbb{Z})$ with coefficients $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we define the integral binary cubic form $g \cdot f$ by

$$(g \cdot f)(x,y) = \frac{1}{\det(g)} \cdot f((x,y)g) = \frac{1}{ad-bc} \cdot f(ax+cy, bx+dy).$$

The map $f \mapsto g \cdot f$ gives a natural left-action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{Sym}^3(\mathbb{Z}^2)$, since for $g, h \in \mathrm{GL}_2(\mathbb{Z})$ and $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$ we have

$$\begin{aligned}(g \cdot (h \cdot f))(x,y) &= \frac{1}{\det g}(h \cdot f)((x,y)g) \\ &= \frac{1}{\det(g)} \cdot \frac{1}{\det(h)} \cdot f((x,y)gh) \\ &= ((gh) \cdot f)(x,y).\end{aligned}$$

Given a binary cubic form

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3,$$

we can define a cubic ring $R(f)$ explicitly as the free abelian group $\mathbb{Z} \oplus \mathbb{Z}\omega \oplus \mathbb{Z}\theta$, with multiplication induced by

$$\begin{aligned}\omega\theta &= -ad, \\ \omega^2 &= -ac - b\omega + a\theta, \\ \theta^2 &= -bd - d\omega + c\theta.\end{aligned}$$

One can check that the resulting multiplication is associative, so that $R(f)$ is actually a ring. For $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$ and $g \in \mathrm{GL}_2(\mathbb{Z})$, it turns out that $R(g \cdot f) \cong R(f)$. Intuitively, this is because the action of g corresponds to changing basis in $R(f)$.

The construction of $R(f)$ is quite opaque. The following lemma gives a more natural interpretation:

Lemma 4.2. *Let $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$, and let ω and θ be as in the definition of $R(f)$. Then we have*

$$f(\omega, a) = f(-d, \theta) = 0.$$

Proof. This follows from the definition of $R(f)$. □

In other words, Lemma 4.2 tells us that $R(f)$ is obtained from $\mathbb{Z}$ by adjoining roots of $f(x, y)$.

Theorem 4.3 (Delone–Fadeev correspondence)**.** *The following four statements are true:*

1. *The map $f \mapsto R(f)$ gives a well-defined bijection*
$$\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{Sym}^3(\mathbb{Z}^2) \to \mathbf{CubRing}(\mathbb{Z})/\cong,$$
between $\mathrm{GL}_2(\mathbb{Z})$-orbits on $\mathrm{Sym}^3(\mathbb{Z}^2)$ and isomorphism classes of cubic rings over $\mathbb{Z}$.
2. *We have $\mathrm{disc}(R(f)) = \mathrm{disc}(f)$, for all $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$.*
3. *The ring $R(f)$ is an integral domain if and only if f is irreducible over $\mathbb{Q}$.*
4. *There is a natural group isomorphism*
$$\mathrm{Aut}(R(f)) \cong \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(f).$$

Proof. For (1), the original reference is [DF64, Section 15]. However, Delone and Fadeev only work with cubic rings arising as orders in number fields; a reference for our slightly more general setting is [BST13, Theorem 9]. The other statements are [BST13, Propositions 10-12]. □

Definition 4.4. A cubic ring R is *maximal* if it is not isomorphic to a proper subring of any other cubic ring.

Lemma 4.5. *Let R be a cubic ring. The following statements are equivalent:*

1. *R is isomorphic to the ring of integers of a number field.*
2. *R is maximal and an integral domain.*

Proof. Let R be a cubic ring and an integral domain. Then $R = R(f)$ for an irreducible integral binary cubic form $f(x, y)$. Lemma 4.2 tells us that R is isomorphic to an order in the number field

$$K_f := \frac{\mathbb{Q}[t]}{(f(t, 1))}.$$

If R is a maximal cubic ring, then it is clearly a maximal order in K_f, hence the ring of integers of K_f. Suppose conversely that R is isomorphic to the ring of integers of K_f. Let R' be another cubic ring such that there is an embedding $R \subseteq R'$. Then $R' = R(g)$ for an irreducible binary cubic form g. But then we have a commutative diagram

$$\begin{tikzcd} R(f) \arrow[r, hook] \arrow[d, hook] & K_f \arrow[d, "\cong"] \\ R(g) \arrow[r, hook] & K_g \end{tikzcd}$$

so in fact $R = R'$. □

For each rational prime p, let $\mathcal{U}_p$ be the set of $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$ such that the following two statements are true:

(1) f is not a multiple of p.
(2) For every binary cubic form $ax^3+bx^2y+cxy^2+dy^3$ in the orbit $\mathrm{GL}_2(\mathbb{Z})\cdot f$ of f, either $p^2 \nmid a$ or $p \nmid b$.

Theorem 4.6 (Davenport–Heilbronn correspondence)**.** *Let $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$. Then $R(f)$ is maximal if and only if $f \in \bigcap_p \mathcal{U}_p$.*

Proof. The original reference is [DH71, Proposition 4]. Our contemporary reference is [BST13, Theorem 14]. □

Write $\mathcal{U} = \bigcap_p \mathcal{U}_p$, and write $\mathcal{U}^{\mathrm{irred}}$ for the set of irreducible elements of $\mathcal{U}$. By Theorem 4.3, Part 3, and Theorem 4.6, the orbits $\mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{U}^{\mathrm{irred}}$ correspond to rings that are both maximal cubic rings and integral domains, hence to cubic number fields by Lemma 4.5. By Theorem 4.3, Part 2, it follows that the number of cubic number fields $K/\mathbb{Q}$ with $|\mathrm{disc}(K/\mathbb{Q})| \leq X$ is equal to

$$N\big(X;\mathcal{U}^{\mathrm{irred}}\big) = \#\big\{[x] \in \mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{U}^{\mathrm{irred}} : |\mathrm{disc}(x)| \leq X\big\}.$$

Remark 4.7. We actually care about S_3-cubics. By Theorem 4.3, Part (4), this requires us to specify the additional constraint that $\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x) = 1$. It will turn out that this is usually the case, so that the count $N\big(X;\mathcal{U}^{\mathrm{irred}}\big)$ is asymptotic to $N_{\mathbb{Q},3}(X)$.

One final consideration is that of local conditions. For each prime p, there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Sym}^3(\mathbb{Z}^2) \arrow[r, "R(-)"] \arrow[d, hook] & \mathbf{CubRing}(\mathbb{Z}) \arrow[d, "-\otimes_{\mathbb{Z}}\mathbb{Z}_p"] \\
\mathrm{Sym}^3(\mathbb{Z}_p^2) \arrow[r, "R(-)"'] & \mathbf{CubRing}(\mathbb{Z}_p)
\end{tikzcd}$$

where the horizontal maps are the Delone–Fadeev correspondence (which is also valid for cubic rings over $\mathbb{Z}_p$). It follows that for a binary cubic form $f \in \mathcal{U}^{\mathrm{irred}}$, corresponding to a field K, the étale algebra K_p is the extension of $\mathbb{Q}_p$ corresponding to the binary cubic form $f \in \mathrm{Sym}^3(\mathbb{Z}_p^2)$. Moreover, it follows from Krasner's Lemma and Lemma 4.2 that[1] the isomorphism class of K_p is determined by $f \pmod{p^m}$ for some positive integer m. Thus, for the full picture, we will consider counts of the form

$$N\big(X;S^{\mathrm{irred}}\big) = \#\big\{[x] \in \mathrm{GL}_2(\mathbb{Z})\backslash S^{\mathrm{irred}} : |\mathrm{disc}(x)| \leq X\big\},$$

for $\mathrm{GL}_2(\mathbb{Z})$-invariant sets $S \subseteq \mathrm{Sym}^3(\mathbb{Z}^2)$ that are *defined by congruence conditions*, in the following sense:

Definition 4.8. Let p be a prime. A set $S_p \subseteq \mathrm{Sym}^3(\mathbb{Z}^2)$ is *defined by p-congruence* if there is some positive integer m such that, for all $f \in \mathrm{Sym}^3(\mathbb{Z}^2)$, membership of S_p is determined by the congruence class $f \pmod{p^m}$. A set $S \subseteq \mathrm{Sym}^3(\mathbb{Z}^2)$ is *defined by congruence conditions* if it is of the form

$$S = \bigcap_p S_p,$$

where for each p, the set S_p is defined by p-congruence.

[1] More properly, for a given cubic étale algebra $L/\mathbb{Q}_p$, there will be a positive integer m_L such that whether $K_p \cong L$ is determined by $f \pmod{p^{m_L}}$. Then the isomorphism class of K_p is determined by $f \pmod{p^m}$, where $m = \max_L\{m_L\}$, which exists since there are finitely many isomorphism classes of cubic étale algebras $L/\mathbb{Q}_p$.

In the case of cubic number fields, we have defined the class of counting problems $N\big(X; S^{\text{irred}}\big)$ we are interested in. As mentioned above, this cubic problem is solved in full detail in e.g. [BST13]; rather than reproducing that work here, we will sketch some of the key ideas. One advantage of our sketch is that it gives equally good insight into counting quartic and quintic number fields, as is done in [BSW15]. We will still work in a simpler context than [BSW15]. In that paper, the authors parametrise low-rank rings over *an arbitrary base ring* (see [BSW15, Section 3]), allowing them to count cubic, quartic, and quintic extensions of an arbitrary number field, as in Theorem 3.53. In our treatment, we will restrict ourselves to the base field $\mathbb{Q}$.

4.2. **Parametrising quartics and quintics: Bhargava.** Above, we saw how the Delone–Fadeev correspondence parametrises cubic rings, and how the Davenport–Heilbronn correspondence then refines the result to parametrise cubic number fields. One of Bhargava's many important contributions is the development of analogous parametrisations for quartic and quintic rings and fields. In this shorter subsection, we will state these parametrisations and see how they fit into a wider counting framework.

In general, we will have a reductive group G over $\mathbb{Z}$ and a representation V of G. Taking integer points yields a concrete group $G_{\mathbb{Z}}$ with a left-action on a concrete $\mathbb{Z}$-module $V_{\mathbb{Z}}$. We will then obtain a bijection

$$G_{\mathbb{Z}} \backslash V_{\mathbb{Z}} \to \mathcal{X},$$

where $\mathcal{X}$ is a family of objects we want to count. So, in the case of cubic rings, we had:

- $G_{\mathbb{Z}} = \mathrm{GL}_2(\mathbb{Z})$.
- $V_{\mathbb{Z}} = \mathrm{Sym}^3(\mathbb{Z}^2)$.
- $(g \cdot f)(x, y) = \frac{1}{\det(g)} \cdot f((x, y)g)$.
- $\mathcal{X} = \mathbf{CubRing}(\mathbb{Z})/\cong$.

In the quartic case, we parametrise slightly more structured data than just that of quartic rings. Given a quartic ring Q, Bhargava defines ([Bha04, Definition 8]) a *cubic resolvent ring of* Q to be another ring R satisfying certain technical properties, which we will not state here. Crucially, a given quartic ring may have multiple resolvent rings up to isomorphism. It turns out that the natural objects to parametrise are not quartic rings, but pairs (Q, R) where Q is a quartic ring and R is a cubic resolvent ring of R. We say that two such pairs (Q, R) and (Q', R') are *isomorphic* if $Q \cong Q'$ and $R \cong R'$. Then we have

$$\mathcal{X} = \{(Q, R) : Q \text{ quartic, } R \text{ cubic resolvent of } Q\}/\cong .$$

Given such a pair (Q, R), Bhargava constructs a map

$$\phi : Q/\mathbb{Z} \to R/\mathbb{Z}.$$

It turns out that, given choices of basis for the free $\mathbb{Z}$-modules $Q/\mathbb{Z} \cong \mathbb{Z}^3$ and $R/\mathbb{Z} \cong \mathbb{Z}^2$, the map $\phi : \mathbb{Z}^3 \to \mathbb{Z}^2$ is of the form

$$v \mapsto (v^T A v, v^T B v),$$

for symmetric 3×3 integer matrices A and B. Write $\mathrm{Sym}^2(\mathbb{Z}^3) \otimes \mathbb{Z}^2$ for the space of such pairs of matrices. Changing basis for $Q/\mathbb{Z}$ and $R/\mathbb{Z}$ by elements $(g_3, g_2) \in \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ is equivalent to replacing (A, B) with the pair

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

To be precise, identifying (A, B) with the corresponding map $f : \mathbb{Z}^3 \to \mathbb{Z}^2$, for each $(g_3, g_2) \in \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ we have a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}^3 \arrow[r, "{(A,B)}"] & \mathbb{Z}^2 \arrow[d, "(-)\cdot g_2^T"] \\
\mathbb{Z}^3 \arrow[u, "g_3^T\cdot(-)"] \arrow[r, "{(g_3,g_2)\cdot(A,B)}"'] & \mathbb{Z}^2
\end{tikzcd}$$

where the vertical maps are left- and right-multiplication by column and row vectors, respectively. Setting $G_{\mathbb{Z}} = \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ and $V_{\mathbb{Z}} = \mathrm{Sym}^2(\mathbb{Z}^3) \otimes \mathbb{Z}^2$, it turns out that the orbits $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ correspond bijectively to the pairs $(Q, R) \in \mathcal{X}$.

To summarise, in the quartic case we have

- $G_{\mathbb{Z}} = \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$.
- $V_{\mathbb{Z}} = \mathrm{Sym}^2(\mathbb{Z}^3) \otimes \mathbb{Z}^2$.
- $(g_3, g_2) \cdot (A, B) = (g_3 A g_3^T, g_3 B g_3^T) g_2^T$.
- $\mathcal{X} = \{(Q, R) : Q$ quartic, R cubic resolvent of $Q\}/\cong$.

The quintic case is even more involved than the quartic. Bhargava unifies the cubic and quartic parametrisations in a geometric framework. He then uses this framework to divine the correct parametrisation for quintic rings. The construction is explained at a high level in [Bha08, Section 1], and in detail in [Bha08, Section 2]. We will now briefly outline the key insights. Given a rank n ring R, Bhargava constructs a certain set

$$X_R = \{x^{(1)}, \ldots, x^{(n)}\} \subseteq \mathbb{P}^{n-2}(\mathbb{C})$$

in projective space. He then constructs certain varieties in $\mathbb{P}^{n-2}$ that vanish on the points of X_R. Taking a suitable intersection of such varieties, Bhargava realises X_R as the vanishing set of a collection of homogeneous polynomials in $n-1$ variables. The idea is then roughly that these polynomials will parametrise the degree n rings from which they arise.

In the case $n = 3$, the variety in question is cut out by a single binary cubic form, which turns out to be none other than the form corresponding to R via Delone–Fadeev. For $n = 4$, the variety is cut out by a pair of ternary quadratic forms, which is precisely the pair $(A, B) \in \mathrm{Sym}^2(\mathbb{Z}^3) \otimes \mathbb{Z}^2$ from Bhargava's parametrisation of quartic rings.

Finally, when $n = 5$, the variety is cut out by five quadrics in four variables. The 5-tuple of quadrics arises as the "sub-Pfaffians" of a 5×5 skew-symmetric matrix of linear forms in four variables, which is equivalent to the data of a 4-tuple (A, B, C, D) of 5×5 skew-symmetric matrices. Write $V_{\mathbb{Z}}$ for the set $\wedge^2(\mathbb{Z}^5) \otimes \mathbb{Z}^4$ of such 4-tuples. The choices made in this construction amount to an action by $G_{\mathbb{Z}} = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ on $V_{\mathbb{Z}}$, given by

$$(g_4, g_5) \cdot (A, B, C, D) = (g_5 A g_5^T, \ldots, g_5 D g_5^T) g_4^T.$$

Similarly to the quartic case, the orbits $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ correspond not to quintic rings, but to pairs (Q, S), where Q is a quintic ring and S is something called a "sextic resolvent ring" of Q, defined in [Bha08, Section 5]. So, for quintics, we have:

- $G_{\mathbb{Z}} = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$.
- $V_{\mathbb{Z}} = \wedge^2(\mathbb{Z}^5) \otimes \mathbb{Z}^4$.
- $(g_4, g_5) \cdot (A, B, C, D) = (g_5 A g_5^T, \ldots, g_5 D g_5^T) g_4^T$.
- $\mathcal{X} = \{(Q, S) : Q$ quintic, S sextic resolvent of $Q\}/\cong$.

We saw that in the cubic case, $R(f)$ was an integral domain if and only if f was irreducible, and $R(f)$ was maximal if and only if f satisfied a certain family of congruence conditions. Thus, cubic number fields correspond bijectively to irreducible orbits $G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$ satisfying the maximality conditions. Moreover, imposing local conditions on the number field corresponds to adding further congruence conditions on the orbits. Thus (ignoring C_3-extensions, which are rare), in order to evaluate $N_{\mathbb{Q},3}(X;\Sigma)$, it suffices to understand the count

$$N_{G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}}\big(X; S^{\mathrm{irred}}\big) = \#\{[x] \in G_{\mathbb{Z}}\backslash S^{\mathrm{irred}} : |\mathrm{disc}(x)| \leq X\}, \tag{5}$$

where $S \subseteq V_{\mathbb{Z}}$ is a certain $G_{\mathbb{Z}}$-invariant set defined by congruence conditions, and S^{irred} is the set of irreducible elements of S.

In the quartic and quintic cases, Bhargava defines similar notions of discriminant, maximality, and irreducibility, such that the relevant number fields correspond to maximal, irreducible elements of $V_{\mathbb{Z}}$, and the discriminant of the number field equals the discriminant of the corresponding element. We can also define congruence conditions in a way analogous to Definition 4.8. Once again, both maximality and local conditions on the number field amount to imposing congruence conditions on $V_{\mathbb{Z}}$. Thus, finding $N_{\mathbb{Q},n}(X;\Sigma)$ for $n = 4, 5$ also boils down to counting problems of essentially the same form as Equation (5). In the next subsection, we sketch the ideas involved in performing such a count.

4.3. **Counting integral orbits: Bhargava's magic machine.** Let (G, V) be one of the group-representation pairs above. Call an element of $V_{\mathbb{Z}}$ *generic* if it is irreducible and corresponds to an order in an S_n-n-ic number field. The name refers to the fact that S_n-n-ics are also called "generic" number fields. Given a subset $S \subseteq V_{\mathbb{Z}}$, we will always write S^{gen} for the set of generic elements of S. Recall that maximality and local conditions on our number field both correspond to congruence conditions on the orbit. Therefore, we want to be able to count generic integer orbits in $G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}$ satisfying congruence conditions. That is, when S is a $G_{\mathbb{Z}}$-invariant subset of $V_{\mathbb{Z}}$ defined by congruence conditions, we want the asymptotics of

$$N_{G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}}\big(X; S^{\mathrm{gen}}\big) = \#\{[x] \in G_{\mathbb{Z}}\backslash S^{\mathrm{gen}} : |\mathrm{disc}(x)| \leq X\}. \tag{6}$$

A priori, it is difficult to understand the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$. Part of this difficulty comes from the discrete nature of the lattice $V_{\mathbb{Z}}$. Therefore, we will make things more continuous by embedding $V_{\mathbb{Z}}$ in the real vector space $V_{\mathbb{R}}$. The left-action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ extends naturally to a left-action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}$. We call an element $v \in V_{\mathbb{R}}$ a *lattice point* if it is in $V_{\mathbb{Z}}$. We call an orbit in $G_{\mathbb{Z}}\backslash V_{\mathbb{R}}$ *integral* if it is in the image of the embedding $G_{\mathbb{Z}}\backslash V_{\mathbb{Z}} \to G_{\mathbb{Z}}\backslash V_{\mathbb{R}}$. In other words, the integral orbits of $G_{\mathbb{Z}}\backslash V_{\mathbb{R}}$ are precisely those of the form $G_{\mathbb{Z}}v$, for lattice points v. So $N_{G_{\mathbb{Z}}\backslash V_{\mathbb{Z}}}(X; S^{\mathrm{gen}})$ is the number of integral orbits of $G_{\mathbb{Z}}\backslash V_{\mathbb{R}}$ that are of the form $G_{\mathbb{Z}}v$, for a lattice point $v \in S^{\mathrm{gen}}$.

Call an element $v \in V_{\mathbb{R}}$ *nondegenerate* if $\mathrm{disc}(v) \neq 0$. It is a fact that, for each pair (G, V) we are considering, for all $g \in G_{\mathbb{R}}$ and $v \in V_{\mathbb{R}}$ we have $\mathrm{disc}(v) = 0$ if and only if $\mathrm{disc}(g \cdot v) = 0$. Thus, nondegeneracy is preserved by the actions of $G_{\mathbb{R}}$ and $G_{\mathbb{Z}}$, so it makes sense to refer to an orbit as nondegenerate.

Lemma 4.9. *Let $n \in \{3, 4, 5\}$ and let (G, V) be the representation associated to degree n rings. Let r be the number of nondegenerate orbits of $G_{\mathbb{R}}\backslash V_{\mathbb{R}}$. Then we have*

$$r = \begin{cases} 2 & \text{if } n = 3, \\ 3 & \text{if } n = 4, 5. \end{cases}$$

Let $V_{\mathbb{R}}^{(1)}, \ldots, V_{\mathbb{R}}^{(r)}$ be these nondegenerate orbits. Then we may order the $V_{\mathbb{R}}^{(i)}$ in such a way that, for any $v_i \in V_{\mathbb{R}}^{(i)}$, the sizes of the stabilisers $\mathrm{Stab}_{G_{\mathbb{R}}}(v_i)$ are given by

$$\Big(\mathrm{Stab}_{G_{\mathbb{R}}}(v_1), \ldots, \mathrm{Stab}_{G_{\mathbb{R}}}(v_r)\Big) = \begin{cases} (6,2) & \textit{if } n = 3, \\ (24,4,8) & \textit{if } n = 4, \\ (120,12,8) & \textit{if } n = 5. \end{cases}$$

Proof. For $n = 3$ this is stated on [BST13, Pages 453 and 455]. The cases $n = 4$ and $n = 5$ are stated on [Bha05, Page 1038] and [Bha10, Page 1567].

We also sketch an explanation of the result. Just as the integral orbits $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ parametrise rank n rings over $\mathbb{Z}$, the real orbits $G_{\mathbb{R}} \backslash V_{\mathbb{R}}$ parametrise rank n rings over $\mathbb{R}$. Moreover, the nondegenerate rank n rings over $\mathbb{R}$ are precisely the degree n real étale algebras. There are two cubic étale algebras over $\mathbb{R}$, and three quartic and quintic ones. Moreover, analogously to Theorem 4.3(4), the elements of $\mathrm{Stab}_{G_{\mathbb{R}}}(v)$ correspond to automorphisms of étale algebras, and it is easy to see that the degree n étale algebras over $\mathbb{R}$ have the stated number of automorphisms. □

We will always write $V_{\mathbb{R}}^{(1)}, \ldots, V_{\mathbb{R}}^{(r)}$ for the orbits of $G_{\mathbb{R}} \backslash V_{\mathbb{R}}$, ordered as in the statement of Lemma 4.9.

Recall that we want to count the generic integral orbits in $G_{\mathbb{Z}} \backslash V_{\mathbb{R}}$. If we had a fundamental domain $\mathcal{G}$ for $G_{\mathbb{Z}} \backslash V_{\mathbb{R}}$, counting such integral orbits would amount to counting integral points in $S^{\mathrm{gen}} \cap \mathcal{G}$. Unfortunately, we do not have a simple candidate for $\mathcal{G}$. On the other hand, it is not too difficult to write down an explicit fundamental domain for $G_{\mathbb{Z}} \backslash G_{\mathbb{R}}$, where $G_{\mathbb{Z}}$ acts by left-multiplication. In the cubic case, a well-known such domain was constructed by Gauss (this construction is stated at the beginning of [BST13, Section 5.1]). Two centuries later, Bhargava generalised Gauss's construction to the quartic and quintic cases (see [Bha05, Page 1038] and [Bha10, Page 1567]). Thus, for each of $n = 3, 4, 5$, one can write down an explicit fundamental domain for $G_{\mathbb{Z}} \backslash G_{\mathbb{R}}$. From now on, we will write $\mathcal{F}$ for this fundamental domain.

Given an element $v \in V_{\mathbb{R}}$, there is a natural "pushforward" of $\mathcal{F}$ to $V_{\mathbb{R}}$, given by

$$\mathcal{F} \to V_{\mathbb{R}}, \quad f \mapsto f \cdot v.$$

Write $\mathcal{F}v$ for the image $\{f \cdot v : f \in \mathcal{F}\}$ of this pushforward. The set $\mathcal{F}v$ will behave somewhat like a fundamental domain for $G_{\mathbb{Z}} \backslash V_{\mathbb{R}}$. Firstly, we obvserve that $\mathcal{F}v$ cannot literally be a fundamental domain because $G_{\mathbb{Z}}\mathcal{F}v \subseteq G_{\mathbb{R}}v$, and the real orbit $G_{\mathbb{R}}v$ will not in general be the whole of $V_{\mathbb{R}}$. In fact, it will turn out that $\mathcal{F}v$ is a union of fundamental domains for the action of $G_{\mathbb{Z}}$ on the orbit $G_{\mathbb{R}}v$, so we may consider these orbits separately.

Let $v \in V_{\mathbb{R}}$ be a nondegenerate element. For $g \in \mathrm{Stab}_{G_{\mathbb{R}}}(v)$ and $f \in \mathcal{F}$, define f^g to be the unique element of $\mathcal{F}$ with $G_{\mathbb{Z}} f^g = G_{\mathbb{Z}}(fg)$. This defines a natural right-action of $\mathrm{Stab}_{G_{\mathbb{R}}}(v)$ on $\mathcal{F}$. Let $\mathcal{F}_0$ be a fundamental domain for this action $\mathcal{F} / \mathrm{Stab}_{G_{\mathbb{R}}}(v)$.

Lemma 4.10. *Let $v \in V_{\mathbb{R}}^{(i)}$ for some $i \in \{1, \ldots, r\}$, and let $\mathcal{F}_0$ be as above. Then the map*

$$\mathcal{F}_0 \to V_{\mathbb{R}}^{(i)}, \quad f \mapsto f \cdot v$$

is injective, and its image $\mathcal{F}_0 v$ is a fundamental domain for $G_{\mathbb{Z}} \backslash V_{\mathbb{R}}^{(i)}$.

Proof. Suppose that $f \cdot v = f' \cdot v$ for $f, f' \in \mathcal{F}_0$. Then $f' = fg$ for some $g \in \operatorname{Stab}_{G_\mathbb{R}}(v)$, so $f = f'$ by definition of $\mathcal{F}_0$. So indeed the map is injective.

To complete the proof, we need to show that for each $x \in V_\mathbb{R}^{(i)}$, there is exactly one element $f_0 \in \mathcal{F}_0$ such that $G_\mathbb{Z} f_0 v = G_\mathbb{Z} x$. Let $x \in V_\mathbb{R}^{(i)}$. Then there is some $\alpha \in G_\mathbb{R}$ such that $x = \alpha v$. By definition of $\mathcal{F}$, there is some $f \in \mathcal{F}$ such that $G_\mathbb{Z} f = G_\mathbb{Z}\alpha$, so $G_\mathbb{Z} f v = G_\mathbb{Z} \alpha v$. It is easy to see that the set

$$\{f' \in \mathcal{F} : G_\mathbb{Z} f' v = G_\mathbb{Z} x\}$$

is precisely the orbit

$$f \operatorname{Stab}_{G_\mathbb{R}}(v) = \{f^\theta : \theta \in \operatorname{Stab}_{G_\mathbb{R}}(v)\}.$$

By definition of $\mathcal{F}_0$, exactly one element of this orbit is in $\mathcal{F}_0$, and this element is the unique f_0 we required. □

For each $i \in \{1, \dots, r\}$, let n_i be the integer from Lemma 4.9, with

$$n_i = \# \operatorname{Stab}_{G_\mathbb{R}}(v) \quad \text{for each } v \in V_\mathbb{R}^{(i)}.$$

Write $\operatorname{Stab}_{G_\mathbb{R}}(v) = \{\theta_1, \dots, \theta_{n_i}\}$, and let $\mathcal{F}_i = \mathcal{F}_0\theta$ for each i. Clearly, each $\mathcal{F}_i$ is a fundamental domain for the right-action of $\operatorname{Stab}_{G_\mathbb{R}}(v)$ on $\mathcal{F}$. Since this action is free, the fundamental domains $\mathcal{F}_i$ are pairwise disjoint, so they constitute a partition of $\mathcal{F}$ into n_i fundamental domains for the right-action of $\operatorname{Stab}_{G_\mathbb{R}}(v)$. It follows that

$$\mathcal{F}v = \bigcup_{j=1}^{n_i} \mathcal{F}_j v.$$

Lemma 4.10 tells us that each set $\mathcal{F}_j v \subseteq V_\mathbb{R}^{(i)}$ is a fundamental domain for $G_\mathbb{Z}\backslash V_\mathbb{R}^{(i)}$, so $\mathcal{F}v$ is a union of n_i such fundamental domains. Naïvely, one might hope that $\mathcal{F}v$ is then an "n_i-fold fundamental domain", in the sense that each orbit has exactly n_i representatives in $\mathcal{F}v$. Unfortunately, this is not the case, because the sets $\mathcal{F}_j v$ are not necessarily disjoint. That is, for distinct j, k, we might have $f \in \mathcal{F}_j$ and $f' \in \mathcal{F}_k$, such that $fv = f'v$. Even though f and f' map to the same point of $V_\mathbb{R}^{(i)}$, Bhargava keeps track of the difference by assigning the point with a multiplicity. Formally, for each $x \in \mathcal{F}v$, we define

$$\operatorname{mult}(x) = \#\{f \in \mathcal{F} : f \cdot v = x\}.$$

For a subset $S \subseteq \mathcal{F}v$, we define the *size of the multiset* S to be

$$\#S = \sum_{x \in S} \operatorname{mult}(x) = \#\{f \in \mathcal{F} : f \cdot v \in S\}.$$

In the sense we discussed above, $\mathcal{F}v$ would be an "n_i-fold fundamental domain" for $G_\mathbb{Z}\backslash V_\mathbb{R}^{(i)}$ if and only if we had $\operatorname{mult}(x) = 1$ for each $x \in \mathcal{F}v$. There is no simple way of knowing the multiplicity of a single point of $\mathcal{F}v$. On the other hand, the combined multiplicity of the points in an *orbit* has the following simple description:

Lemma 4.11. *Let $i \in \{1, \dots, r\}$ and let $v \in V_\mathbb{R}^{(i)}$. For each $x \in G_\mathbb{R} v$, we have*

$$\#(G_\mathbb{Z} x \cap \mathcal{F}v) = \frac{n_i}{\# \operatorname{Stab}_{G_\mathbb{Z}}(x)},$$

where the quantity on the left is a multiset cardinality.

Proof. The quantity on the left is just

$$\#\{f \in \mathcal{F} : G_\mathbb{Z} f v = G_\mathbb{Z} x\}.$$

Since x is in the $G_{\mathbb{R}}$-orbit of v, there is some $\alpha \in G_{\mathbb{R}}$ with $\alpha v = x$. Given $\theta \in \operatorname{Stab}_{G_{\mathbb{R}}}(x)$, let $\varphi(\theta)$ be the unique element of $\mathcal{F}$ with $G_{\mathbb{Z}}\varphi(\theta) = G_{\mathbb{Z}}\theta\alpha$. Then we have a well-defined map

$$\varphi : \operatorname{Stab}_{G_{\mathbb{R}}}(x) \to \{f \in \mathcal{F} : G_{\mathbb{Z}} f v = G_{\mathbb{Z}} x\}.$$

It is easy to see that φ is surjective, and that, for all $\theta, \theta' \in \operatorname{Stab}_{G_{\mathbb{R}}}(x)$, we have $\varphi(\theta) = \varphi(\theta')$ if and only if $\operatorname{Stab}_{G_{\mathbb{Z}}}(x)\theta = \operatorname{Stab}_{G_{\mathbb{Z}}}(x)\theta'$. Therefore, φ descends to a bijection

$$\operatorname{Stab}_{G_{\mathbb{Z}}}(x)\backslash \operatorname{Stab}_{G_{\mathbb{R}}}(x) \to \{f \in \mathcal{F} : G_{\mathbb{Z}} f v = G_{\mathbb{Z}} x\},$$

where the left-hand side is the set of right-cosets of $\operatorname{Stab}_{G_{\mathbb{Z}}}(x)$ in $\operatorname{Stab}_{G_{\mathbb{R}}}(x)$. The result follows. □

For any subset $S \subseteq V_{\mathbb{R}}$, write

$$S_{\leq X} = \{x \in S : 0 < |\operatorname{disc}(x)| \leq X\}.$$

Remark 4.12. Recall that the action of $G_{\mathbb{Z}}$ preserves absolute discriminant. Therefore, if $S \subseteq V_{\mathbb{R}}$ is a $G_{\mathbb{Z}}$-invariant set, then for every X, the set $S_{\leq X}$ is also $G_{\mathbb{Z}}$-invariant.

Let S be a $G_{\mathbb{Z}}$-invariant subset of $V_{\mathbb{Z}}$, and let X be a positive real number. Define $N_{\text{stab}}(X; S)$ to be the inverse-stabiliser-weighted count

$$N_{\text{stab}}(X; S) = \sum_{G_{\mathbb{Z}}x \in G_{\mathbb{Z}}\backslash S^{\text{gen}}_{\leq X}} \frac{1}{\# \operatorname{Stab}_{G_{\mathbb{Z}}}(x)}.$$

Moreover, for $i \in \{1, \ldots, r\}$, define the refinement $N^{(i)}_{\text{stab}}(X; S)$ of $N_{\text{stab}}(X; S)$ by

$$N^{(i)}_{\text{stab}}(X; S) = N_{\text{stab}}\big(X; S \cap V^{(i)}_{\mathbb{Z}}\big).$$

Remark 4.13. Theorem 4.3(4) tells us that, in the cubic case $n = 3$, for each $x \in V_{\mathbb{Z}}$, the ring $R(x)$ corresponding to x has

$$\# \operatorname{Aut}(R(x)) = \# \operatorname{Stab}_{G_{\mathbb{Z}}}(x).$$

The same is true when $n = 4$ and $n = 5$, so $N^{(i)}_{\text{stab}}(X; S)$ counts fields weighted inversely to their number of automorphisms.

Lemma 4.14. *Let $n \in \{3, 4, 5\}$, and let (G, V) be the representation parametrising rings of rank n. Let $v \in V^{(i)}_{\mathbb{R}}$ for some $i \in \{1, \ldots, r\}$. Recall that we write n_i for the size of the stabiliser $\operatorname{Stab}_{G_{\mathbb{R}}}(v)$. For a $G_{\mathbb{Z}}$-invariant subset S of $V_{\mathbb{Z}}$, we have*

$$N^{(i)}_{\text{stab}}(X; S) = \frac{1}{n_i} \cdot \#(\mathcal{F}v \cap S^{\text{gen}}_{\leq X}),$$

where the cardinality on the right is the size of the multiset, i.e. counting multiplicities.

Proof. Lemma 4.11 tells us that

$$\begin{aligned} N^{(i)}_{\text{stab}}(X; S) &= \sum_{G_{\mathbb{Z}}x \in G_{\mathbb{Z}}\backslash (S^{\text{gen}}_{\leq X} \cap V^{(i)}_{\mathbb{Z}})} \frac{1}{n_i} \cdot \#(G_{\mathbb{Z}}x \cap \mathcal{F}v) \\ &= \frac{1}{n_i} \cdot \#(\mathcal{F}v \cap S^{\text{gen}}_{\leq X}). \end{aligned}$$

□

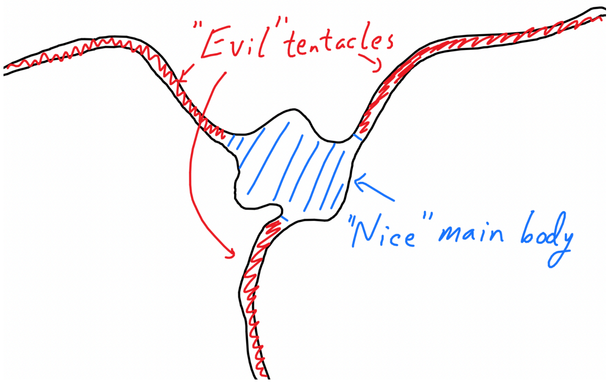
Lemma 4.14 tells us that we want to count lattice points in the region $\mathcal{F}v$. Given a lattice $L \subseteq V_{\mathbb{R}}$ and a subset $S \subseteq V_{\mathbb{R}}$, write $\operatorname{Vol}_L(S)$ for the volume of S, normalised so that the fundamental region of L has volume 1. Our intuition for nice geometric spaces might suggest that the number of lattice points in a region should be approximately equal to the volume of that region, leading us to the following "Hope":

Hope 4.15. *Naïvely, one might hope that, given a lattice $L \subseteq V_{\mathbb{R}}$, we have*

$$\#(\mathcal{F}v \cap L^{\mathrm{gen}}_{\leq X}) \approx \mathrm{Vol}_L((\mathcal{F}v)_{\leq X}).$$

This hope turns out to be true, but it is difficult to prove. Intuitively, we expect such results to hold for nicely shaped regions, like spheres or cubes. The problem is that $\mathcal{F}v$ is not nicely shaped at all; it has long, thin cusps stretching to infinity. These cusps are often referred to more evocatively as "tentacles", and the region $\mathcal{F}v$ is often visualised as in Figure 1. As illustrated in Figure 2, these cusps are exactly the sort of thing that might cause Hope 4.15 to fail, since they could pass through many lattice points, while having small volume because they are so thin.

Figure 1. Intuitive visual representation of the region $\mathcal{F}v$. It is somewhat easy to count lattice points in the main body, but more difficult in the cusps.



In the cubic case, there is only one such cusp. This cusp turns out not to contain any irreducible points, so we can ignore it and just count lattice points in the main body, as was done by Davenport–Heilbronn. For $n = 4$, two of the cusps do contain irreducible points. Finally, in the case $n = 5$, there are hundreds of cusps containing irreducible points. Thus, Davenport–Heilbronn's methods are difficult to extend to $n = 4$ and $n = 5$.

Bhargava's famous insight is as follows. Since the quantity in Lemma 4.14 is independent of choice of v, we can select v at random (from some suitable distribution) and then take expectations over our random variable v. We make this precise in Lemma 4.16.

Figure 2. A narrow cusp can pass through many lattice points, while having arbitrarily small volume, causing the volume estimate to fail.

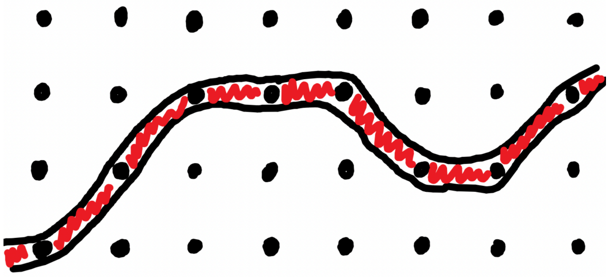
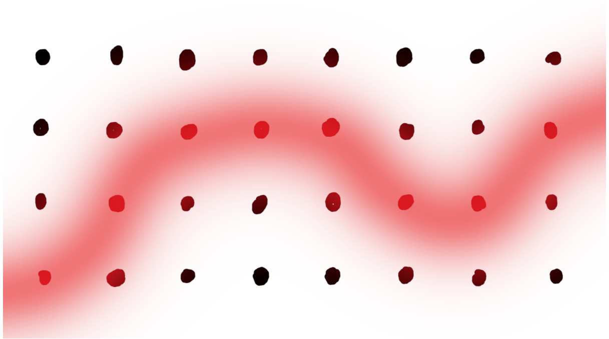


Figure 3. If we thicken the cusps probabilistically, the resulting "fuzzy cusps" behave well enough that they can't have such small volume, so the volume estimates can be salvaged.



Lemma 4.16 (Bhargava's averaging method)**.** *Given some $i \in \{1, \ldots, r\}$, let v be a random variable taking values in $V_{\mathbb{R}}^{(i)}$. For each $G_{\mathbb{Z}}$-invariant subset $S \subseteq V_{\mathbb{Z}}$, we have*

$$N_{\mathrm{stab}}^{(i)}(X; S) = \frac{1}{n_i} \cdot \mathbb{E}_v \left[\#(\mathcal{F}v \cap S_{\leq X}^{\mathrm{gen}}) \right].$$

Proof. This is immediate from Lemma 4.14, since we are taking the expectation of a constant. □

The averaging method replaces the thin, concrete cusp of Figure 2 with a thicker, fuzzy, probabilistic cusp, as illustrated in Figure 3. In other words, we perform a probability-weighted count of lattice points, where the weight of a lattice point x is the probability that the random set $\mathcal{F}v$ contains x. It turns out that these thickened cusps are nice enough that they do obey Hope 4.15.

People often use the slogan "averaging over many fundamental domains" to describe Bhargava's averaging method. This slogan refers to the fact that, up to multiplicity, $\mathcal{F}v$ is a random fundamental(ish) domain, and we are averaging the lattice point count over all possible choices of this random domain.

Fix a lattice $L \subseteq V_{\mathbb{Z}}$. We will now sketch the steps in actually evaluating $N_{\mathrm{stab}}^{(i)}(X; L)$, using the averaging method. Bhargava starts by constructing a subset $G_0 \subseteq G_{\mathbb{R}}$ with certain desirable properties, and fixing an arbitrary element $v_0 \in V_{\mathbb{R}}^{(i)}$. He then defines a Haar measure μ on $G_{\mathbb{R}}$, which induces a probability measure on G_0. Through our probabilistic lens, Bhargava uses this probability measure to take a random $g \in G_0$, and then uses $\mathcal{F}gv_0$ as his random multi-fundamental domain. Bhargava uses integral instead of probabilistic notation, writing

$$N_{\mathrm{stab}}^{(i)}(X; L) = \frac{1}{n_i} \cdot \frac{\int_{g \in G_0} \#(\mathcal{F}gv_0 \cap L_{\leq X}^{\mathrm{gen}}) dg}{\int_{g \in G_0} dg}.$$

In an imprecise sense, the numerator above is counting pairs $(g, f) \in G_0 \times \mathcal{F}$ such that $fgv_0 \in L_{\leq X}^{\mathrm{gen}}$. More precisely, this "counting" consists of integrating continuously over G_0 and summing discretely over $\mathcal{F}$. A careful argument (see Problem 63 of the Arizona Winter School problems) allows us to exchange the integration and summation, to obtain

$$\int_{g \in G_0} \#(\mathcal{F}gv_0 \cap L_{\leq X}^{\mathrm{gen}}) dg = \int_{f \in \mathcal{F}} \#(fG_0v_0 \cap L_{\leq X}^{\mathrm{gen}}) df.$$

We are now performing a different but related averaging operation: previously, we had a fixed set $\mathcal{F} \subseteq G_{\mathbb{R}}$, and we were pushing it forward to $V_{\mathbb{R}}$ using the randomly selected element $v = gv_0$; now, we instead have a fixed region $G_0 v_0 \subseteq V_{\mathbb{R}}^{(i)}$, and we are translating it by a randomly selected element $f \in \mathcal{F}$.

The idea is that, since G_0 is a specially chosen region in $G_{\mathbb{R}}$, the subset $(fG_0v_0)_{\leq X}$ of $V_{\mathbb{R}}$ should be nice enough that its lattice point count $\#((fG_0v_0)_{\leq X} \cap L^{\mathrm{gen}})$ is approximately equal to its volume. The crucial difference between G_0 and $\mathcal{F}$ is that G_0 is *compact*; it is the openness of $\mathcal{F}$ that makes the cusps particularly unruly, since they stretch off to infinity. While the region fG_0v_0 still has cusps, its compactness makes them bounded, hence easier to work with.

The cusps are defined by explicit conditions involving the coefficients of the parametrising objects. For example, in the cubic case, the unique cusp is given by the subset $\{a = 0\}$ of $V_{\mathbb{Z}} = \{ax^3 + bx^2y + cxy^2 + dy^3\}$. In the cases $n = 4$ and $n = 5$, there are multiple cusps, but they are handled one at a time. Therefore, we will assume without loss of generality that there is only one cusp, allowing us to write

$$fG_0v_0 = (fG_0v_0)^{\mathrm{main}} \sqcup (fG_0v_0)^{\mathrm{cusp}},$$

where $(fG_0v_0)^{\mathrm{main}}$ and $(fG_0v_0)^{\mathrm{cusp}}$ refer to the points of fG_0v_0 that are in the main body and the cusp, respectively. Using the explicit definition of the cusp, Bhargava does one of the following:

- Either he shows that all points in the cusp are nongeneric[1], as is the case when $n = 3$, since $a = 0$ implies that $f(x, y) = y(bx^2 + cxy + dy^2)$;
- or he shows that the region $(fG_0v_0)^{\mathrm{cusp}}$ is nice enough that
$$\#((fG_0v_0)^{\mathrm{cusp}}_{\leq X} \cap L^{\mathrm{gen}}) \ll \mathrm{Vol}_L((fG_0v_0)^{\mathrm{cusp}}_{\leq X}).$$
In this case, he shows that the volume $\mathrm{Vol}_L((fG_0v_0)^{\mathrm{cusp}}_{\leq X})$ is $O(X^{1-\delta})$, for a positive real number δ, stated explicitly in [BSW15, Theorem 11].

On the other hand, Bhargava also shows that the region $(fG_0v_0)^{\mathrm{main}}$ is nice enough that

$$\#((fG_0v_0)^{\mathrm{main}}_{\leq X} \cap L) \approx \mathrm{Vol}((fG_0v_0)^{\mathrm{main}}_{\leq X}).$$

He also shows that 100% of the points in the main body are generic, so we have

$$\#((fG_0v_0)^{\mathrm{main}}_{\leq X} \cap L^{\mathrm{gen}}) \approx \mathrm{Vol}_L((fG_0v_0)^{\mathrm{main}}_{\leq X}).$$

As we will discuss shortly, Bhargava also finds that $\mathrm{Vol}_L((fG_0v_0)^{\mathrm{main}}_{\leq X}) \sim cX$ for a positive constant c, so the contributions from the cusp are negligible, meaning that

$$\#((fG_0v_0)_{\leq X} \cap L^{\mathrm{gen}}) \approx \mathrm{Vol}_L((fG_0v_0)_{\leq X}).$$

Thus, we obtain

$$N^{(i)}_{\mathrm{stab}}(X; L) \approx \frac{1}{n_i} \cdot \frac{\int_{f \in \mathcal{F}} \mathrm{Vol}_L((fG_0v_0)_{\leq X}) df}{\mathrm{Vol}(G_0)},$$

where the volume in the denominator is computed with respect to the Haar measure μ. The quantity in the numerator is a double integral over $\mathcal{F}$ and G_0, and we can again (via a similar

[1] In the cubic and quintic cases, he shows that these points are all reducible, whereas in the quartic he shows that they are not "absolutely irreducible", meaning that they are either reducible or the corresponding number field has a nontrivial automorphism.

careful argument to the one we used before) change the order of integration to obtain

$$N^{(i)}_{\mathrm{stab}}(X;L) \approx \frac{1}{n_i \cdot \mathrm{Vol}(G_0)} \int_{g\in G_0} \mathrm{Vol}_L((\mathcal{F}gv_0)_{\leq X})dg. \tag{7}$$

For each $g \in G_0$, the volume $\mathrm{Vol}_L((\mathcal{F}gv_0)_{\leq X})$ is by definition given by an integral over $\mathcal{F}gv_0$. Bhargava gives[1] a change of variables formula relating integrals over $\mathcal{F}gv_0$ to integrals over $\mathcal{F}$. This change of variables formula allows us to do two things:

- The integral may be shown to be independent of g, in the sense that
  $$\mathrm{Vol}_L((\mathcal{F}gv_0)_{\leq X}) = \mathrm{Vol}_L((\mathcal{F}v_0)_{\leq X}),$$
  for all $g \in G_{\mathbb{R}}$, so Equation (7) reduces to
  $$N^{(i)}_{\mathrm{stab}}(X;L) \approx \frac{1}{n_i} \cdot \mathrm{Vol}_L((\mathcal{F}v_0)_{\leq X}),$$
  which Lemma 4.14 tells us implies that Hope 4.15 is true. Thus, the asymptotic count we want reduces to computing the "fundamental volume" $\mathrm{Vol}_L((\mathcal{F}v_0)_{\leq X})$ for an arbitrary element $v_0 \in V^{(i)}_{\mathbb{R}}$.
- Moreover, the same change of variables formula expresses this fundamental volume as an integral over $\mathcal{F}$, which can be evaluated using the explicit definition of $\mathcal{F}$. Performing this integral, one obtains
  $$\mathrm{Vol}_L((\mathcal{F}v_0)_{\leq X}) = \frac{c}{\det(L)} \cdot X,$$
  where $\det(L)$ is the covolume of the lattice L, normalised such that $\det(V_{\mathbb{Z}}) = 1$, and c is a constant given by[2]
  $$c = \begin{cases} \frac{1}{2}\zeta(2) & \text{if } n = 3, \\ \frac{1}{2}\zeta(2)^2\zeta(3) & \text{if } n = 4, \\ \frac{1}{2}\zeta(2)^2\zeta(3)^2\zeta(4)^2\zeta(5) & \text{if } n = 5. \end{cases}$$

Thus, we have shown that

$$\lim_{X\to\infty} \frac{N^{(i)}_{\mathrm{stab}}(X;L)}{X} = \frac{c}{n_i \cdot \det(L)}$$

for any lattice $L \subseteq V_{\mathbb{Z}}$, where c is the constant defined above, which depends on n. Recall that, rather than points in a lattice L, we actually want to count points in a set S defined by congruence conditions. To that end, let $S = \bigcap_p S_p \subseteq V_{\mathbb{Z}}$ be a $G_{\mathbb{Z}}$-invariant set, where each S_p is defined by congruence conditions modulo p. Let P be a positive real number. Then the finite intersection

$$S_P = \bigcap_{p<P} S_p \subseteq V_{\mathbb{Z}}$$

is defined by congruence modulo some integer m, so it is a disjoint union of finitely many translates of the lattice $mV_{\mathbb{Z}}$. Let J be the number of such translates, and denote them by $L_1, \ldots, L_J$, so

$$S_P = \bigsqcup_{j=1}^{J} L_j.$$

[1] In the cubic, quartic, and quintic cases, this formula is [BST13, Proposition 23], [Bha04, Proposition 21], and [Bha08, Proposition 16], respectively; a more abstract, general version of the same formula is [BSW15, Proposition 20].

[2] See [BST13, Section 5.4], [Bha04, Page 1055], and [Bha08, Page 1585], respectively. Each paper denotes $(\mathcal{F}v_0)_{\leq X}$ by $\mathcal{R}_X(v_0)$.

For each j, we have $\det(L_j) = m^d$, where $d = \dim V_{\mathbb{R}}$, so

$$\lim_{X\to\infty} \frac{N^{(i)}_{\text{stab}}(X; L_j)}{X} = \frac{c}{n_i \cdot m^d}.$$

For each p, write $\mu_p(S_p)$ for the p-adic density of the p-adic closure $S_p \otimes_{\mathbb{Z}} \mathbb{Z}_p$ of S_p in $V_{\mathbb{Z}_p}$. That is, μ_p is the Haar measure on $V_{\mathbb{Z}_p}$, normalised so that $\mu_p(V_{\mathbb{Z}_p}) = 1$. It is easy to see that

$$\frac{J}{m^d} = \prod_{p<P} \mu_p(S_p),$$

and hence we obtain

$$\begin{aligned} N^{(i)}_{\text{stab}}(X; S_P) &= \sum_{j=1}^{J} N^{(i)}_{\text{stab}}(X; L_j) \\ &\sim \frac{c}{n_i} \cdot \frac{J}{m^d} \cdot X \\ &= \frac{c}{n_i} \cdot \prod_{p<P} \mu_p(S_p) \cdot X. \end{aligned}$$

Bhargava, Shankar, and Wang then apply a sieving argument to show that, for well-behaved collections of congruence conditions $(S_p)_p$, this product formula holds in the limit, by which we mean that

$$N^{(i)}_{\text{stab}}\Big(X; \bigcap_{p\in\Pi^{\text{fin}}_{\mathbb{Q}}} S_p\Big) \sim \frac{c}{n_i} \cdot \prod_{p\in\Pi^{\text{fin}}_{\mathbb{Q}}} \mu_p(S_p) \cdot X. \tag{8}$$

This formula looks very similar to the statement of Theorem 3.53. In that theorem, we have a product of masses $m(\Sigma_p)$ of local conditions, and in Equation (8), we have a product of p-adic densities $\mu_p(S_p)$ of congruence conditions. We can relate these masses and densities using essentially the same change of variables formula we mentioned earlier, adapted to the p-adic setting:

Lemma 4.17. *Let p be a rational prime, let $n \in \{3, 4, 5\}$, and let $\Sigma_p \subseteq \text{Ét}_{n/\mathbb{Q}_p}$. Let $S(\Sigma_p)$ be the set of $v \in V_{\mathbb{Z}}$ such that v is maximal at p and $R(v) \otimes_{\mathbb{Z}} \mathbb{Q}_p \in \Sigma_p$. Then we have*

$$\mu_p(S(\Sigma_p)) = f(p) \cdot m(\Sigma_p),$$

where $f(p)$ is the function given by

$$f(p) = \begin{cases} 1 - p^{-2} & \text{if } n = 3, \\ (1-p^{-2})^2(1-p^{-3}) & \text{if } n = 4, \\ (1-p^{-2})^2(1-p^{-3})^2(1-p^{-4})^2(1-p^{-5}) & \text{if } n = 5. \end{cases}$$

Sketch proof. The case $n = 3$ is essentially [BST13, Lemma 32]. We restate the proof of that result in our own words, asserting that the statements extend naturally to the cases $n = 4$ and $n = 5$.

Write dg and dv for the Haar measures on $G_{\mathbb{Z}_p}$ and $V_{\mathbb{Z}_p}$, respectively, normalised so that

$$\int_{g\in G_{\mathbb{Z}_p}} dg = \int_{v\in V_{\mathbb{Z}_p}} dv = 1.$$

Let $L \in \text{Ét}_{n/\mathbb{Q}_p}$, let $\mathcal{O}_L$ be the ring of integral elements of L, and let $v_0 \in V_{\mathbb{Z}_p}$ be such that $R(v_0) \cong \mathcal{O}_L$. We have

$$S(\{L\}) = \{v \in V_{\mathbb{Z}} : R(v) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{O}_L\},$$

so

$$\mu_p(S(\{L\})) = \int_{v \in G_{\mathbb{Z}_p} v_0} dv.$$

There is a natural right-action of $\operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0)$ on $G_{\mathbb{Z}_p}$. Write $G_{\mathbb{Z}_p}/\operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0)$ as shorthand for a fundamental domain of this action, and assume that this fundamental domain has nice measure-theoretic properties. There is a continuous bijection

$$G_{\mathbb{Z}_p}/\operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0) \to G_{\mathbb{Z}_p} \cdot v_0, \quad g \mapsto g \cdot v_0.$$

With respect to the Haar measures dg and dv, [BSW15, Proposition 20] tells us[1] that the Jacobian of this bijection is given by

$$\frac{\partial \varphi}{\partial g}(g) = a_p \cdot |\operatorname{disc}(\varphi(g))|_p,$$

for some constant a_p, depending on p. Since $|\operatorname{disc}(gv_0)|_p = |\operatorname{disc}(v_0)|_p$ for all $g \in G_{\mathbb{Z}_p}$, we obtain

$$\begin{aligned}
\mu_p(S(\{L\})) &= \int_{v \in G_{\mathbb{Z}_p} v_0} dv \\
&= \int_{g \in G_{\mathbb{Z}_p}/\operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0)} \frac{\partial \varphi}{\partial g} dg \\
&= a_p \cdot \int_{g \in G_{\mathbb{Z}_p}/\operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0)} |\operatorname{disc}(g \cdot v_0)|_p dg \\
&= a_p \cdot |\operatorname{disc}(v_0)|_p \int_{g \in G_{\mathbb{Z}_p}/\operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0)} dg \\
&= a_p \cdot \frac{|\operatorname{disc}(v_0)|_p}{\# \operatorname{Stab}_{G_{\mathbb{Z}_p}}(v_0)} \\
&= a_p \cdot \frac{|\operatorname{disc}(L/\mathbb{Q}_p)|_p}{\# \operatorname{Aut}(L/\mathbb{Q}_p)} \\
&= a_p \cdot \widetilde{m}(\{L\}).
\end{aligned}$$

It follows that

$$\mu_p(S(\Sigma_p)) = a_p \cdot \widetilde{m}(\Sigma_p)$$

for any subset $\Sigma_p \subseteq \text{Ét}_{n/\mathbb{Q}_p}$. By definition of $S(\Sigma_p)$, we have

$$S(\text{Ét}_{n/\mathbb{Q}_p}) = \mathcal{U}_p,$$

so we have

$$a_p = \frac{\mu_p(\mathcal{U}_p)}{\widetilde{m}(\text{Ét}_{n/\mathbb{Q}_p})}.$$

By Corollary 3.10, we have

$$\widetilde{m}(\text{Ét}_{n/\mathbb{Q}_p}) = \begin{cases} (p^2+p+1)/p^2 & \text{if } n = 3, \\ (p^3+p^2+2p+1)/p^3 & \text{if } n = 4, \\ (p^4+p^3+2p^2+2p+1)/p^4 & \text{if } n = 5. \end{cases}$$

[1] The Jacobian calculation can also be performed directly from explicit descriptions of G and V. Bhargava does this in his earlier work, but never includes any details of the computation. The 2014 Arizona Winter School problems give more context on the Jacobian of the analogous map $G_{\mathbb{R}} \to G_{\mathbb{R}} \cdot v_0$ in the cubic case. In Problems 64 and 65, they describe dg explicitly in terms of a parametrisation of $G_{\mathbb{R}}$. Subsequently, in Problem 74, the reader is tasked with proving the change of variables formula $dg = |\operatorname{disc}(v_0)|^{-1} dv$, which is essentially the same as computing the Jacobian.

For $n = 3, 4, 5$, the densities $\mu_p(\mathcal{U}_p)$ are stated explicitly in [BST13, Lemma 19], [Bha04, Equation (45)], and [Bha08, Equation (48)], respectively, and it follows from those references that

$$a_p = \begin{cases} (p-1)(p^2-1)/p^3 \quad \text{if } n = 3, \\ (p-1)^4(p+1)^2(p^2+p+1)/p^8 \quad \text{if } n = 4, \\ (p-1)^8(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)/p^{24} \quad \text{if } p = 5. \end{cases}$$

Finally,

$$\mu_p(S(\Sigma_p)) = a_p \cdot \frac{p}{p-1} \cdot m(\Sigma_p),$$

and the result follows. □

Lemma 4.18. *Let $f(p)$ be the function from Lemma 4.17. Then we have*

$$\prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} f(p) = \begin{cases} \frac{1}{\zeta(2)} \quad \textit{if } n = 3, \\ \frac{1}{\zeta(2)^2\zeta(3)} \quad \textit{if } n = 4, \\ \frac{1}{\zeta(2)^2\zeta(3)^2\zeta(4)^2\zeta(5)} \quad \textit{if } n = 5. \end{cases}$$

Proof. This is immediate from the well-known Euler product for $\zeta(s)$. □

Let Σ be an acceptable collection of local conditions on $\mathbb{Q}$, and define the sets $S(\Sigma_p)$ as in Lemma 4.17. Let

$$S_{\text{fin}}(\Sigma) = \bigcap_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} S(\Sigma_p).$$

Then Equation (8), Lemma 4.17, and Lemma 4.18 tell us that

$$\begin{aligned} N_{\text{stab}}^{(i)}(X; S_{\text{fin}}(\Sigma)) &\sim \frac{c}{n_i} \cdot \prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} \mu_p(S(\Sigma_p)) \cdot X \\ &= \frac{c}{n_i} \cdot \prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} f(p) \cdot \prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} m(\Sigma_p) \cdot X \\ &= \frac{1}{2n_i} \prod_{p \in \Pi_{\mathbb{Q}}^{\text{fin}}} m(\Sigma_p) \cdot X. \end{aligned}$$

Each real étale algebra L in $\text{Ét}_{n/\mathbb{R}}$ corresponds to a real orbit $V_{\mathbb{R}}^{(i)}$. Let

$$S(\Sigma_\infty) = \{i \in \{1, \ldots, r\} : \text{the real étale algebra corresponding to } V_{\mathbb{R}}^{(i)} \text{ is in } \Sigma_\infty\}$$

and

$$S(\Sigma) = S_{\text{fin}}(\Sigma) \cap \Big(\bigcup_{i \in S(\Sigma_\infty)} V_{\mathbb{Z}}^{(i)} \Big),$$

so that the irreducible elements of $S(\Sigma)$ are precisely the lattice points $x \in V_{\mathbb{Z}}$ corresponding to maximal orders in degree n number fields satisfying the local conditions Σ. Since $N_{\text{stab}}(X; S(\Sigma))$ counts generic orbits of such elements, it follows that

$$N_{\text{stab}}(X; S(\Sigma)) = N_{\mathbb{Q},n}(X; \Sigma).$$

Since stabilisers of points in $V_{\mathbb{R}}$ correspond to automorphism groups of étale algebras, each $L \in \Sigma_\infty$ has

$$\# \operatorname{Aut}(L/\mathbb{R}) = n_i,$$

where L corresponds to the real orbit $V_{\mathbb{R}}^{(i)}$, so

$$\sum_{i \in S(\Sigma_\infty)} \frac{1}{n_i} = m(\Sigma_\infty).$$

Therefore, we have

$$\begin{aligned} N_{\mathbb{Q},n}(X;\Sigma) &= N_{\mathrm{stab}}(X; S(\Sigma)) \\ &= \sum_{i \in S(\Sigma_\infty)} N_{\mathrm{stab}}^{(i)}(X; S_{\mathrm{fin}}(\Sigma)) \\ &\sim \frac{1}{2} \prod_{v \in \Pi_{\mathbb{Q}}} m(\Sigma_v) \cdot X. \end{aligned}$$

This is precisely Theorem 3.53, in the special case $k = \mathbb{Q}$.

Part 3. Counting wildly ramified quartic extensions with prescribed discriminant and Galois closure group

5. Introduction

By a 2-*adic field*, we mean a finite field extension of the 2-adic numbers $\mathbb{Q}_2$. Recall that the *Galois closure group* of a field extension L/F is the Galois group of its Galois closure. Recall also that we write $\text{Ét}_{n/F}$ for the set of isomorphism classes of degree n étale algebras over F, and $\text{Ét}_{\sigma/F}$ for the set of étale algebras with a given splitting symbol σ. Moreover, for an integer m, we add the subscript m to specialise to étale algebras with discriminant valuation m. That is, we define

$$\text{Ét}_{n/F,m} = \{L \in \text{Ét}_{n/F} : v_F(d_{L/F}) = m\}$$

and

$$\text{Ét}_{\sigma/F,m} = \text{Ét}_{n/F,m} \cap \text{Ét}_{\sigma/F}.$$

In particular, $\text{Ét}_{(1^n)/F}$ denotes the set of all totally ramified degree n field extensions of F, and $\text{Ét}_{(1^n)/F,m}$ is the set of such extensions with discriminant valuation m. For a p-adic field F, write q_F for the size of its residue field. Recall that the *pre-mass* of a set $S \subseteq \text{Ét}_{n/F}$ is the quantity

$$\widetilde{m}(S) = \sum_{L\in S} \frac{1}{\#\operatorname{Aut}(L/F)} \cdot q_F^{-v_F(d_{L/F})},$$

for all choices of n and F. Earlier, in Theorem 3.3, we stated Serre's mass formula, which is probably the most famous result concerning mass. Serre's formula states that

$$\widetilde{m}(\text{Ét}_{(1^n)/F}) = \frac{1}{q_F^{n-1}}.$$

Given a finite group G, write $\text{Ét}_{n/F}^{G/F}$ for the set of $L \in \text{Ét}_{n/F}$ such that L/F is a field extension with Galois closure group isomorphic to G. Define $\text{Ét}_{\sigma/F}^{G/F}$ similarly, where σ is any splitting symbol of the form (f^e). When $n = 4$, each $L \in \text{Ét}_{(1^4)/F}$ has Galois closure group among S_4, A_4, D_4, V_4, and C_4. The main objective of Part 3 is to obtain, for each such group G, a formula for the pre-mass

$$\widetilde{m}(\text{Ét}_{(1^4)/F}^{G/F}),$$

where F is an arbitrary 2-adic field. In order to obtain this mass formula, we actually compute the size of the set

$$\text{Ét}_{(1^4)/F,m}^{G/F} = \big\{L \in \text{Ét}_{(1^4)/F}^{G/F} : v_F(d_{L/F}) = m\big\},$$

for each G and m, whenever F is a 2-adic field.

Remark 5.1. It would perhaps have been more natural to let G be a permutation group and define $\text{Ét}_{n/F}^{G/F}$ to be the set of all étale algebras with Galois permutation group isomorphic to G. We have opted not to do this, because it would make our results less convenient to state.

Remark 5.2. Our discussion so far has been focused on mass formulae, but the quantities

$$\#\text{Ét}_{(1^4)/F,m}^{G/F}$$

are natural to consider in their own right; there are finitely many such objects, so it makes sense to ask how many. Questions of this sort were already studied by Krasner in [Kra66, Théorème 1], where he gives a formula for the size $\#\text{Ét}_{(1^n)/F,m}$, for each m and n. More recently, Sinclair [Sin15] and Pauli–Sinclair [PS15] refined Krasner's formula by enumerating the elements of $\acute{\mathrm{E}}\mathrm{t}_{(1^n)/F,m}$ with certain prescribed ramification polygons (along with some other invariants). In the Galois group direction, Wei and Ji [WJ07] enumerated the sets $\acute{\mathrm{E}}\mathrm{t}_{4/F}^{S_4/F}$ and $\acute{\mathrm{E}}\mathrm{t}_{4/F}^{A_4/F}$, without imposing conditions on discriminant. The problem we are solving can be viewed as a combination of the flavours of [PS15] and [WJ07]; we take Pauli–Sinclair's prescribed discriminant valuations, but replace their invariants with the Galois closure groups of Wei–Ji.

5.1. **Outline and key results.**

Given a 2-adic field F, write e_F and f_F for the absolute ramification index and absolute inertia degree of F, respectively, so $q_F = 2^{f_F}$. When the choice of field F is clear, we will drop the subscript and write q for q_F. In Section 6, we use a result of Serre to relate

$$\#\left(\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{S_4/F} \cup \acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{A_4/F}\right)$$

to the density of the corresponding Eisenstein polynomials. We then find explicit congruence conditions for these Eisenstein polynomials and use them to compute the required density. Finally, we establish conditions for distinguishing between $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{S_4/F}$ and $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{A_4/F}$, which we use to obtain the following two results:

Theorem 5.3. *Suppose that f_F is even. Then $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{S_4/F}$ is empty for all m. Moreover, $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{A_4/F}$ is nonempty if and only if m is an even integer with $4 \le m \le 6e_F + 2$. In that case, we have*

$$\#\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{A_4/F} = \begin{cases} \frac{1}{3} q^{\lfloor \frac{m}{3} \rfloor - 2}(q^2-1) & \text{if } 3 \mid m, \\ q^{\lfloor \frac{m}{3} \rfloor - 1}(q-1) & \text{if } 3 \nmid m. \end{cases}$$

Theorem 5.4. *Suppose that f_F is odd.*

- *The set $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{S_4/F}$ is nonempty if and only if $m \in 2\mathbb{Z} \setminus 6\mathbb{Z}$ and $4 \le m \le 6e_F + 2$. In that case, we have*
$$\#\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{S_4/F} = q^{\lfloor \frac{m}{3} \rfloor - 1}(q-1).$$
- *The set $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{A_4/F}$ is nonempty if and only if m is a multiple of 6 and $6 \le m \le 6e_F$. In that case, we have*
$$\#\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{A_4/F} = \frac{1}{3} \cdot q^{\lfloor \frac{m}{3} \rfloor - 2}(q^2-1).$$

The case V_4 was addressed by Tunnell in [Tun78]. We repackage his result in Section 7 as the following theorem:

Theorem 5.5. *If $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{V_4/F}$ is nonempty, then m is an even integer with $6 \le m \le 6e_F + 2$. For all such m, we have*

$$\#\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{V_4/F} = 2(q-1)q^{\frac{m-4}{2}}\left(q^{-\lfloor \frac{m}{6} \rfloor}(1 + \mathbb{1}_{3\mid m} \cdot \frac{q-2}{3}) - \mathbb{1}_{m \le 4e_F + 2} \cdot q^{-\lfloor \frac{m-2}{4} \rfloor}\right).$$

The bulk of our work goes into the C_4 case, which spans Section 8. In [CDO05], Cohen, Diaz y Diaz, and Olivier obtain asymptotic formulae for the number of C_4-extensions of a number field. We adapt their methods to compute the size of $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{C_4/F}$. Our formula depends on the discriminant valuation

$$d_{(-1)} = v_F(d_{F(\sqrt{-1})/F}),$$

which is an even integer by Lemma 8.16.

Theorem 5.6. *If $\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m}$ is nonempty, then either $m = 8e_F + 3$ or m is an even integer with $8 \leq m \leq 8e_F$. For even m with $8 \leq m \leq 8e_F$, the number $\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m}$ is the sum of the following four quantities:*

(1) $\mathbb{1}_{8\leq m\leq 5e_F-2} \cdot \mathbb{1}_{m\equiv 3 \pmod 5} \cdot 2q^{\frac{3m-14}{10}}(q-1)$.
(2) $\mathbb{1}_{4e_F+4\leq m\leq 5e_F+2} \cdot 2q^{\frac{m}{2}-e_F-2}(q-1)$.
(3) $\mathbb{1}_{5e_F+3\leq m\leq 8e_F} \cdot \mathbb{1}_{m\equiv 2e_F \pmod 3} \cdot 2q^{\frac{m+4e_F}{6}-1}(1+\mathbb{1}_{m\leq 8e_F-3d_{(-1)}})(q-1-\mathbb{1}_{m=8e_F-3d_{(-1)}+6})$.
(4) $\mathbb{1}_{10\leq m\leq 5e_F} \cdot 2(q-1)(q^{\lfloor\frac{3m}{10}\rfloor-1} - q^{\max\{\lceil\frac{m+2}{4}\rceil,\frac{m}{2}-e_F\}-2})$.

We also have

$$\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,8e_F+3} = \begin{cases} 4q^{2e_F} & \textit{if } -1 \in F^{\times 2}, \\ 2q^{2e_F} & \textit{if } F(\sqrt{-1})/F \textit{ is quadratic and totally ramified,} \\ 0 \quad \textit{if } F(\sqrt{-1})/F \textit{ is quadratic and unramified.} \end{cases}$$

Finally, in Section 9, we compute the number of towers of two quadratic extensions $L/E/F$ with $v_F(d_{L/F}) = m$ and express this number in terms of $\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m}$, $\#\acute{\mathrm{E}}\mathrm{t}^{V_4/F}_{(1^4)/F,m}$, and $\#\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F,m}$. Rearranging, we obtain:

Theorem 5.7. *If $\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F,m}$ is nonempty, then one of the following holds:*

(1) m *is an even integer with* $6 \leq m \leq 8e_F + 2$.
(2) $m \equiv 1 \pmod 4$ *and* $4e_F + 5 \leq m \leq 8e_F + 1$.
(3) $m = 8e_F + 3$.

For even m with $6 \leq m \leq 8e_F + 2$, we have

$$\begin{aligned}\#\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F,m} = 2(q-1)q^{\frac{m}{2}-2}(\mathbb{1}_{m\geq 4e_F+4} \cdot q^{-e_F} + \mathbb{1}_{m\leq 8e_F} \cdot (q^{\min\{0,e_F+1-\lceil\frac{m}{4}\rceil\}} - q^{-\min\{\lfloor\frac{m-2}{4}\rfloor,e_F\}})) \\ - \frac{1}{2}\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m} - \frac{3}{2}\#\acute{\mathrm{E}}\mathrm{t}^{V_4/F}_{(1^4)/F,m}.\end{aligned}$$

For $m \equiv 1 \pmod 4$ with $4e_F + 5 \leq m \leq 8e_F + 1$, we have

$$\#\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F,m} = 2(q-1)q^{e_F+\frac{m-1}{4}-1} - \frac{1}{2}\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m} - \frac{3}{2}\#\acute{\mathrm{E}}\mathrm{t}^{V_4/F}_{(1^4)/F,m}.$$

If $m = 8e_F + 3$, then

$$\#\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F,m} = 2q^{3e_F} - \frac{1}{2}\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,8e_F+3}.$$

Theorems 5.5 and 5.6 make these expressions completely explicit.

5.2. **Application: refinements of Serre's mass formula.**

As we discussed in Part 2, masses play a vital role in the Malle–Bhargava heuristics, which are our best tool for understanding S_n-n-ic extensions. We use the results of Section 5.1 to find explicit formulae for $\widetilde{m}(\acute{\mathrm{E}}\mathrm{t}^{G/F}_{(1^4)/F})$ for each G, which we state in the current subsection. The proofs are deferred to later sections.

Our results find genuine application in upcoming work of Newton–Varma, which uses a slightly modified version of Corollary 5.11. More generally, we expect our refined mass formulae to be useful for obtaining explicit masses when counting S_4-quartic extensions with local conditions. In our own work in Part 4, we will apply the theory to our concrete number field counting problem.

Corollary 5.8. *If f_F is even, then*

$$\widetilde{m}\big(\text{Ét}^{S_4/F}_{(1^4)/F}\big) = 0,$$

and

$$\widetilde{m}\big(\text{Ét}^{A_4/F}_{(1^4)/F}\big) = \frac{1}{3}(q-1)\cdot\frac{q^{4e_F}-1}{q^4-1}\cdot q^{-4e_F-3}\Big(3q^3+q^2+q+3\Big).$$

Corollary 5.9. *Suppose that f_F is odd. Then*

$$\widetilde{m}\big(\text{Ét}^{S_4/F}_{(1^4)/F}\big) = \frac{q^3+1}{q^3+q^2+q+1}\cdot(q^{-3}-q^{-4e_F-3}),$$

and

$$\widetilde{m}\big(\text{Ét}^{A_4/F}_{(1^4)/F}\big) = \frac{1}{3}\cdot\frac{1}{q^2+1}\cdot(q^{-2}-q^{-4e_F-2}).$$

Corollary 5.10. *We have*

$$\widetilde{m}\big(\text{Ét}^{V_4/F}_{(1^4)/F}\big) = \frac{q-1}{6}\cdot\Big(q^{-4e_F-3}\cdot\frac{q^{4e_F}-1}{q^4-1}\cdot(3q^3+q^2+q+3) - 3q^{-3e_F-3}\cdot\frac{q^{3e_F}-1}{q^3-1}\cdot(q^2+1)\Big).$$

Corollary 5.11. *The mass $\widetilde{m}\big(\text{Ét}^{C_4/F}_{(1^4)/F}\big)$ is the sum of the following nine quantities:*

(1)
$$\frac{1}{2}\cdot\frac{(q-1)(1-q^{-7\lfloor\frac{e_F}{2}\rfloor})}{q^7-1}.$$

(2)
$$\frac{1}{2}\cdot q^{-3e_F-3}(1-q^{-\lfloor\frac{e_F}{2}\rfloor}).$$

(3)
$$\mathbb{1}_{d_{(-1)}<e_F}\cdot\frac{(q-1)(q^{-5\lfloor\frac{e_F}{2}\rfloor-e_F-1}-q^{\frac{5}{2}d_{(-1)}-6e_F-1})}{q^5-1}.$$

(4)
$$\frac{1}{2}\cdot\mathbb{1}_{d_{(-1)}\geq 2}\cdot q^{-6e_F+\frac{5}{2}d_{(-1)}-6}(q-2).$$

(5)
$$\frac{1}{2}\cdot\mathbb{1}_{d_{(-1)}\geq 4}\cdot\frac{(q-1)(q^{\frac{5}{2}d_{(-1)}-6e_F-6}-q^{-6e_F-1})}{q^5-1}.$$

(6)
$$\mathbb{1}_{e_F\geq 2}\cdot\frac{1}{2}(q-1)q^{-7\lfloor\frac{e_F}{2}\rfloor-1}\Big(\frac{q(q^{7\lfloor\frac{e_F}{2}\rfloor-7}-1)(q^6+q^4+q^3+q+1)}{q^7-1}+1+\mathbb{1}_{2\nmid e_F}(q^{-2}+q^{-3})\Big).$$

(7)
$$-\mathbb{1}_{e_F\geq 2}\cdot\frac{1}{2}\cdot\frac{(q-1)(q+1)(q^{-7}-q^{-3e_F-1})}{q^3-1}.$$

(8)
$$-\frac{1}{2}q^{-3e_F-2}(1-q^{-\lfloor\frac{e_F}{2}\rfloor}).$$

(9)
$$\begin{cases} q^{-6e_F-3} & \textit{if } -1\in F^{\times 2}, \\ \frac{1}{2}q^{-6e_F-3} & \textit{if } F(\sqrt{-1})/F \textit{ is quadratic and totally ramified}, \\ 0 & \textit{otherwise.} \end{cases}$$

Corollary 5.12. *We have the following formula for* $\widetilde{m}\big(\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F}\big)$*, which is made completely explicit by Corollaries 5.10 and 5.11.*

$$\widetilde{m}\big(\acute{\mathrm{E}}\mathrm{t}^{D_4/F}_{(1^4)/F}\big) = \frac{1}{q^2+q+1}\cdot\big(q^{-3e_F-3}+q^{-3e_F-1}+q^{-2}\big) - \widetilde{m}\big(\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F}\big) - 3\widetilde{m}\big(\acute{\mathrm{E}}\mathrm{t}^{V_4/F}_{(1^4)/F}\big).$$

5.3. **Correctness of results.** Using MAGMA [BCP97] and the LMFDB [LMFDB], we have verified Theorems 5.3-5.7 and Corollaries 5.8-5.12 for all extensions $F/\mathbb{Q}_2$ of degree at most 3. Whenever $e_F \leq 10$ and $f_F \leq 10$, we have also checked numerically the deduction of Corollaries 5.8-5.12 from Theorems 5.3-5.7. Our code is available at `https://github.com/Sebastian-Monnet/Mass-Formula-Checks`.

In Table 1, we state the size of $\mathrm{Ext}^{G/\mathbb{Q}_2}_{(1^4)/\mathbb{Q}_2,m}$ for each m and G. The values in Table 1 are taken from the LMFDB, but it is easy to check that they agree with our formulae in Theorems 5.3-5.7. We find the case with $G = C_4$ and $m = 8$ particularly interesting, since it illustrates the dependence of the count $\#\mathrm{Ext}^{C_4/F}_{(1^4)/F,m}$ on the extension $F(\sqrt{-1})/F$. Since $q = 2$ and $e_F = 1$, Theorem 5.6 tells us that

$$\#\mathrm{Ext}^{C_4/\mathbb{Q}_2}_{(1^4)/\mathbb{Q}_2,8} = 4(1+\mathbb{1}_{d_{(-1)}=0})(1-\mathbb{1}_{d_{(-1)}=2}).$$

Thus, even though we already knew that $\#\mathrm{Ext}^{C_4/\mathbb{Q}_2}_{(1^4)/\mathbb{Q}_2,8} = 0$, our formula tells us *why*; it is precisely because the extension $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$ has discriminant exponent 2.

G m	S_4	A_4	D_4	V_4	C_4
4	1	0	0	0	0
6	0	1	2	0	0
8	2	0	2	4	0
9	0	0	8	0	0
10	0	0	8	0	0
11	0	0	12	0	8

Table 1. Number of totally ramified quartic extensions of $\mathbb{Q}_2$ by discriminant exponent m and Galois group G.

6. The cases $G = S_4$ and $G = A_4$

Fix a 2-adic field F. An *Eisenstein polynomial* over F is a monic polynomial

$$X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in F[X],$$

such that $v_F(a_i) \geq 1$ for all i and $v_F(a_0) = 1$. Write P for the set of quartic Eisenstein polynomials in $F[X]$. For $f \in P$, let L_f be the field $F[X]/(f)$, which is a totally ramified quartic extension of F. Given a finite group G, let P^G be the set of $f \in P$ such that L_f/F has Galois closure group isomorphic to G. For any integer m, let P_m be the set of $f \in P$ such that $v_F(d_{L_f/F}) = m$, or equivalently such that $v_F(\mathrm{disc}(f)) = m$. For each G, write P^G_m for the intersection $P^G \cap P_m$. Write $P^{1-\mathrm{aut}}$ and $P^{1-\mathrm{aut}}_m$ as shorthand[1] for $P^{S_4} \cup P^{A_4}$ and $P^{S_4}_m \cup P^{A_4}_m$ respectively. Similarly, write $\acute{\mathrm{E}}\mathrm{t}^{1-\mathrm{aut}/F}_{(1^4)/F}$ and $\acute{\mathrm{E}}\mathrm{t}^{1-\mathrm{aut}/F}_{(1^4)/F,m}$ for $\acute{\mathrm{E}}\mathrm{t}^{S_4/F}_{(1^4)/F} \cup \acute{\mathrm{E}}\mathrm{t}^{A_4/F}_{(1^4)/F}$ and $\acute{\mathrm{E}}\mathrm{t}^{S_4/F}_{(1^4)/F,m} \cup \acute{\mathrm{E}}\mathrm{t}^{A_4/F}_{(1^4)/F,m}$ respectively.

[1] The superscript "$1-\mathrm{aut}$" refers to the fact that $\#\operatorname{Aut}(L/F) = 1$ if and only if $L \in \acute{\mathrm{E}}\mathrm{t}^{S_4/F}_{(1^4)/F} \cup \acute{\mathrm{E}}\mathrm{t}^{A_4/F}_{(1^4)/F}$.

The quartic Eisenstein polynomials in $F[X]$ embed naturally into $\mathcal{O}_F^4$ via

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \mapsto (a_3, a_2, a_1, a_0).$$

Write μ for the Haar measure on $\mathcal{O}_F^4$, normalised such that $\mu(\mathcal{O}_F^4) = 1$. We will apply this Haar measure to sets of Eisenstein polynomials, viewed as subsets of $\mathcal{O}_F^4$ via the embedding described above.

Lemma 6.1. *Let $G \in \{S_4, A_4\}$, and let m be a positive integer. We have*

$$\#\acute{\mathrm{E}}\mathrm{t}^{G/F}_{(1^4)/F,m} = \frac{q^{m+2}}{q-1} \cdot \mu(P^G_m).$$

Proof. This follows easily from [Ser78, Equation 13]. □

So our problem reduces to finding the density of Eisenstein polynomials that give rise to the desired Galois closure groups. We will do this by establishing explicit congruence conditions on the polynomials for this to be the case.

6.1. **Congruence conditions for $P_m^{1-\mathrm{aut}}$.** In [Lbe09, Theorem 2.9], Lbekkouri gives congruence conditions for a quartic Eisenstein polynomial $f(X) \in \mathbb{Q}_2[X]$ to define a Galois extension. We extend his methods to Eisenstein polynomials over arbitrary 2-adic base fields, to obtain congruence conditions for the set $P_m^{1-\mathrm{aut}}$, which we will state in Lemma 6.4 and Corollary 6.7.

It should be noted that Lbekkouri's statement of [Lbe09, Theorem 2.9] is incorrect. In items (2i) and (2ii), both instances of "$a_0 + a_2$" should read "$a_0 + 2$". This typo is first introduced in the statement of Proposition 2.8 and is carried over into Theorem 2.9.

For $f \in P$, we will always denote the coefficients of f by $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$. Whenever we refer to the coefficients a_i, the choice of f will be clear. Let $\pi_f = X + (f)$ be the natural uniformiser of L_f. We will always drop the subscript and denote π_f by π, since our choice of f will be clear. Write v_π for the 2-adic valuation on L_f, normalised such that $v_\pi(\pi) = 1$. Fix an algebraic closure $\overline{F}$ of L_f, and let

$$\sigma_i : L_f \to \overline{F}, \quad i = 1, 2, 3, 4$$

be the four embeddings of L_f, where σ_1 is the identity embedding. For elements α of algebraic extensions of F, we will write $v_F(\alpha)$ as shorthand for $\widetilde{v}_F(\alpha)$, where $\widetilde{v}_F$ is the unique extension of v_F to the algebraic closure $\overline{F}$ of F.

Lemma 6.2. *For all $f \in P^{1-\mathrm{aut}}$, the three valuations*

$$v_F(\sigma_i(\pi) - \pi), \quad i = 2, 3, 4$$

are equal.

Proof. Suppose that $f \in P$ and the quantities $v_F(\sigma_i(\pi) - \pi)$ are not all equal for $i = 2, 3, 4$. Reordering the σ_i if necessary, we have

$$v_F(\sigma_2(\pi) - \pi) \neq v_F(\sigma_i(\pi) - \pi)$$

for $i = 3$ and $i = 4$. The cubic polynomial $X^{-1}f(X + \pi) \in L_f[X]$ has roots

$$\sigma_i(\pi) - \pi, \quad i = 2, 3, 4.$$

Therefore, the minimal polynomial of $\sigma_2(\pi)-\pi$ over L_f divides $X^{-1}f(X+\pi)$, and all its roots have the same valuation, so

$$\sigma_2(\pi)-\pi \in L_f,$$

and therefore f has at least two roots in L_f, so $f \notin P^{1-\mathrm{aut}}$. □

For each even integer $4 \leq m \leq 6e_F+2$, define T_m to be the set of $f \in P$ such that

$$\begin{cases} v_F(a_1) = \frac{m}{4}, \quad v_F(a_2) \geq \frac{m}{6}, \quad v_F(a_3) \geq \frac{m}{4}, & \text{if } m \equiv 0 \pmod 4, \\ v_F(a_1) \geq \frac{m+2}{4}, \quad v_F(a_2) \geq \frac{m}{6}, \quad v_F(a_3) = \frac{m-2}{4}, & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

Lemma 6.3. *The following two statements are true:*

(1) Let m be an even integer with $4 \leq m \leq 6e_F+2$ and let $f \in P_m$. Then $f \in T_m$ if and only if

$$v_F(\sigma_i(\pi)-\pi) = \frac{m}{12}$$

for $i = 2, 3, 4$.

(2) Let m be a positive integer. If $P_m^{1-\mathrm{aut}}$ is nonempty then m is even, $4 \leq m \leq 6e_F+2$, and $P_m^{1-\mathrm{aut}} \subseteq T_m$.

Proof. Let $f \in P_m$ for any positive integer m, not necessarily even. Define the polynomial

$$g(X) := X^{-1}f(X+\pi),$$

and write $g(X) = \sum_{i=0}^{3} b_i X^i$ for $b_i \in L_f$. It is easy to see that

$$\begin{aligned} b_0 &= a_1 + 2\pi a_2 + 3\pi^2 a_3 + 4\pi^3, \\ b_1 &= a_2 + 3\pi a_3 + 6\pi^2, \\ b_2 &= a_3 + 4\pi. \end{aligned}$$

Since the $v_\pi(a_i)$ are all multiples of 4, we have

$$\begin{aligned} v_\pi(b_0) &= \min\{v_\pi(a_1), v_\pi(2\pi a_2), v_\pi(3\pi^2 a_3), v_\pi(4\pi^3)\}, \\ v_\pi(b_1) &= \min\{v_\pi(a_2), v_\pi(3\pi a_3), v_\pi(6\pi^2)\}, \\ v_\pi(b_2) &= \min\{v_\pi(a_3), v_\pi(4\pi)\}. \end{aligned}$$

The polynomial $g(X) \in L_f[X]$ has roots $\sigma_i(\pi)-\pi$ for $i = 2, 3, 4$. Suppose that

$$v_F(\sigma_i(\pi)-\pi) = \frac{m}{12}$$

for each i. Then the Newton polygon of $g(X)$ consists of one line segment $(0, m) \leftrightarrow (3, 0)$, so

$$(*) \qquad \begin{cases} m = \min\{v_\pi(a_1), v_\pi(2\pi a_2), v_\pi(3\pi^2 a_3), v_\pi(4\pi^3)\}, \\ \frac{2m}{3} \leq \min\{v_\pi(a_2), v_\pi(3\pi a_3), v_\pi(6\pi^2)\}, \\ \frac{m}{3} \leq \min\{v_\pi(a_3), v_\pi(4\pi)\}, \end{cases}$$

and for even m this implies membership of T_m. Reversing the argument, it is easy to see that for even m with $4 \leq m \leq 6e_F+2$, every $f \in T_m$ has

$$v_F(\sigma_i(\pi)-\pi) = \frac{m}{12}, \quad i = 2, 3, 4.$$

Thus we have proven (1). Now let $f \in P_m^{1-\mathrm{aut}}$ for some positive integer m. Then Lemma 6.2 implies that

$$v_F(\sigma_i(\pi)-\pi) = \frac{m}{12}$$

for $i = 2, 3, 4$, and we have shown that this implies Equation $(*)$, so

$$\begin{cases} m = \min\{v_\pi(a_1), v_\pi(a_2) + 4e_F + 1, v_\pi(a_3) + 2, 8e_F + 3\}, \\ \frac{2m}{3} \leq \min\{v_\pi(a_2), 4e_F + 2\}. \end{cases}$$

Since f is Eisenstein, $v_\pi(a_i) \geq 4$ for each i, and therefore $4 \leq m \leq 6e_F + 3$. Moreover, $v_\pi(a_2) \geq \frac{2m}{3}$ implies that $m \leq v_\pi(a_2) + 2e_F + 1$, so $m \neq v_\pi(a_2) + 4e_F + 1$. Since $m < 8e_F + 3$, we obtain

$$m = \min\{v_\pi(a_1), v_\pi(a_3) + 2\},$$

so m is even, so in fact $4 \leq m \leq 6e_F + 2$. Finally, Part (1) of this lemma shows that $f \in T_m$, completing the proof of (2). □

Lemma 6.4. *Let m be an even integer with $4 \leq m \leq 6e_F + 2$. If m is not a multiple of 3, then $P_m^{1-\mathrm{aut}} = T_m$.*

Proof. Lemma 6.3 tells us that $P_m^{1-\mathrm{aut}} \subseteq T_m$, so we just need to show that $T_m \subseteq P_m^{1-\mathrm{aut}}$. Let $f \in T_m$. Lemma 6.3 tells us that

$$v_\pi(\sigma_i(\pi) - \pi) = \frac{m}{3}, \quad i = 2, 3, 4,$$

so $\sigma_i(\pi) \notin L_f$ for each i, since $\frac{m}{3}$ is not an integer, and therefore $T_m \subseteq P_m^{1-\mathrm{aut}}$. □

From now on, fix a system of representatives $\mathcal{R}$ for $(\mathcal{O}_F/\mathfrak{p}_F)^\times$. When $3 \mid m$, for each $u \in \mathcal{R}$ and $f \in P_m$, define the polynomial

$$g_f^{(u)}(X) := f(X + \pi + u\pi^{\frac{m}{3}}),$$

and write $g_f^{(u)}(X) = \sum_{i=0}^4 b_i^{(u)} X^i$ for $b_i^{(u)} \in L_f$. We will always omit the subscript and write $g^{(u)}(X)$ for $g_f^{(u)}(X)$, leaving f implicit.

Lemma 6.5. *Let m be a multiple of 6 with $4 \leq m \leq 6e_F + 2$. Let $f \in T_m$ and $u \in \mathcal{R}$. The following four statements are true:*

(1) $v_F(b_3^{(u)}) \geq \frac{m-2}{4}$.
(2) $v_F(b_2^{(u)}) \geq \frac{m}{6}$.
(3) $v_F(b_1^{(u)}) = \frac{m}{4}$.
(4)

$$v_F(b_0^{(u)}) \begin{cases} \geq \frac{m}{3} + 1 & \textit{if } 4 \mid m \textit{ and } a_1 + ua_2a_0^{\frac{m}{12}} + u^3a_0^{\frac{m}{4}} \equiv 0 \pmod{\mathfrak{p}_F^{\frac{m}{4}+1}}, \\ \geq \frac{m}{3} + 1 & \textit{if } 4 \nmid m \textit{ and } a_3 + ua_2a_0^{\lfloor\frac{m}{12}\rfloor} + u^3a_0^{\lfloor\frac{m}{4}\rfloor} \equiv 0 \pmod{\mathfrak{p}_F^{\lfloor\frac{m}{4}\rfloor+1}}, \\ = \frac{m}{3} & \textit{otherwise.} \end{cases}$$

Proof. It is easy to see that for each i and u, we have

$$b_i^{(u)} = \sum_{j=i}^{4} \binom{j}{i} a_j(\pi + u\pi^{\frac{m}{3}})^{j-i},$$

where we adopt the convention that $a_4 = 1$. Using this formula for the $b_i^{(u)}$, along with the congruence conditions defining T_m, gives us the following three congruences:

$$b_3^{(u)} \equiv a_3 \pmod{\pi^{m+1}}.$$
$$b_2^{(u)} \equiv a_2 \pmod{\pi^{\frac{2m}{3}+1}}.$$
$$b_1^{(u)} \equiv \begin{cases} a_1 \pmod{\pi^{m+1}} & \text{if } m \equiv 0 \pmod{4}, \\ 3\pi^2 a_3 \pmod{\pi^{m+1}} & \text{if } m \equiv 2 \pmod{4}. \end{cases}$$

We can read off the first three claims from these congruences. Expanding the formula for $b_0^{(u)}$ and ignoring the high-valuation terms, we obtain

$$b_0^{(u)} \equiv \begin{cases} ua_1\pi^{\frac{m}{3}} + u^2a_2\pi^{\frac{2m}{3}} + u^4\pi^{\frac{4m}{3}} \pmod{\pi^{\frac{4m}{3}+1}} & \text{if } m \equiv 0 \pmod{4}, \\ u^2a_2\pi^{\frac{2m}{3}} + ua_3\pi^{\frac{m}{3}+2} + u^4\pi^{\frac{4m}{3}} \pmod{\pi^{\frac{4m}{3}+1}} & \text{if } m \equiv 2 \pmod{4}. \end{cases}$$

It follows that $v_F(b_0^{(u)}) \geq \frac{m}{3}$, and $v_F(b_0^{(u)}) \geq \frac{m}{3} + 1$ if and only if

$$\begin{cases} a_1 + ua_2\pi^{\frac{m}{3}} + u^3\pi^m \equiv 0 \pmod{\pi^{m+1}} & \text{if } m \equiv 0 \pmod{4}, \\ a_3 + ua_2\pi^{\frac{m}{3}-2} + u^3\pi^{m-2} \equiv 0 \pmod{\pi^{m-1}} & \text{if } m \equiv 2 \pmod{4}. \end{cases}$$

The result then follows from the fact that[1], for any positive integer k, we have

$$\pi^{4k} \equiv (-a_0)^k \pmod{\pi^{4k+\frac{2m}{3}-2}}.$$

□

Lemma 6.6. *Let $4 \leq m \leq 6e_F + 2$ be a multiple of 6 and let $f \in T_m$. Then $f \notin P_m^{1-\mathrm{aut}}$ if and only if $v_F(b_0^{(u)}) \geq \frac{m}{3} + 1$ for some $u \in \mathcal{R}$.*

Proof. Suppose that $f \notin P_m^{1-\mathrm{aut}}$. Then f has at least two roots in L_f. Reordering the σ_i if necessary, we may assume that $\sigma_2(\pi) \in L_f$. Since $f \in T_m$, it follows from Lemma 6.3 that $v_F(\sigma_2(\pi) - \pi) = \frac{m}{12}$, so

$$\sigma_2(\pi) = \pi + \tilde{u}\pi^{\frac{m}{3}}$$

for some $\tilde{u} \in \mathcal{O}_{L_f}^\times$. Since L_f/F is totally ramified, there is some $u \in \mathcal{R}$ with $u \equiv \tilde{u} \pmod{\pi}$, which means that

$$v_F\big(\sigma_2(\pi) - \pi - u\pi^{\frac{m}{3}}\big) > \frac{m}{12}.$$

The other three roots of $g^{(u)}$ all have valuation at least $\frac{m}{12}$, so

$$v_F(b_0^{(u)}) \geq \frac{m}{3} + 1.$$

Suppose conversely that $v_F(b_0^{(u)}) \geq \frac{m}{3} + 1$ for some $u \in \mathcal{R}$. Lemma 6.5 tells us that $v_F(b_1^{(u)}) = \frac{m}{4}$ and $v_F(b_2^{(u)}) \geq \frac{m}{6}$, so considering the Newton polygon of $g^{(u)}$ tells us that it has exactly one root $\sigma_i(\pi) - \pi - u\pi^{\frac{m}{3}}$ with

$$v_\pi\big(\sigma_i(\pi) - \pi - u\pi^{\frac{m}{3}}\big) \geq \frac{m}{3} + 1.$$

Therefore we have

$$\sigma_i(\pi) - \pi - u\pi^{\frac{m}{3}} \in L_f,$$

so $\sigma_i(\pi) \in L_f$, which means that $f \notin P^{1-\mathrm{aut}}$. □

[1] This follows from expanding the binomial on the right-hand side of

$$(\pi^4)^k = ((-a_0) + (-a_1\pi - a_2\pi^2 - a_3\pi^3))^k.$$

Corollary 6.7. *Let m be a multiple of 6 with $4 \leq m \leq 6e_F + 2$, and let $f \in T_m$. The following are equivalent:*

(1) We have $f \notin P_m^{1-\mathrm{aut}}$.
(2) There is some $u \in \mathcal{R}$ such that

$$\begin{cases} a_1 + ua_2a_0^{\lfloor \frac{m}{12} \rfloor} + u^3 a_0^{\lfloor \frac{m}{4} \rfloor} \equiv 0 \pmod{\mathfrak{p}_F^{\lfloor \frac{m}{4} \rfloor + 1}} & \textit{if } m \equiv 0 \pmod 4, \\ a_3 + ua_2a_0^{\lfloor \frac{m}{12} \rfloor} + u^3 a_0^{\lfloor \frac{m}{4} \rfloor} \equiv 0 \pmod{\mathfrak{p}_F^{\lfloor \frac{m}{4} \rfloor + 1}} & \textit{if } m \equiv 2 \pmod 4. \end{cases}$$

Proof. This is immediate from Lemmas 6.5 and 6.6. □

Remark 6.8. The examiners pointed out a much slicker proof of Corollary 6.7. We have opted to retain our original proof, as we would like this thesis to be a record of our personal experience and thought process during the PhD. However, since the examiners' proof is nicer than ours, we include a sketch of it here. Recall that, given $f \in T_m$ with $6 \mid m$, we defined $g(X) = \frac{1}{X} f(X + \pi)$, whose roots are $\sigma_i(\pi) - \pi$ for $i = 2, 3, 4$. We may then define $h(X) = \frac{1}{\pi^m} g(\pi^{\frac{m}{3}} X)$, whose roots are $\frac{\sigma_i(\pi) - \pi}{\pi^{\frac{m}{3}}}$, for $i = 2, 3, 4$. The differences between these roots have discriminant valuation 0, so the discriminant of h has valuation 0, and therefore h is separable modulo π, hence Hensel's Lemma tells us that it has a root in L_f if and only if it has a root modulo π. Thus, $f \notin P_m^{1-\mathrm{aut}}$ if and only if h has a root modulo π, which is equivalent to the existence of an element $u \in \mathcal{R}$ with

$$\frac{b_0}{\pi^m} + \frac{b_1}{\pi^{\frac{2m}{3}}} u + \frac{b_2}{\pi^{\frac{m}{3}}} u^2 + u^3 \equiv 0 \pmod{\pi}.$$

Using the expressions for the coefficients b_i in the proof of Lemma 6.3, and the definition of T_m, this reduces to Condition (2) in Corollary 6.7. Moreover, since h is separable modulo π, its splitting field over L_f is unramified, hence cyclic, which implies that the splitting field of f over F is an A_4-extension, rather than an S_4-extension.

6.2. **Computing the densities.**

Lemma 6.9. *Let m be an even integer with $4 \leq m \leq 6e_F + 2$. Then*

$$\mu(T_m) = q^{-\lceil \frac{2m}{3} \rceil - 3}(q-1)^2.$$

Proof. This is easy to see from the definition of T_m. □

Since $\mathbb{F}_F \cong \mathbb{F}_{2^{f_F}}$, the Galois group $\mathrm{Gal}(\mathbb{F}_F/\mathbb{F}_2)$ is generated by the squaring map. Therefore, the trace map $\mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2} : \mathbb{F}_F \to \mathbb{F}_2$ is given by

$$\mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}(x) = x + x^2 + \ldots + x^{2^{f_F - 1}}.$$

Lemma 6.10. *Let $\alpha, \beta, \gamma \in \mathbb{F}_F$ with $\alpha \neq 0$, and let g be the polynomial $\alpha X^2 + \beta X + \gamma$ in $\mathbb{F}_F[X]$. The number of roots of g in $\mathbb{F}_F$ is*

$$\begin{cases} 1 & \textit{if } \beta = 0, \\ 2 & \textit{if } \beta \neq 0 \textit{ and } \mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}(\alpha\gamma/\beta^2) = 0, \\ 0 & \textit{if } \beta \neq 0 \textit{ and } \mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}(\alpha\gamma/\beta^2) = 1. \end{cases}$$

Proof. The case with $\beta = 0$ is clear, so assume $\beta \neq 0$. Let u be a root of g in a splitting field over $\mathbb{F}_F$, and let $\theta = \frac{\alpha u}{\beta}$. Clearly $u \in \mathbb{F}_F$ if and only if $\theta \in \mathbb{F}_F$, which is equivalent to $\theta + \theta^q = 0$.

Since

$$\mathrm{Gal}(\mathbb{F}_F/\mathbb{F}_2) = \{x \mapsto x^{2^i} : i = 0, 1, \dots, f_F - 1\},$$

it is easy to see that

$$\mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}(\theta + \theta^2) = \theta + \theta^q,$$

and also that

$$\theta + \theta^2 = \frac{\alpha\gamma}{\beta^2}.$$

Therefore, $u \in \mathbb{F}_F$ if and only if $\mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}(\frac{\alpha\gamma}{\beta^2}) = 0$, and the result follows. □

Lemma 6.11. *Let $n \geq 0$ be an integer and let $\lambda, \mu \in \mathfrak{p}_F^n$, with $\mu \notin \mathfrak{p}_F^{n+1}$. Define the map*

$$\alpha : \mathcal{O}_F/\mathfrak{p}_F \to \mathcal{O}_F/\mathfrak{p}_F^{n+1}, \quad c \mapsto \lambda c + \mu c^3.$$

The following two statements are true:

(1) For $c \in (\mathcal{O}_F/\mathfrak{p}_F)^\times$, we have

$$\#\big\{c' \in (\mathcal{O}_F/\mathfrak{p}_F)^\times : \alpha(c') = \alpha(c)\big\} = \begin{cases} 1 & \text{if } c^2 \equiv \lambda/\mu \pmod{\mathfrak{p}_F}, \\ 1 & \text{if } c^2 \not\equiv \lambda/\mu \text{ and } \mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}\left(\frac{\lambda}{c^2\mu}\right) \not\equiv f_F \pmod{2}, \\ 3 & \text{if } c^2 \not\equiv \lambda/\mu \text{ and } \mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}\left(\frac{\lambda}{c^2\mu}\right) \equiv f_F \pmod{2}. \end{cases}$$

(2) We have

$$\#\operatorname{im}\alpha = \begin{cases} \frac{2q+(-1)^{f_F}}{3} & \text{if } \lambda \notin \mathfrak{p}_F^{n+1}, \\ \frac{q+1+(-1)^{f_F}}{2+(-1)^{f_F}} & \text{if } \lambda \in \mathfrak{p}_F^{n+1}. \end{cases}$$

Proof. It is easy to see that for $c, c' \in (\mathcal{O}_F/\mathfrak{p}_F)^\times$, we have $\alpha(c) = \alpha(c')$ if and only if

$$(c - c')\Big((c')^2 + cc' + \frac{\lambda}{\mu} + c^2\Big) \equiv 0 \pmod{\mathfrak{p}_F}.$$

The first statement then follows from Lemma 6.10. For the second statement, suppose first that $\lambda \notin \mathfrak{p}_F^{n+1}$. Then there is some $c \in (\mathcal{O}_F/\mathfrak{p}_F)^\times$ with $\alpha(c) = 0$, so

$$\begin{aligned} \#\operatorname{im}\alpha &= \sum_{c \in (\mathcal{O}_F/\mathfrak{p}_F)^\times} \frac{1}{\#\{c' \in (\mathcal{O}_F/\mathfrak{p}_F)^\times : \alpha(c') = \alpha(c)\}} \\ &= 1 + (q - 2 - a) + \frac{a}{3}, \end{aligned}$$

where

$$a = \#\Big\{c \in (\mathcal{O}_F/\mathfrak{p}_F)^\times : c^2 \not\equiv \frac{\lambda}{\mu} \text{ and } \mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}\Big(\frac{\lambda}{c^2\mu}\Big) \equiv f_F \pmod{2}\Big\}.$$

Since $\lambda \notin \mathfrak{p}_F^{n+1}$, the map

$$(\mathfrak{p}_F/\mathcal{O}_F)^\times \to (\mathfrak{p}_F/\mathcal{O}_F)^\times, \quad c \mapsto \frac{\lambda}{c^2\mu}$$

is a bijection, so

$$\begin{aligned} a &= \#\big\{u \in (\mathcal{O}_F/\mathfrak{p}_F)^\times \setminus \{1\} : \mathrm{Tr}_{\mathbb{F}_F/\mathbb{F}_2}(u) \equiv f_F \pmod{2}\big\} \\ &= \frac{1}{2}\big(q - 3 - (-1)^{f_F}\big), \end{aligned}$$

and the result follows. Now suppose that $\lambda \in \mathfrak{p}_F^{n+1}$. Then $\alpha(c) = 0$ if and only if $c = 0$, so

$$\#\operatorname{im}\alpha = 1 + \sum_{c \in (\mathcal{O}_F/\mathfrak{p}_F)^\times} \frac{1}{\#\{c' \in (\mathcal{O}_F/\mathfrak{p}_F)^\times : \alpha(c') = \alpha(c)\}}.$$

We have $\frac{\lambda}{c^2\mu} \equiv 0 \pmod{\mathfrak{p}_F}$ for all $c \in (\mathcal{O}_F/\mathfrak{p}_F)^\times$, so

$$\#\Big\{c' \in (\mathcal{O}_F/\mathfrak{p}_F)^\times : \alpha(c') = \alpha(c)\Big\} = 2 + (-1)^{f_F},$$

and the result follows. □

Lemma 6.12. *Let a and b be positive integers, and let S be the set of triples $(x_0, x_1, x_2) \in \mathcal{O}_F^3$ such that the following two conditions hold:*

(1) $v_F(x_0) = 1, \quad v_F(x_1) = a + b, \quad v_F(x_2) \geq b.$
(2) There is some $u \in \mathcal{R}$ such that $x_1 + ux_2x_0^a + u^3x_0^{a+b} \equiv 0 \pmod{\mathfrak{p}_F^{a+b+1}}$.

Then $\mu(S) = \frac{1}{3}q^{-a-2b-4}(q-1)^2(2q-1)$.

Proof. Suppose that, for x_i and x_i' in $\mathcal{O}_F$, we have $x_i \equiv x_i' \pmod{\mathfrak{p}_F^{a+b+1}}$ for $i = 0, 1, 2$. Then $(x_0, x_1, x_2) \in S$ if and only if $(x_0', x_1', x_2') \in S$, so

$$\mu(S) = \frac{\#\overline{S}}{q^{3a+3b+3}},$$

where $\overline{S}$ is the set of triples

$$(\bar{x}_0, \bar{x}_1, \bar{x}_2) \in \Big((\mathfrak{p}_F/\mathfrak{p}_F^{a+b+1}) \setminus (\mathfrak{p}_F^2/\mathfrak{p}_F^{a+b+1})\Big) \times \Big((\mathfrak{p}_F^{a+b}/\mathfrak{p}_F^{a+b+1}) \setminus \{0\}\Big) \times \big(\mathfrak{p}_F^b/\mathfrak{p}_F^{a+b+1}\big)$$

such that there is some $u \in \mathcal{R}$ with

$$\bar{x}_1 + u\bar{x}_2\bar{x}_0^a + u^3\bar{x}_0^{a+b} = 0.$$

For each $\bar{x}_0 \in (\mathfrak{p}_F/\mathfrak{p}_F^{a+b+1}) \setminus (\mathfrak{p}_F^2/\mathfrak{p}_F^{a+b+1})$ and $\bar{x}_2 \in \mathfrak{p}_F^b/\mathfrak{p}_F^{a+b+1}$, define the map

$$\alpha_{\bar{x}_0,\bar{x}_2} : \mathcal{O}_F/\mathfrak{p}_F \to \mathfrak{p}_F^{a+b}/\mathfrak{p}_F^{a+b+1}, \quad u \mapsto -u\bar{x}_2\bar{x}_0^a - u^3\bar{x}_0^{a+b}.$$

Then

$$\overline{S} = \bigsqcup_{\substack{\bar{x}_0 \in (\mathfrak{p}_F/\mathfrak{p}_F^{a+b+1}) \setminus (\mathfrak{p}_F^2/\mathfrak{p}_F^{a+b+1}) \\ \bar{x}_2 \in \mathfrak{p}_F^b/\mathfrak{p}_F^{a+b+1}}} \{\bar{x}_0\} \times \Big(\operatorname{im}\alpha_{\bar{x}_0,\bar{x}_2} \setminus \{0\}\Big) \times \{\bar{x}_2\}.$$

Since $\alpha_{\bar{x}_0,\bar{x}_2}(0) = 0$, we always have $0 \in \operatorname{im}\alpha_{\bar{x}_0,\bar{x}_2}$, so

$$\#\Big(\operatorname{im}\alpha_{\bar{x}_0,\bar{x}_2} \setminus \{0\}\Big) = \#\operatorname{im}\alpha_{\bar{x}_0,\bar{x}_2} - 1,$$

and therefore

$$\#\overline{S} = \sum_{\substack{\bar{x}_0 \in (\mathfrak{p}_F/\mathfrak{p}_F^{a+b+1}) \setminus (\mathfrak{p}_F^2/\mathfrak{p}_F^{a+b+1}) \\ \bar{x}_2 \in \mathfrak{p}_F^b/\mathfrak{p}_F^{a+b+1}}} (\#\operatorname{im}\alpha_{\bar{x}_0,\bar{x}_2} - 1),$$

Lemma 6.11 tells us that

$$\#\operatorname{im}\alpha_{\bar{x}_0,\bar{x}_2} = \begin{cases} \frac{2q+(-1)^{f_F}}{3} & \text{if } \bar{x}_2 \notin \mathfrak{p}_F^{b+1}/\mathfrak{p}_F^{a+b+1}, \\ \frac{q+1+(-1)^{f_F}}{2+(-1)^{f_F}} & \text{if } \bar{x}_2 \in \mathfrak{p}_F^{b+1}/\mathfrak{p}_F^{a+b+1}. \end{cases}$$

It follows that

$$\#\overline{S} = \frac{1}{3}q^{2a+b-1}(q-1)^2(2q-1),$$

so

$$\mu(S) = \frac{1}{3}q^{-a-2b-4}(q-1)^2(2q-1).$$

□

Remark 6.13. As was the case in Remark 6.8, the examiners proposed a more elegant proof of Lemma 6.12. For the same reasons as before, we opt to describe their proof in addition to, rather than instead of, our own. Define S' to be the set of triples

$$(y_0, y_1, y_2) \in (\mathfrak{p}_F \setminus \mathfrak{p}_F^2) \times \mathcal{O}_F^\times \times \mathcal{O}_F$$

such that the polynomial $X^3 + y_2X + y_1$ has a root in $\mathbb{F}_F$. Then there is a bijection

$$\varphi : S' \to S, \quad (y_0, y_1, y_2) \mapsto (y_0, y_0^{a+b}y_1, y_0^b y_2).$$

From the definition of φ, it is easy to see that

$$\mu(S) = \frac{1}{q^{a+2b}}\mu(S').$$

By definition of S', we have

$$\mu(S') = \Big(\frac{1}{q} - \frac{1}{q^2}\Big) \cdot \frac{1}{q^2} \cdot \#\big\{(\lambda_1, \lambda_2) \in \mathbb{F}_F^\times \times \mathbb{F}_F : X^3 + \lambda_2X + \lambda_1 \text{ has a root in } \mathbb{F}_F\big\}.$$

The cardinality of the set above is equal to

$$q(q-1) - \#\{\text{irreducible polynomials } X^3 + \lambda_2X + \lambda_1 \text{ in } \mathbb{F}_F[X]\}.$$

Let $\mathbb{F}'$ be the unique cubic field extension of $\mathbb{F}_F$. There is a 3-to-1 surjection

$$\{\alpha \in \mathbb{F}' \setminus \mathbb{F}_F : \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_F}(\alpha) = 0\} \to \{\text{irreducible polynomials } X^3 + \lambda_2X + \lambda_1 \text{ in } \mathbb{F}_F\},$$

taking α to its minimal polynomial over $\mathbb{F}_F$. It is easy to see that

$$\#\{\alpha \in \mathbb{F}' \setminus \mathbb{F}_F : \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_F}(\alpha) = 0\} = q^2 - 1,$$

and the result of Lemma 6.12 follows.

Corollary 6.14. *Let $4 \leq m \leq 6e_F + 2$ be a multiple of 6. Then*

$$\mu(T_m \setminus P_m^{1-\mathrm{aut}}) = \frac{1}{3}q^{-\frac{2m}{3}-4}(q-1)^2(2q-1).$$

Proof. Suppose first that $4 \mid m$. Setting $x_i = a_i$ for $i = 0, 1, 2$ and $(a, b) = (\frac{m}{12}, \frac{m}{6})$, Corollary 6.7 tells us that $T_m \setminus P_m^{1-\mathrm{aut}}$ is the set S from Lemma 6.12, together with the added congruence condition that $v_F(a_3) \geq \frac{m}{4}$, so

$$\mu(T_m \setminus P_m^{1-\mathrm{aut}}) = \mu(S) \cdot q^{-\frac{m}{4}} = \frac{1}{3}q^{-\frac{2m}{3}-4}(q-1)^2(2q-1).$$

If $4 \nmid m$, then set

$$(x_0, x_1, x_2) := (a_0, a_3, a_2), \quad (a, b) = \Big(\frac{m-6}{12}, \frac{m}{6}\Big),$$

and proceed similarly. □

Corollary 6.15. *Let $4 \leq m \leq 6e_F + 2$ be an even integer. Then*

$$\mu(P_m^{1-\mathrm{aut}}) = q^{-\lceil\frac{2m}{3}\rceil-3}(q-1)^2 \cdot \Big(1 + \mathbb{1}_{6|m} \cdot \Big(\frac{1-2q}{3q}\Big)\Big).$$

Proof. This is immediate from Lemma 6.9 and Corollary 6.14. □

Corollary 6.16. *If $\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{1-\mathrm{aut}/F}$ is nonempty, then m is an even integer with $4 \leq m \leq 6e_F + 2$, and*

$$\#\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{1-\mathrm{aut}/F} = q^{\lfloor\frac{m}{3}\rfloor-1}(q-1)\Big(1 + \mathbb{1}_{6|m} \cdot \Big(\frac{1-2q}{3q}\Big)\Big).$$

Proof. This is immediate from Lemma 6.1, Lemma 6.3 Part (2), and Corollary 6.15. □

6.3. **Distinguishing between A_4 and S_4.** Write μ_3 for the group of cube roots of unity in the algebraic closure of F.

Lemma 6.17. *The following three statements are true:*

1. *(Tower law for discriminant) Let $M/L/F$ be extensions of 2-adic fields. Then*
$$v_F(d_{M/F}) = [M:L] \cdot v_F(d_{L/F}) + f(L/F) \cdot v_L(d_{M/L}).$$
2. *We have $\mu_3 \subseteq F$ if and only if f_F is even.*
3. *If $\mu_3 \not\subseteq F$, then F has only one C_3-extension up to isomorphism, namely the unramified extension.*

Proof. Claim (1) is [Ser95, Proposition III.8]. Claim (2) follows from Hensel's Lemma. As for Claim (3), let L/F be a C_3-extension. Then L/F is either unramified or tamely ramified. If L/F is tamely ramified, then it is well-known that $L = F(\sqrt[3]{\pi_F})$ for some uniformiser π_F of F. But then L/F is Galois if and only if $\mu_3 \subseteq F$, proving the claim. □

Lemma 6.18. *If $\mu_3 \subseteq F$, then F has no S_4-extensions.*

Proof. Suppose for contradiction that there is an S_4-extension M/F. Take a copy of D_8 inside S_4, and let $L = M^{D_8}$. Then L/F is cubic. If L/F is unramified, then it is cyclic. On the other hand, if L/F is ramified, then it is tamely ramified, so $L = F(\sqrt[3]{\pi_F})$ for some uniformiser π_F of F, and therefore L/F is Galois since $\mu_3 \subseteq F$. This implies that D_8 is a normal subgroup of S_4, which is not the case, so the result follows by contradiction. □

Proof of Theorem 5.3. By Lemma 6.17(2), we have $\mu_3 \subseteq F$, so Lemma 6.18 tells us that $\mathrm{\acute{E}t}^{A_4/F}_{(1^4)/F,m} = \mathrm{\acute{E}t}^{1-\mathrm{aut}/F}_{(1^4)/F,m}$, and the result follows by Corollary 6.16. □

Lemma 6.19. *Let M/F be a V_4-extension of 2-adic fields, and let E_1, E_2, E_3 be its three quadratic intermediate extensions. Then the following two statements are true:*

1. *We have $v_F(d_{M/F}) = \sum_{i=1}^{3} v_F(d_{E_i/F})$.*
2. *If $v_F(d_{E_1/F}) < v_F(d_{E_2/F})$, then $v_F(d_{E_3/F}) = v_F(d_{E_2/F})$.*

Proof. This proof relies on some class field theory that we will develop in Section 12.2. We feel that developing that theory here would disrupt the flow of the section, so we instead use forward references. This does not introduce circularity, since the proofs of Theorem 12.10, Lemma 12.11, and Lemma 12.12 are self-contained, and do not reference any other results in this thesis.

The first statement follows easily from [Keu23, Theorem 17.50]. For the second statement, suppose that $v_F(d_{E_1/F}) < v_F(d_{E_2/F})$. For each i, let $\chi_i : F^\times/F^{\times 2} \to C_2$ be the quadratic character associated to E_i, as in Lemma 12.12. Theorem 12.10 and Lemma 12.11 tell us that
$$v_F(d_{E_i/F}) = \mathfrak{f}(E_i/F) = \mathfrak{f}(\chi_i),$$
for each i. It is easy to see that $\chi_3 = \chi_1\chi_2$, so $\mathfrak{f}(\chi_3) = \mathfrak{f}(\chi_2)$, and the result follows. □

Lemma 6.20. *Suppose that $\mu_3 \not\subseteq F$ and let $L \in \mathrm{\acute{E}t}^{1-\mathrm{aut}}_{(1^4)/F}$. Then $3 \mid v_F(d_{L/F})$ if and only if L is an A_4-quartic.*

Proof. Suppose that $3 \mid v_F(d_{L/F})$. Then the final line of Remark 6.8 shows that L/F is an A_4-quartic extension. Suppose conversely that L/F is A_4-quartic. Let M be a normal closure of L over F, so $\mathrm{Gal}(M/F) \cong A_4$, and let $K = M^{V_4}$. The extension K/F is a C_3-extension, so it is unramified by Lemma 6.17(3). Since L/F is totally ramified, we have $e(M/F) = 4$ and $f(M/F) = 3$, so V_4 is the inertia group of M/F. Since K/F is unramified, the tower law for discriminant gives

$$v_F(d_{M/F}) = 3v_K(d_{M/K}).$$

Let E_1, E_2, E_3 be the three intermediate extensions of the V_4-extension M/K. Since the three double transpositions in A_4 are conjugate, the extensions E_i/F are isomorphic, so they have the same discriminant. By the tower law for discriminant, it follows that the valuations

$$v_K(d_{E_i/K}), \quad i = 1, 2, 3$$

are all equal. By Lemma 6.19, we have

$$v_K(d_{M/K}) = \sum_{i=1}^{3} v_K(d_{E_i/K}) = 3v_K(d_{E_1/K}),$$

so

$$v_F(d_{M/F}) = 9v_K(d_{E_1/K}).$$

Since M/L is unramified, the tower law also gives

$$v_F(d_{M/F}) = 3v_F(d_{L/F}),$$

and the result follows. □

In the statement and proof of the following lemma, the term “A_4-extension” refers to a Galois extension with Galois group A_4.

Lemma 6.21. *Suppose that $\mu_3 \not\subseteq F$. Then there is a bijection between $\text{Ét}^{A_4/F}_{(1^4)/F}$ and the set of isomorphism classes of A_4-extensions of F.*

Proof. For an A_4-quartic extension L/F, let $\widetilde{L}$ be the normal closure of L over F. The map $L \mapsto \widetilde{L}$ is a well-defined bijection between the set of isomorphism classes of A_4-quartics and the set of isomorphism classes of A_4-extensions. Therefore, to prove the lemma, it suffices to show that every A_4-quartic is totally ramified.

Let L/F be an A_4-quartic. Then there is an extension M/L such that M/F is an A_4-extension and $L = M^{A_3}$ for some choice of embedding $A_3 \subseteq A_4$. Let $G_0 \subseteq A_4$ be the inertia group of M/F. Since M^{V_4}/F is a C_3-extension, it is unramified by Lemma 6.17(3), and therefore $G_0 \subseteq V_4$. Since M/F is not cyclic, it is ramified, so $\#G_0 \geq 2$. Since G_0 is a normal subgroup of A_4, we must have $G_0 = V_4$, so $e(M/F) = 4$. Since M/L is a C_3-extension, it is unramified by Lemma 6.17(3), so L/F is totally ramified, as required. □

Proof of Theorem 5.4. Lemma 6.17(2) tells us that $\mu_3 \not\subseteq F$. The result then follows from Corollary 6.16 and Lemma 6.20. □

Proof of Corollary 5.8. Theorem 5.3 tells us that $\widetilde{m}\big(\text{Ét}^{S_4/F}_{(1^4)/F}\big) = 0$ and

$$\widetilde{m}\big(\text{Ét}^{A_4/F}_{(1^4)/F}\big) = \sum_{\substack{4 \leq m \leq 6e_F + 2 \\ m \text{ even}}} q^{-\lceil \frac{2m}{3} \rceil - 1}(q-1)\Big(1 + \mathbb{1}_{6|m} \cdot \Big(\frac{1-2q}{3q}\Big)\Big).$$

The result then follows from a tedious computation, which we omit since it is straightforward. □

Proof of Corollary 5.9. By Theorem 5.4, we have

$$\widetilde{m}\big(\text{Ét}^{S_4/F}_{(1^4)/F}\big) = \sum_{\substack{4\le m\le 6e_F+2\\ 2\mid m,\ 3\nmid m}} q^{\lfloor \frac{m}{3}\rfloor - m - 1}(q-1),$$

which can easily be rearranged into the required form. The computation of $\widetilde{m}\big(\text{Ét}^{A_4/F}_{(1^4)/F}\big)$ is similar. □

7. The case $G = V_4$

This case is essentially already in the literature. We collect the relevant results here.

Lemma 7.1. *Let $d \in F^\times \setminus F^{\times 2}$ and let $E = F(\sqrt{d})$. If $v_F(d)$ is even, then $v_F(d_{E/F})$ is an even integer with $0 \le v_F(d_{E/F}) \le 2e_F$. If $v_F(d)$ is odd, then $v_F(d_{E/F}) = 2e_F + 1$.*

Proof. This is part of the $p = 2$ case of [Dab01, Theorem 2.4]. □

Lemma 7.2. *If $\text{Ét}^{V_4/F}_{(1^4)/F,m}$ is nonempty, then m is an even integer and $6 \le m \le 6e_F + 2$.*

Proof. Let $L \in \text{Ét}^{V_4/F}_{(1^4)/F,m}$, and let E_1, E_2 and E_3 be the intermediate quadratic subfields of L. Let $c_i = v_F(d_{E_i/F})$ for each i, so that

$$m = c_1 + c_2 + c_3,$$

by Lemma 6.19. We may write $E_i = F(\sqrt{d_i})$, for $d_i \in F^\times \setminus F^{\times 2}$, such that $d_1 d_2 d_3 \in F^{\times 2}$. Since $v_F(d_1 d_2 d_3)$ is even, it follows from Lemma 7.1 that either 0 or 2 of the c_i are equal to $2e_F + 1$, and the rest are even integers with $2 \le c_i \le 2e_F$. The result follows. □

Lemma 7.3 (Tunnell). *Let m be a positive even integer with $2 \le m \le 6e_F + 2$. Then*

$$\#\text{Ét}^{V_4/F}_{(1^4)/F,m} = 2(q-1)q^{\frac{m-4}{2}}\Big(q^{-\lfloor\frac{m}{6}\rfloor}\Big(1+\mathbb{1}_{3\mid m}\cdot\frac{q-2}{3}\Big) - \mathbb{1}_{m\le 4e_F+2}\cdot q^{-\lfloor\frac{m-2}{4}\rfloor}\Big).$$

Proof. This is [Tun78, Lemma 4.7]. □

Proof of Theorem 5.5. The result follows immediately from Lemmas 7.2 and 7.3. □

Proof of Corollary 5.10. By Lemmas 7.2 and 7.3, we have

$$\widetilde{m}(\text{Ét}^{V_4/F}_{(1^4)/F}) = \frac{1}{2}(q-1)\cdot\Big(\sum_{\substack{4\le m\le 6e_F+2\\ m \text{ even}}} q^{-\frac{m+4}{2}-\lfloor\frac{m}{6}\rfloor}\Big(1+\mathbb{1}_{3\mid m}\cdot\frac{q-2}{3}\Big) - \sum_{\substack{4\le m\le 4e_F+2\\ m \text{ even}}} q^{-\frac{m+4}{2}-\lfloor\frac{m-2}{4}\rfloor}\Big),$$

and it is straightforward to rearrange this expression into the desired form. □

8. The case $G = C_4$

8.1. **Sketch of our approach.** Let F be a p-adic field and let n be a positive integer. We will write $\text{Ext}_{n/F}$ for the set of isomorphism classes of degree n field extensions of F. The notation Ext can be adorned with all the same decorators as Ét, with the obvious meanings. That is, for any choice of decorators $\text{Ét}^{\bullet}_{\bullet}$, we have

$$\text{Ext}^{\bullet}_{\bullet} = \{L \in \text{Ét}^{\bullet}_{\bullet} : L \text{ is a field}\}.$$

Remark 8.1. If σ is a splitting symbol of the form (f^e), then $\text{Ét}_{\sigma/F} = \text{Ext}_{\sigma/F}$. In these cases, we will prefer the notation $\text{Ét}_{\sigma/F}$, since morally we view field extensions as a special case of étale algebras.

We define a *C_4-extendable extension of F* to be a quadratic field extension E/F such that there is some quadratic extension L/E such that L/F is a C_4-extension. For any real number m_1, write $\text{Ext}_{2/F,m_1}^{\uparrow C_4}$ (respectively $\text{Ext}_{2/F,\leq m_1}^{\uparrow C_4}$) for the set of C_4-extendable extensions E/F such that $v_F(d_{E/F}) = m_1$ (respectively $v_F(d_{E/F}) \leq m_1$). For any quadratic extension E/F, write $\text{Ext}_{2/E}^{C_4/F}$ for the set of quadratic extensions L/E such that L/F is a C_4-extension. Note that $\text{Ext}_{2/E}^{C_4/F}$ is nonempty if and only if E/F is C_4-extendable. We allow the usual discriminant-related decorators, writing $\text{Ext}_{2/E,m_2}^{C_4/F}$ and $\text{Ext}_{2/E,\leq m_2}^{C_4/F}$ to denote elements $L \in \text{Ext}_{2/E}^{C_4/F}$ with $v_E(d_{L/E}) = m_2$ and $v_E(d_{L/E}) \leq m_2$, respectively.

Recall that we write $d_{(-1)} = v_F(d_{F(\sqrt{-1})/F})$. In the current subsection, we state the main results, whose proofs are postponed to the later subsections.

For even integers m_1 with $2 \leq m_1 \leq 2e_F$, define

$$N_{\text{ext}}(m_1) = (1 + \mathbb{1}_{m_1 \leq 2e_F - d_{(-1)}}) q^{\frac{m_1}{2}-1}(q - 1 - \mathbb{1}_{m_1 = 2e_F - d_{(-1)}+2}).$$

For $m_1 = 2e_F + 1$, define

$$N_{\text{ext}}(2e_F + 1) = \begin{cases} 2q^{e_F} & \text{if } -1 \in F^{\times 2}, \\ q^{e_F} & \text{if } F(\sqrt{-1})/F \text{ is quadratic and totally ramified,} \\ 0 & \text{if } F(\sqrt{-1})/F \text{ is quadratic and unramified.} \end{cases}$$

Set $N_{\text{ext}}(m_1) = 0$ for all other real numbers m_1. For the reader's convenience, we will also state the definition of $N_{\text{ext}}(m_1)$ in Appendix B.

Lemma 8.2. *If E/F is a totally ramified C_4-extendable extension, then $2 \leq v_F(d_{E/F}) \leq 2e_F+1$ and $v_F(d_{E/F})$ is either even or equal to $2e_F + 1$. For such m_1, we have*

$$\#\text{Ext}_{2/F,m_1}^{\uparrow C_4} = N_{\text{ext}}(m_1),$$

where $N_{\text{ext}}(m_1)$ is the explicit function defined above.

Let m_1 be an even integer with $2 \leq m_1 \leq e_F$. For each integer m_2, define

$$N^{C_4}(m_1, m_2) = \begin{cases} q^{m_1-1} & \text{if } m_2 = 3m_1 - 2, \\ q^{\lfloor \frac{m_1+m_2}{4} \rfloor} - q^{\lfloor \frac{m_1+m_2-2}{4} \rfloor} & \text{if } 3m_1 \leq m_2 \leq 4e_F - m_1 \text{ and } m_2 \text{ is even,} \\ q^{e_F} & \text{if } m_2 = 4e_F - m_1 + 2, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $m_1 = 2e_F + 1$ or m_1 is even with $e_F < m_1 \leq 2e_F$. Then define

$$N^{C_4}(m_1, m_2) = \begin{cases} 2q^{e_F} & \text{if } m_2 = m_1 + 2e_F, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, define $N^{C_4}(m_1, m_2) = 0$ for all other pairs of integers (m_1, m_2). As with $N_{\text{ext}}(m_2)$, we will also state the definition of $N^{C_4}(m_1, m_2)$ in Appendix B.

Lemma 8.3. *Let E be a totally ramified C_4-extendable extension and let $m_1 = v_F(d_{E/F})$. For all m_2, we have*

$$\#\text{Ext}_{2/E,m_2}^{C_4/F} = N^{C_4}(m_1, m_2),$$

where $N^{C_4}(m_1, m_2)$ is the explicit function defined above.

Corollary 8.4. *If $\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m}$ is nonempty, then either $m = 8e_F + 3$ or m is an even integer with $8 \leq m \leq 8e_F$. For any even integer m, the number $\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,m}$ is the sum of the following four quantities:*

(1) $\mathbb{1}_{8 \leq m \leq 5e_F - 2} \cdot q^{\frac{m-3}{5}} \cdot N_{\text{ext}}(\frac{m+2}{5})$.

(2)
$$\sum_{\substack{\max\{2, m-4e_F\} \leq m_1 \leq \min\{\frac{m}{5}, e_F\} \\ m_1 \equiv m \pmod 4}} q^{\frac{m-m_1}{4}-1}(q-1)N_{\text{ext}}(m_1).$$

(3) $\mathbb{1}_{4e_F+4 \leq m \leq 5e_F+2} \cdot q^{e_F} \cdot N_{\text{ext}}(m - 4e_F - 2)$.

(4) $\mathbb{1}_{5e_F+3 \leq m \leq 8e_F} \cdot 2q^{e_F} \cdot N_{\text{ext}}(\frac{m-2e_F}{3})$.

Moreover,

$$\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^4)/F,8e_F+3} = \begin{cases} 4q^{2e_F} & \text{if } -1 \in F^{\times 2}, \\ 2q^{2e_F} & \text{if } F(\sqrt{-1})/F \text{ is quadratic and totally ramified,} \\ 0 & \text{if } F(\sqrt{-1})/F \text{ is quadratic and unramified.} \end{cases}$$

8.2. **Counting C_4-extendable extensions.** The aim of this subsection is to prove Lemma 8.2. The paper [CDO05] gives conditions on $d \in F^\times$ for the extension $F(\sqrt{d})/F$ to be C_4-extendable. We use these conditions and adapt the methods of [CDO05] to parametrise and count C_4-extendable extensions.

Lemma 8.5 (Hecke's Theorem)**.** *Let E be a 2-adic field, let $\alpha \in E^\times \setminus E^{\times 2}$, and let $L = E(\sqrt{\alpha})$. If $v_E(\alpha)$ is odd, then $v_E(d_{L/E}) = 2v_E(2) + 1$. If $v_E(\alpha)$ is even, then L/E is totally ramified if and only if $\alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_E^{2v_E(2)}}$ has no solution $x \in E$. In that case, we have*

$$v_E(d_{L/E}) = 2v_E(2) + 1 - \kappa_{E,\alpha},$$

where

$$\kappa_{E,\alpha} = \max\{0 \leq l < 2v_E(2) : \alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_E^l} \text{ has a solution in } E\}.$$

Proof. This is the special case $p = 2$ of [Dab01, Theorem 2.4]. □

Corollary 8.6. *Let E, α, and L be as in Lemma 8.5, and assume that $v_E(\alpha)$ is even. Let t be an integer with $0 \leq t \leq v_E(2)$. Then $v_E(d_{L/E})$ is an even integer and*

$$v_E(d_{L/E}) \leq 2v_E(2) - 2t$$

if and only if there is some $x \in E^\times$ with $\alpha/x^2 \equiv 1 \pmod{\mathfrak{p}_E^{2t}}$.

Proof. This follows from Lemma 8.5, along with the fact[1] that for $0 \leq t < v_E(2)$ and $u \in \mathcal{O}_E^\times$, if u is square modulo $\mathfrak{p}_E^{2t}$, then it is also square modulo $\mathfrak{p}_E^{2t+1}$. □

[1] If $u \equiv x^2 \pmod{\mathfrak{p}_E^{2t}}$, then $u/x^2 = 1 + \pi_E^{2t}y$ for some $y \in \mathcal{O}_E$. Taking $z \in \mathcal{O}_E$ with $y \equiv z^2 \pmod{\mathfrak{p}_E}$, we obtain $u/x^2 \equiv (1 + \pi_E^t z)^2 \pmod{\mathfrak{p}_E^{2t+1}}$.

Lemma 8.7. *Let $E = F(\sqrt{d})$ for $d \in F^\times \setminus F^{\times 2}$ and let $L = E(\sqrt{\alpha})$ for $\alpha \in E^\times \setminus E^{\times 2}$. The Galois closure group of L/F is*

$$\begin{cases} V_4 & \text{if } N_{E/F}(\alpha) \in F^{\times 2}, \\ C_4 & \text{if } N_{E/F}(\alpha) \in dF^{\times 2}, \\ D_4 & \text{otherwise.} \end{cases}$$

Proof. Write $\alpha = a + b\sqrt{d}$ for $a, b \in F$ and let $\theta = \sqrt{\alpha}$. Let $m(X)$ be the minimal polynomial of θ over F. Let N be a splitting field of $m(X)$ over L. The polynomial $m(X)$ has roots $\pm\theta, \pm\varphi$ for some element $\varphi \in N$.

We claim that L/F is a V_4-extension if and only if $\theta\varphi \in F$. Suppose that L/F is a V_4-extension. Since L/F is the splitting field of $m(X)$, there are $\sigma, \tau \in \mathrm{Gal}(L/F)$ with $\sigma(\theta) = \varphi$ and $\tau(\theta) = -\theta$. These have order 2, so $\sigma(\theta\varphi) = \tau(\theta\varphi) = \theta\varphi$, and therefore $\theta\varphi \in F$. Suppose conversely that $\theta\varphi \in F$. Then $F(\theta) = F(\varphi)$, so L is the splitting field of $m(X)$ over F, and therefore there are $\sigma, \tau \in \mathrm{Gal}(L/F)$ with $\sigma(\theta) = \varphi$ and $\tau(\theta) = -\theta$. Since $\theta\varphi \in F$, it is fixed by σ, so

$$\theta\varphi = \varphi\sigma(\varphi),$$

and therefore $\theta = \sigma(\varphi)$, so σ has order 2. Clearly τ has order 2, so $\mathrm{Gal}(L/F) \cong V_4$.

Let $\lambda := \frac{\theta}{\varphi} - \frac{\varphi}{\theta}$. We claim that L/F is a C_4-extension if and only if $\lambda \in F$. Suppose that L/F is a C_4-extension. Then $\theta, \varphi \in L$, so there is a generator $\sigma \in \mathrm{Gal}(L/F)$ such that $\sigma(\theta) = \varphi$. It follows that $\sigma(\lambda) = \lambda$, so $\lambda \in F$. Suppose conversely that $\lambda \in F$. There is some element $\sigma \in \mathrm{Gal}(N/F)$ such that $\sigma(\theta) = \varphi$. It is easy to see that $\sigma^2(\theta) = \varepsilon\theta$ for some $\varepsilon \in \{\pm 1\}$. Since $\lambda \in F$, we have $\varepsilon = -1$, so σ has order 4. Clearly $\theta^2 + \varphi^2 = 2a$, so

$$\lambda = \frac{2\theta^2 - 2a}{\theta\varphi},$$

which means that

$$\varphi = \frac{2\theta^2 - 2a}{\theta\lambda} \in L,$$

so L/F is Galois and hence C_4 with Galois group $\langle\sigma\rangle$. Finally,

$$\lambda^2 = \frac{4b^2 d}{N_{E/F}(\alpha)},$$

and the result follows. □

Corollary 8.8. *For $d \in F^\times \setminus F^{\times 2}$, the following are equivalent:*

(1) The extension $F(\sqrt{d})/F$ is C_4-extendable.
(2) The element d is a sum of two squares in F.
(3) The element d is in the norm group of the extension $F(\sqrt{-1})/F$.

Proof. The equivalence of (1) and (2) follows from Lemma 8.7. If $-1 \in F^{\times 2}$, then (2) and (3) are equivalent because every element of F can be written as a sum of two squares, due to the identity

$$d = \Big(\frac{d+1}{2}\Big)^2 + \Big(\frac{d-1}{2\sqrt{-1}}\Big)^2.$$

If $-1 \notin F^{\times 2}$, then the equivalence of (2) and (3) is trivial. □

By symmetry of the quadratic Hilbert symbol, it follows from Corollary 8.8 that we need to count extensions $F(\sqrt{d})$ such that $-1 \in \operatorname{Nm} F(\sqrt{d})$. It turns out that this is a special case of a problem we will need to solve in Part 4, whose solution is stated in Corollary 12.31. However, the special case we currently need admits a more elementary proof, which we will include, eventually stating the result in Corollary 8.13.

Remark 8.9. The more general proof of Corollary 12.31 will involve using class field theory to parametrise C_p-extensions of F by the associated characters $F^\times \to \mathbb{F}_p$. In our current special case, we can instead parametrise quadratic extensions of F by $F^\times/F^{\times 2}$ in the obvious way. Thus, the techniques of the upcoming proof rely on the fact that all quadratic extensions are Kummer extensions, so we will genuinely need different ideas for the generalisation in Part 4.

We start by defining some notation. Let $\mathcal{A}$ be a finitely generated subgroup of $F^\times$. Write $\overline{\mathcal{A}}^2$ for the subgroup $\mathcal{A}F^{\times 2}/F^{\times 2}$ of $F^\times/F^{\times 2}$. For each nonnegative integer t, define

$$\mathcal{A}_t = \mathcal{A} \cap \big(U_F^{(t)} F^{\times 2}\big)$$

and

$$\overline{\mathcal{A}}_t^2 = \overline{\mathcal{A}}_t^2 \cap \big(U_F^{(t)} F^{\times 2}/F^{\times 2}\big),$$

where $U_F^{(t)}$ is the t^{th} term in the unit filtration of F, defined by $U_F^{(t)} = 1 + \mathfrak{p}_F^t$, and we adopt the convention that $U_F^{(0)} = \mathcal{O}_F^\times$. Let $F(\sqrt{\mathcal{A}})$ be the field extension

$$F(\{\sqrt{\alpha} : \alpha \in \mathcal{A}\})$$

of F, and write $N(\mathcal{A})$ for the norm group $N_{F(\sqrt{\mathcal{A}})/F} F(\sqrt{\mathcal{A}})^\times$. Let $\operatorname{Ext}_{\bullet/F,\bullet}^{\bullet}$ be a set of field extensions of F, for some choice of decorators $\bullet$. Then we define

$$\operatorname{Ext}_{\bullet/F,\bullet}^{\bullet,\mathcal{A}} = \{E \in \operatorname{Ext}_{\bullet/F,\bullet}^{\bullet} : \mathcal{A} \subseteq N_{E/F} E^\times\}.$$

Lemma 8.10. *Let t be an integer with $0 \le t \le e_F$, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. We have a bijection*

$$\overline{N(\mathcal{A})}_{2t}^2 \to \operatorname{Ext}_{2/F,\le 2e_F - 2t}^{\mathcal{A}} \cup \{F\}, \quad u \mapsto F(\sqrt{u}).$$

Proof. By Lemma 8.5, the map $u \mapsto F(\sqrt{u})$ gives a well-defined bijection

$$\mathcal{O}_F^\times/\mathcal{O}_F^{\times 2} \to \operatorname{Ext}_{2/F,\le 2e_F} \cup \{F\}.$$

For $u \in \mathcal{O}_F^\times \setminus \mathcal{O}_F^{\times 2}$, we claim that the following two statements are true:

(1) $F(\sqrt{u}) \in \operatorname{Ext}_{2/F,\le 2e_F}^{\mathcal{A}}$ if and only if $u \in N(\mathcal{A})$.
(2) $F(\sqrt{u}) \in \operatorname{Ext}_{2/F,\le 2e_F - 2t}$ if and only if $u \in U_F^{(2t)} F^{\times 2}$.

The first statement follows from symmetry of the quadratic Hilbert symbol, and the second follows from Corollary 8.6. The result then follows by definition of $\overline{N(\mathcal{A})}_{2t}^2$. □

Lemma 8.11. *Let t be an integer with $0 \le t \le e_F$, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. Then we have*

$$U_F^{(2e_F - 2t)} N(\mathcal{A}) = N(\mathcal{A}_{2t}).$$

Proof. For $\alpha \in \mathcal{A}_{2t}$, Corollary 8.6 tells us that $v_F(d_{F(\sqrt{\alpha})/F}) \leq 2e_F - 2t$, so[1] $U_F^{(2e_F-2t)} \subseteq \operatorname{Nm} F(\sqrt{\alpha})$, and therefore

$$U_F^{(2e_F-2t)} \subseteq \operatorname{Nm} F(\sqrt{\mathcal{A}_{2t}}).$$

Since $\mathcal{A}_{2t} \subseteq \mathcal{A}$, class field theory tells us that

$$\operatorname{Nm} F(\sqrt{\mathcal{A}}) \subseteq \operatorname{Nm} F(\sqrt{\mathcal{A}_{2t}}),$$

and therefore

$$U_F^{(2e_F-2t)} \operatorname{Nm} F(\sqrt{\mathcal{A}}) \subseteq \operatorname{Nm} F(\sqrt{\mathcal{A}_{2t}}).$$

Suppose that

$$U_F^{(2e_F-2t)} \operatorname{Nm} F(\sqrt{\mathcal{A}}) \subseteq G \subseteq \operatorname{Nm} F(\sqrt{\mathcal{A}_{2t}}),$$

for a subgroup G of $F^\times$. By class field theory, there is a unique abelian extension L/F such that $\operatorname{Nm} L = G$. We have

$$F(\sqrt{\mathcal{A}_{2t}}) \subseteq L \subseteq F(\sqrt{\mathcal{A}}),$$

so

$$L = F(\sqrt{\mathcal{B}})$$

for some subgroup $\mathcal{B} \subseteq \mathcal{A}$. Let $\beta \in \mathcal{B}$. Since $U_F^{(2e_F-2t)} \subseteq \operatorname{Nm} L \subseteq \operatorname{Nm} F(\sqrt{\beta})$, we have $v_F(d_{F(\sqrt{\beta})/F}) \leq 2e_F - 2t$, so Corollary 8.6 tells us that $\beta \in U_F^{(2t)} F^{\times 2}$, and therefore $\beta \in \mathcal{A}_{2t}$. It follows that $\mathcal{B} \subseteq \mathcal{A}_{2t}$, and therefore $L \subseteq F(\sqrt{\mathcal{A}_{2t}})$, so $G = \operatorname{Nm} F(\sqrt{\mathcal{A}_{2t}})$. Therefore, as claimed, we have

$$\operatorname{Nm} F(\sqrt{\mathcal{A}_{2t}}) = U_F^{(2e_F-2t)} \operatorname{Nm} F(\sqrt{\mathcal{A}}).$$

□

Lemma 8.12. *Let t be an integer with $0 \leq t \leq e_F$, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. Then*

$$\#\overline{N(\mathcal{A})}^2_{2t} = 2q^{e_F - t} \cdot \frac{\#\overline{\mathcal{A}}^2_{2e_F-2t}}{\#\overline{\mathcal{A}}^2}.$$

Proof. By definition, we have

$$\overline{N(\mathcal{A})}^2_{2t} = \big(N(\mathcal{A})/F^{\times 2}\big) \cap \big(U_F^{(2t)} F^{\times 2}/F^{\times 2}\big).$$

Viewing these groups as $\mathbb{F}_2$-vector spaces, it is easy to see that

$$\begin{aligned}
\#\overline{N(\mathcal{A})}^2_{2t} &= \frac{\#(N(\mathcal{A})/F^{\times 2}) \cdot \#(U_F^{(2t)} F^{\times 2}/F^{\times 2})}{\#(U_F^{(2t)} N(\mathcal{A})/F^{\times 2})} \\
&= \frac{\#(N(\mathcal{A})/F^{\times 2}) \cdot \#(U_F^{(2t)} F^{\times 2}/F^{\times 2})}{\#(N(\mathcal{A}_{2e_F-2t})/F^{\times 2})} \\
&= \frac{[F^\times : N(\mathcal{A}_{2e_F-2t})]}{[F^\times : N(\mathcal{A})]} \cdot [U_F^{(2t)} F^{\times 2} : F^{\times 2}] \\
&= \frac{\#\overline{\mathcal{A}}^2_{2e_F-2t}}{\#\overline{\mathcal{A}}^2} \cdot [U_F^{(2t)} F^{\times 2} : F^{\times 2}].
\end{aligned}$$

where the second equality follows from Lemma 8.11, and the final equality follows from class field theory. Finally, we claim that

$$[U_F^{(2t)} F^{\times 2} : F^{\times 2}] = 2q^{e_F - t}.$$

[1] Here we are using the well-known fact that, for a quadratic extension E/F, the discriminant valuation $v_F(d_{E/F})$ equals the smallest integer c such that $U_F^{(c)} \subseteq N_{E/F} E^\times$. We will later prove a more general version of this statement, in Lemma 12.11.

We consider this final fact well-known; it may be seen e.g. from the proof of [Tun78, Lemma 4.3]. Alternatively, we prove a more general result later in this thesis, in Corollary 12.22. □

Corollary 8.13. *Let m_1 be an even integer with $0 \leq m_1 \leq 2e_F$, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. Then we have*

$$\#\mathrm{Ext}^{\mathcal{A}}_{2/F,\leq m_1} = 2q^{m_1/2} \cdot \frac{\#\overline{\mathcal{A}}^2_{m_1}}{\#\overline{\mathcal{A}}^2} - 1.$$

Proof. This is immediate from Lemma 8.10 and Lemma 8.12. □

Corollary 8.14. *Let m_1 be an even integer with $2 \leq m_1 \leq 2e_F$. We have*

$$\#\mathrm{Ext}^{\uparrow C_4}_{2/F,\leq m_1} = (1 + \mathbb{1}_{m_1 \leq 2e_F - d_{(-1)}}) \cdot q^{m_1/2} - 1.$$

Proof. Let $\mathcal{A} = \langle -1 \rangle \subseteq F^\times$. Corollary 8.8 tells us that

$$\mathrm{Ext}^{\uparrow C_4}_{2/F,\leq m_1} = \mathrm{Ext}^{\mathcal{A}}_{2/F,\leq m_1},$$

and it follows by Corollary 8.13 that

$$\mathrm{Ext}^{\uparrow C_4}_{2/F,\leq m_1} = 2q^{m_1/2} \cdot \frac{\#\overline{\mathcal{A}}^2_{m_1}}{\#\overline{\mathcal{A}}^2} - 1.$$

Suppose first that $-1 \in F^{\times 2}$. Then $\#\overline{\mathcal{A}}^2 = \#\overline{\mathcal{A}}^2_{m_1} = 1$, and the result follows since $d_{(-1)} = 0$. Suppose instead that $-1 \notin F^{\times 2}$. Then

$$\#\overline{\mathcal{A}}^2 = 2,$$

and, by Corollary 8.6, we have

$$\#\overline{\mathcal{A}}^2_{m_1} = 1 + \mathbb{1}_{d_{(-1)} \leq 2e_F - m_1},$$

and the result follows. □

Lemma 8.15 (Tunnell)**.** *Let F be a 2-adic field with residue field of size q, and let m be an integer. Then we have*

$$\#\mathrm{Ext}_{2/F,m} = \begin{cases} 1 & \textit{if } m = 0, \\ 2(q-1)q^{m/2-1} & \textit{if } m \textit{ is even and } 2 \leq m \leq 2e_F, \\ 2q^{e_F} & \textit{if } m = 2e_F + 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This is [Tun78, Lemma 4.3]. □

Proof of Lemma 8.2. The first claim follows from Lemma 8.15. The result for $2 \leq m_1 \leq 2e_F$ follows from Corollary 8.14. By Lemma 8.5, for any quadratic extension E/F, we have $v_F(d_{E/F}) = 2e_F + 1$ if and only if $E = F(\sqrt{\alpha})$ for some $\alpha \in F^\times$ with $v_F(\alpha) = 1$. Assume that this is the case. Then Corollary 8.8 tells us that E/F is C_4-extendable if and only if α is in the norm group of $F(\sqrt{-1})/F$, and the result follows from the fact that $\mathcal{O}_F^\times \subseteq N_{F(\sqrt{-1})/F}F(\sqrt{-1})^\times$ if and only if $F(\sqrt{-1})/F$ is unramified. □

Since Lemma 8.2 expresses the number of C_4-extendable extensions in terms of the discriminant $d_{(-1)}$, we will need to know the possible values of $d_{(-1)}$. We state these in the following lemma.

Lemma 8.16. *The constant $d_{(-1)}$ is an even integer with*

$$d_{(-1)} \leq 2\left\lceil \frac{e_F}{2} \right\rceil.$$

Proof. This follows from Corollary 8.6, along with the trivial fact that

$$-1 \equiv 1 \pmod{\mathfrak{p}_F^{e_F}}.$$

□

8.3. **Counting C_4-extensions with a given intermediate field.**

Lemma 8.17. *Let $E = F(\sqrt{d})$ be a totally ramified C_4-extendable extension of F with $m_1 = v_F(d_{E/F})$, and let $0 \leq m_2 \leq 4e_F$ be an even integer. The following are equivalent:*

1. *The set $\mathrm{Ext}_{2/E,\leq m_2}^{C_4/F}$ is nonempty.*
2. *There is some $\beta \in \mathcal{O}_E^\times$ such that $\beta \equiv 1 \pmod{\mathfrak{p}_E^{4e_F - m_2}}$ and $N_{E/F}(\beta) \in dF^{\times 2}$.*
3. *We have $m_2 \geq \min\{m_1 + 2e_F, 3m_1 - 2\}$.*

Proof. The first two points are equivalent by Corollary 8.6 and Lemma 8.7. The equivalence of (2) and (3) is essentially [CDO05, Proposition 3.15]. At the start of the proof, the authors state that their "condition $(*)$" is equivalent to (2), and the statement of their proposition is equivalent to (3), where $t = 2e_F - \frac{m_2}{2}$. Their result is stated for prime ideals of number fields lying over 2, but it is trivial to check that the proof works for 2-adic fields. □

The following parametrisation is due to Cohen, Diaz y Diaz, and Olivier:

Lemma 8.18 (Parametrisation of C_4-extensions)**.** *Let E/F be a C_4-extendable extension, and suppose that m_2 is an integer such that $\mathrm{Ext}_{2/E,\leq m_2}^{C_4/F}$ is nonempty. Let $\omega \in E^\times$ be such that $E(\sqrt{\omega}) \in \mathrm{Ext}_{2/E,\leq m_2}^{C_4/F}$. If $m_2 \leq 2e_E$, then we have a 2-to-1 surjection*

$$\left(U_E^{(2e_E - 2\lfloor \frac{m_2}{2} \rfloor)} E^{\times 2} \cap F^\times\right)/F^{\times 2} \to \mathrm{Ext}_{2/E,\leq m_2}^{C_4/F}, \quad u \mapsto E(\sqrt{u\omega}).$$

If $m_2 > 2e_E$, then we have a 2-to-1-surjection

$$F^\times/F^{\times 2} \to \mathrm{Ext}_{2/E,\leq m_2}^{C_4/F}, \quad u \mapsto E(\sqrt{u\omega}).$$

Proof. By [CDO05, Proposition 1.2], there is a 2-to-1 surjection

$$F^\times/F^{\times 2} \to \mathrm{Ext}_{2/E}^{C_4/F}, \quad u \mapsto E(\sqrt{u\omega}),$$

and the result follows from Lemma 8.5 and Corollary 8.6. □

Lemma 8.19. *Let F be a 2-adic field and let E/F be a quadratic extension. The following two statements are true:*

1. *If E/F is unramified, then for integers t with $0 \leq t \leq e_F$, we have*

$$U_E^{(2t)} E^{\times 2} \cap F^\times = U_F^{(2t)} F^{\times 2}.$$

(2) If $v_F(d_{E/F}) = m_1$ for a positive integer m_1, and t is an integer with $0 \leq t \leq 2e_F - \frac{m_1}{2}$, then we have

$$(U_E^{(2t)} E^{\times 2} \cap F^\times)/F^{\times 2} = \begin{cases} F^\times/F^{\times 2} & \textit{if } t \leq \frac{m_1}{2} - 1, \\ U_F^{\left(2\left\lceil \frac{t - \frac{m_1}{2}}{2} \right\rceil\right)} F^{\times 2}/F^{\times 2} & \textit{if } t \geq \frac{m_1}{2}. \end{cases}$$

Proof. Claim (1) is essentially [CDO05, Proposition 3.6]. We now prove Claim (2). The case $t = 0$ is obvious. For $t \geq 1$, the result is essentially [CDO05, Proposition 3.11], combined with the fact that

$$U_F^{(2c)} F^{\times 2} = U_F^{(2c+1)} F^{\times 2}$$

for all nonnegative integers c with $0 \leq c < e_F$. This fact is stated in the proof of [Tun78, Lemma 4.3], and we will also prove it later ourselves, in Corollary 12.21. □

Corollary 8.20. *Let E/F be a totally ramified C_4-extendable extension such that the discriminant valuation $m_1 = v_F(d_{E/F})$ is even. Let $m_2 \leq 4e_F$ be an even integer and write $n_0 := \min\{m_1 + 2e_F, 3m_1 - 2\}$. Then we have*

$$\#\mathrm{Ext}_{2/E,\leq m_2}^{C_4/F} = \begin{cases} 0 & \textit{if } m_2 < n_0, \\ q^{\lfloor \frac{m_1 + m_2}{4} \rfloor} & \textit{if } n_0 \leq m_2 \leq 4e_F - m_1, \\ 2q^{e_F} & \textit{if } m_2 \geq \max\{4e_F - m_1 + 2, n_0\}. \end{cases}$$

Proof. Lemma 8.17 deals with the case $m_2 < n_0$. Let $n_0 \leq m_2 \leq 4e_F$. By Lemma 8.17, the set $\mathrm{Ext}_{2/E,\leq m_2}^{C_4/F}$ is nonempty, and the result follows from Lemma 8.18 and Lemma 8.19. □

Proof of Lemma 8.3. By Lemma 8.15, either $m_1 = 2e_F + 1$ or m_1 is even with $2 \leq m_1 \leq 2e_F$. The case where m_1 is even follows easily from Corollary 8.20. For the case with m_1 odd, suppose that $m_1 = 2e_F + 1$. Then by Lemma 8.5 we have $E = F(\sqrt{d})$ for $d \in F^\times$ with $v_F(d) = 1$. By Lemma 8.7, each C_4-extension L/F extending E has $L = E(\sqrt{\alpha})$ for some $\alpha \in E^\times$ with $v_F(N_{E/F}(\alpha))$ odd. It follows that $v_E(\alpha)$ is odd, so $v_E(d_{L/E}) = 4e_F + 1$ by Lemma 8.5. Therefore,

$$\mathrm{Ext}_{2/E}^{C_4/F} = \mathrm{Ext}_{2/E,4e_F+1}^{C_4/F},$$

so the result follows from Lemma 8.18. □

Proof of Corollary 8.4. Suppose that L/F is a C_4-extension with intermediate quadratic field E. By the tower law for discriminant, we have

$$v_F(d_{L/F}) = 2v_F(d_{E/F}) + f(E/F) \cdot v_E(d_{L/E}).$$

So if $L \in \acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{C_4/F}$ with $m_1 = v_F(d_{E/F})$ and $m_2 = v_E(d_{L/E})$, then $m = 2m_1 + m_2$, and Lemmas 8.2 and 8.3 tell us that either $(m_1, m_2) = (2e_F + 1, 4e_F + 1)$ or m_1 and m_2 are both even with $2 \leq m_1 \leq 2e_F$ and $4 \leq m_2 \leq 4e_F$. It follows that either m is even with $8 \leq m \leq 8e_F$ or $m = 8e_F + 3$. If $m = 8e_F + 3$, then the result follows from Lemmas 8.2 and 8.3.

Now consider the case where $8 \leq m \leq 8e_F$ and m is even. For positive integers m_1 and m_2, write $\Sigma_{m_1,m_2}^{C_4}$ for the set of totally ramified C_4-extensions L/F such that $v_F(d_{E/F}) = m_1$ and $v_E(d_{L/E}) = m_2$. By the discussion above, we have

$$\#\acute{\mathrm{E}}\mathrm{t}_{(1^4)/F,m}^{C_4/F} = \sum_{\substack{2 \leq m_1 \leq 2e_F \\ m_1 \text{ even}}} \#\Sigma_{m_1,m-2m_1}^{C_4}.$$

Let $2 \leq m_1 \leq 2e_F$ be even. By Lemmas 8.2 and 8.3, whenever $N_{\text{ext}}(m_1) \neq 0$ we have

$$\frac{\#\Sigma^{C_4}_{m_1,m-2m_1}}{N_{\text{ext}}(m_1)} = \begin{cases} q^{m_1-1} \quad \text{if } m_1 = \frac{m+2}{5} \text{ and } m_1 \leq e_F, \\ q^{\lfloor \frac{m-m_1}{4} \rfloor} - q^{\lfloor \frac{m-m_1-2}{4} \rfloor} \quad \text{if } m-4e_F \leq m_1 \leq \min\{\frac{m}{5}, e_F\}, \\ q^{e_F} \quad \text{if } m_1 = m-4e_F-2 \text{ and } m_1 \leq e_F, \\ 2q^{e_F} \quad \text{if } e_F < m_1 \leq 2e_F \text{ and } m_1 = \frac{m-2e_F}{3}, \\ 0 \quad \text{otherwise.} \end{cases}$$

$$= \begin{cases} q^{\frac{m-3}{5}} \quad \text{if } m_1 = \frac{m+2}{5} \text{ and } 8 \leq m \leq 5e_F - 2, \\ q^{\lfloor \frac{m-m_1}{4} \rfloor} - q^{\lfloor \frac{m-m_1-2}{4} \rfloor} \quad \text{if } m-4e_F \leq m_1 \leq \min\{\frac{m}{5}, e_F\}, \\ q^{e_F} \quad \text{if } m_1 = m-4e_F-2 \text{ and } 4e_F+4 \leq m \leq 5e_F+2, \\ 2q^{e_F} \quad \text{if } m_1 = \frac{m-2e_F}{3} \text{ and } 5e_F < m \leq 8e_F, \\ 0 \quad \text{otherwise.} \end{cases}$$

To finish the proof, we just need to observe that

$$q^{\lfloor \frac{m-m_1}{4} \rfloor} - q^{\lfloor \frac{m-m_1-2}{4} \rfloor} = \begin{cases} q^{\frac{m-m_1}{4}-1}(q-1) \quad \text{if } m_1 \equiv m \pmod 4, \\ 0 \quad \text{if } m_1 \not\equiv m \pmod 4. \end{cases}$$

□

Proof of Theorem 5.6. The possible values of m come from Corollary 8.4. The result for $m = 8e_F + 3$ is immediate from Corollary 8.4. Now consider the case where m is even and $8 \leq m \leq 8e_F$. The first, third, and fourth items of Corollary 8.4 respectively are equal to

(1) $\mathbb{1}_{8 \leq m \leq 5e_F-2} \cdot \mathbb{1}_{m \equiv 3 \pmod 5} \cdot q^{\frac{3m-14}{10}}(1 + \mathbb{1}_{m \leq 10e_F - 5d_{(-1)}-2})(q - 1 - \mathbb{1}_{m = 10e_F - 5d_{(-1)}+8})$.
(2) $\mathbb{1}_{4e_F+4 \leq m \leq 5e_F+2} \cdot q^{\frac{m}{2}-e_F-2}(1 + \mathbb{1}_{m \leq 6e_F - d_{(-1)}+2})(q - 1 - \mathbb{1}_{m = 6e_F - d_{(-1)}+4})$.
(3) $\mathbb{1}_{5e_F+3 \leq m \leq 8e_F} \cdot \mathbb{1}_{m \equiv 2e_F \pmod 3} \cdot 2q^{\frac{m+4e_F}{6}-1}(1 + \mathbb{1}_{m \leq 8e_F - 3d_{(-1)}})(q - 1 - \mathbb{1}_{m = 8e_F - 3d_{(-1)}+6})$.

Lemma 8.16 turns these into the first three points of Theorem 5.6. It remains to compute the value of

$$\sum_{\substack{\max\{2, m-4e_F\} \leq m_1 \leq \min\{\frac{m}{5}, e_F\} \\ m_1 \equiv m \pmod 4}} q^{\frac{m-m_1}{4}-1}(q-1)N_{\text{ext}}(m_1).$$

For such m_1, we have

$$N_{\text{ext}}(m_1) = \begin{cases} 2q^{\frac{m_1}{2}-1}(q-1) \quad \text{if } m_1 \leq 2e_F - d_{(-1)}, \\ q^{\frac{m_1}{2}-1}(q-2) \quad \text{if } m_1 = 2e_F - d_{(-1)} + 2, \\ q^{\frac{m_1}{2}-1}(q-1) \quad \text{if } m_1 \geq 2e_F - d_{(-1)} + 4. \end{cases}$$

Lemma 8.16 tells us that $2e_F - d_{(-1)} + 2 > e_F$, so the sum is actually

$$\sum_{\substack{\max\{2, m-4e_F\} \leq m_1 \leq \min\{\frac{m}{5}, e_F\} \\ m_1 \equiv m \pmod 4}} 2q^{\frac{m+m_1}{4}-2}(q-1)^2.$$

For integers l and u, the substitution $m_1 = -m + 4k$ makes it easy to see that

$$\sum_{\substack{l \leq m_1 \leq u \\ m_1 \equiv m \pmod 4}} q^{\frac{m+m_1}{4}} = \mathbb{1}_{l \leq u} \cdot \frac{q^{b+1} - q^a}{q-1},$$

where $a = \lceil \frac{m+l}{4} \rceil$ and $b = \lfloor \frac{m+u}{4} \rfloor$. In this case, we have $l = \max\{2, m - 4e_F\}$ and $u = \min\{e_F, \frac{m}{5}\}$, which gives

$$a = \left\lceil \max\left\{\frac{m+2}{4}, \frac{m}{2} - e_F\right\}\right\rceil, \quad b = \left\lfloor \min\left\{\frac{m+e_F}{4}, \frac{3m}{10}\right\}\right\rfloor.$$

Finally, it is easy to see that $l \leq u$ if and only if $10 \leq m \leq 5e_F$. In that case, we have $b = \lfloor \frac{3m}{10} \rfloor$, so

$$\sum_{\substack{\max\{2,m-4e_F\} \leq m_1 \leq \min\{e_F, \frac{m}{5}\} \\ m_1 \equiv m \pmod 4}} q^{\frac{m+m_1}{4}} = \mathbb{1}_{10 \leq m \leq 5e_F} \cdot \frac{q^{\lfloor \frac{3m}{10} \rfloor + 1} - q^{\lceil \max\{\frac{m+2}{4}, \frac{m}{2} - e_F\}\rceil}}{q-1},$$

and the result follows. □

Proof of Corollary 5.11. Theorem 5.6 and Lemma 8.16 tell us that the mass is the sum of the following quantities:

(1)
$$\frac{1}{2} \cdot \sum_{\substack{8 \leq m \leq 5e_F - 2 \\ m \equiv 8 \pmod{10}}} q^{-\frac{7m+14}{10}}(q-1).$$

(2)
$$\frac{1}{2} \cdot \sum_{\substack{4e_F + 4 \leq m \leq 5e_F + 2 \\ m \text{ even}}} q^{-\frac{m}{2} - e_F - 2}(q-1).$$

(3) (a)
$$\sum_{\substack{5e_F + 3 \leq m \leq 8e_F - 3d_{(-1)} \\ m \equiv 2e_F \pmod 6}} q^{\frac{4e_F - 5m}{6} - 1}(q-1).$$

(b)
$$\mathbb{1}_{d_{(-1)} \geq 2} \cdot \frac{1}{2} \cdot q^{-6e_F + \frac{5}{2}d_{(-1)} - 6}(q-2).$$

(c)
$$\frac{1}{2} \cdot \sum_{\substack{8e_F - 3d_{(-1)} + 12 \leq m \leq 8e_F \\ m \equiv 2e_F \pmod 6}} q^{\frac{4e_F - 5m}{6} - 1}(q-1).$$

(4) (a)
$$\frac{1}{2}(q-1)q^{-1} \sum_{\substack{10 \leq m \leq 5e_F \\ m \text{ even}}} q^{\lfloor -\frac{7m}{10} \rfloor}.$$

(b)
$$-\frac{1}{2}(q-1)q^{-2} \sum_{\substack{10 \leq m \leq 5e_F \\ m \text{ even}}} q^{\max\{\lceil \frac{-3m+2}{4} \rceil, -\frac{m}{2} - e_F\}}.$$

(5)
$$\begin{cases} q^{-6e_F - 3} & \text{if } -1 \in F^{\times 2}, \\ \frac{1}{2}q^{-6e_F - 3} & \text{if } F(\sqrt{-1})/F \text{ is quadratic and totally ramified,} \\ 0 & \text{otherwise.} \end{cases}$$

We address these one by one.

(1) Making the substitution $m = 10k + 8$, we have

$$\sum_{\substack{8 \le m \le 5e_F - 2 \\ m \equiv 8 \pmod{10}}} q^{-\frac{7m+14}{10}} = \mathbb{1}_{e_F \ge 2} \cdot \frac{1 - q^{-7\lfloor \frac{e_F}{2} \rfloor}}{q^7 - 1},$$

so the contribution to the mass is

$$\frac{1}{2} \cdot \mathbb{1}_{e_F \ge 2} \cdot \frac{(q-1)(1 - q^{-7\lfloor \frac{e_F}{2} \rfloor})}{q^7 - 1},$$

and we can omit the indicator function since $e_F = 1$ gives $1 - q^{-7\lfloor \frac{e_F}{2} \rfloor} = 0$.

(2) Making the substitution $m = 2k$, it is easy to see that

$$\sum_{\substack{4e_F + 4 \le m \le 5e_F + 2 \\ m \text{ even}}} q^{-\frac{m}{2}} = \mathbb{1}_{e_F \ge 2} \cdot \frac{q^{-2e_F - 1} - q^{-\lfloor \frac{5e_F + 2}{2} \rfloor}}{q - 1},$$

so the contribution is

$$\frac{1}{2} \cdot (q^{-3e_F - 3} - q^{-\lfloor \frac{7e_F + 6}{2} \rfloor}) = \frac{1}{2} \cdot q^{-3e_F - 3}(1 - q^{-\lfloor \frac{e_F}{2} \rfloor}),$$

where we omit the indicator function since $e_F = 1$ gives $q^{-2e_F - 1} - q^{-\lfloor \frac{5e_F + 2}{2} \rfloor} = 0$.

(3) (a) The substitution $m = 2e_F + 6k$ gives

$$\sum_{\substack{5e_F + 3 \le m \le 8e_F - 3d_{(-1)} \\ m \equiv 2e_F \pmod{6}}} q^{\frac{4e_F - 5m}{6}} = \mathbb{1}_{d_{(-1)} < e_F} \frac{q^{-5\lfloor \frac{e_F}{2} \rfloor - e_F} - q^{\frac{5}{2} d_{(-1)} - 6e_F}}{q^5 - 1},$$

so the contribution is

$$\mathbb{1}_{d_{(-1)} < e_F} \cdot \frac{(q-1)(q^{-5\lfloor \frac{e_F}{2} \rfloor - e_F - 1} - q^{\frac{5}{2} d_{(-1)} - 6e_F - 1})}{q^5 - 1}.$$

(b) This is already in closed form.

(c) The substitution $m = 2e_F + 6k$ gives

$$\sum_{\substack{8e_F - 3d_{(-1)} + 12 \le m \le 8e_F \\ m \equiv 2e_F \pmod{6}}} q^{\frac{4e_F - 5m}{6}} = \mathbb{1}_{d_{(-1)} \ge 4} \cdot \frac{q^{\frac{5}{2} d_{(-1)} - 6e_F - 5} - q^{-6e_F}}{q^5 - 1}.$$

Therefore, the contribution is

$$\frac{1}{2} \cdot \mathbb{1}_{d_{(-1)} \ge 4} \cdot \frac{(q-1)(q^{\frac{5}{2} d_{(-1)} - 6e_F - 6} - q^{-6e_F - 1})}{q^5 - 1}.$$

(4) (a) We need to compute

$$\sum_{\substack{10 \le m \le 5e_F \\ m \text{ even}}} q^{\lfloor \frac{-7m}{10} \rfloor} = \sum_{k=5}^{\lfloor \frac{5e_F}{2} \rfloor} q^{-\lceil \frac{7k}{5} \rceil}.$$

For an integer $b \ge 1$, it is easy to see that

$$\sum_{k=5}^{5b} q^{-\lceil \frac{7k}{5} \rceil} = \frac{(q^{-6} - q^{1-7b})(q^6 + q^4 + q^3 + q + 1)}{q^7 - 1} + q^{-7b}.$$

If e_F is even, then we have

$$\begin{aligned}\sum_{k=5}^{\lfloor\frac{5e_F}{2}\rfloor} q^{-\lceil\frac{7k}{5}\rceil} &= \sum_{k=5}^{5\cdot\frac{e_F}{2}} q^{-\lceil\frac{7k}{5}\rceil}\\ &= \mathbb{1}_{e_F\geq 2}\cdot\Big(\frac{(q^{-6}-q^{1-\frac{7e_F}{2}})(q^6+q^4+q^3+q+1)}{q^7-1}+q^{-\frac{7e_F}{2}}\Big).\end{aligned}$$

If e_F is odd, then we have

$$\begin{aligned}\sum_{k=5}^{\lfloor\frac{5e_F}{2}\rfloor} q^{-\lceil\frac{7k}{5}\rceil} &= \Big(\sum_{k=5}^{5\cdot\frac{e_F-1}{2}} q^{-\lceil\frac{7k}{5}\rceil}\Big)+q^{-\lceil\frac{7}{5}\cdot\frac{5e_F-3}{2}\rceil}+q^{-\lceil\frac{7}{5}\cdot\frac{5e_F-1}{2}\rceil}\\ &= \mathbb{1}_{e_F\geq 2}\cdot\Big(\frac{(q^{-6}-q^{1-7\cdot\frac{e_F-1}{2}})(q^6+q^4+q^3+q+1)}{q^7-1}+q^{-7\cdot\frac{e_F-1}{2}}\\ &\qquad +q^{-7\cdot\frac{e_F-1}{2}-2}+q^{-7\cdot\frac{e_F-1}{2}-3}\Big).\end{aligned}$$

In other words, the sum $\sum_{k=5}^{\lfloor\frac{5e_F}{2}\rfloor} q^{-\lceil\frac{7k}{5}\rceil}$ is equal to

$$\mathbb{1}_{e_F\geq 2}\cdot\Big(\frac{(q^{-6}-q^{1-7\lfloor\frac{e_F}{2}\rfloor})(q^6+q^4+q^3+q+1)}{q^7-1}+q^{-7\lfloor\frac{e_F}{2}\rfloor}(1+\mathbb{1}_{2\nmid e_F}(q^{-2}+q^{-3}))\Big),$$

and therefore we have a contribution of

$$\mathbb{1}_{e_F\geq 2}\cdot\frac{1}{2}(q-1)\Big(\frac{(q^{-7}-q^{-7\lfloor\frac{e_F}{2}\rfloor})(q^6+q^4+q^3+q+1)}{q^7-1}+q^{-7\lfloor\frac{e_F}{2}\rfloor-1}(1+\mathbb{1}_{2\nmid e_F}(q^{-2}+q^{-3}))\Big).$$

(b) We need to evaluate

$$\sum_{k=5}^{\lfloor\frac{5e_F}{2}\rfloor} q^{\max\{\lceil\frac{-3k+1}{2}\rceil,-k-e_F\}} = \sum_{k=5}^{2e_F} q^{\lceil\frac{-3k+1}{2}\rceil}+\sum_{k=2e_F+1}^{\lfloor\frac{5e_F}{2}\rfloor} q^{-k-e_F}.$$

We have

$$\sum_{k=5}^{2e_F} q^{\lceil\frac{-3k+1}{2}\rceil} = \mathbb{1}_{e_F\geq 3}\cdot\frac{(q^2+q)(q^{-6}-q^{-3e_F})}{q^3-1},$$

so the first half of the sum gives a contribution of

$$-\mathbb{1}_{e_F\geq 2}\cdot\frac{1}{2}\cdot\frac{(q-1)(q+1)(q^{-7}-q^{-3e_F-1})}{q^3-1}.$$

We also have

$$\sum_{k=2e_F+1}^{\lfloor\frac{5e_F}{2}\rfloor} q^{-k-e_F} = \mathbb{1}_{e_F\geq 2}\cdot\frac{q^{-3e_F}-q^{-\lfloor\frac{5e_F}{2}\rfloor-e_F}}{q-1},$$

so we also get a contribution of

$$-\frac{1}{2}(q^{-3e_F-2}-q^{-\lfloor\frac{7e_F}{2}\rfloor-2}).$$

□

For $G \in \{V_4, C_4, D_4\}$ and $L \in \text{Ét}^{G/F}_{(1^4)/F}$, let

$$\text{Ext}^{\hookrightarrow L}_{2/F} := \{E \in \text{Ext}_{2/F} : \exists F\text{-morphism } E \hookrightarrow L\}.$$

Let $L \in \text{Ét}^{G/F}_{(1^4)/F}$ and $E \in \text{Ext}^{\hookrightarrow L}_{2/F}$. There is a unique embedding $E \hookrightarrow L$, so we may naturally view L as an extension of E. We define an *F-twist of L/E* to be an element of the set

$$\text{Twist}_F(L/E) = \{L' \in \text{Ext}_{2/E} : \exists F\text{-isomorphism } L' \cong L\}.$$

Lemma 9.1. *Let $G \in \{V_4, C_4, D_4\}$. The following two statements are true:*

(1) For $L \in \text{Ét}^{G/F}_{(1^4)/F}$, we have

$$\#\text{Ext}^{\hookrightarrow L}_{2/F} = \begin{cases} 1 & \text{if } G \in \{C_4, D_4\}, \\ 3 & \text{if } G = V_4. \end{cases}$$

(2) For $L \in \text{Ét}^{G/F}_{(1^4)/F}$ and $E \in \text{Ext}^{\hookrightarrow L}_{2/F}$, we have

$$\#\,\text{Twist}_F(L/E) = \begin{cases} 1 & \text{if } G \in \{C_4, V_4\}, \\ 2 & \text{if } G = D_4. \end{cases}$$

Proof. Claim (1) is obvious. For Claim (2), write $E = F(\sqrt{d})$ and $L = E(\sqrt{\alpha})$, where $d \in F$ and $\alpha \in E$. Let $L' \in \text{Twist}_F(L/E)$. Then there is a F-isomorphism $\varphi : E(\sqrt{\alpha}) \to L'$. We will view E as a subset of both extensions L and L', even though L and L' are not necessarily inside the same algebraic closure of E.

The element $\varphi(\sqrt{\alpha}) \in L'$ has the same minimal polynomial over F as $\sqrt{\alpha} \in L$, so either $L' \cong E(\sqrt{\alpha})$ or $L' \cong E(\sqrt{\overline{\alpha}})$, where $\overline{\alpha}$ is the conjugate of α over F. It is easy to see that both these choices for L' are in $\text{Twist}_F(L/E)$, so

$$\text{Twist}_F(L/E) = \{E(\sqrt{\alpha}), E(\sqrt{\overline{\alpha}})\}.$$

By elementary Galois theory, we have $E(\sqrt{\alpha}) \ncong E(\sqrt{\overline{\alpha}})$ over E if and only if $G = D_4$. □

For an integer m, define an *m-tower* to be a pair (E, L), where $E \in \text{Ext}_{2/F}$ and $L \in \text{Ext}_{2/E}$, such that L/F is a totally ramified extension with $v_F(d_{L/F}) = m$. Write Tow_m for the set of m-towers. There is a natural surjection

$$\Phi_m : \text{Tow}_m \to \text{Ét}^{C_4/F}_{(1^4)/F,m} \cup \text{Ét}^{V_4/F}_{(1^4)/F,m} \cup \text{Ét}^{D_4/F}_{(1^4)/F,m}, \quad (E, L) \mapsto L.$$

Lemma 9.2. *Let $G \in \{C_4, V_4, D_4\}$, let m be an integer, and let $L_0 \in \text{Ét}^{G/F}_{(1^4)/F,m}$. The fibre $\Phi_m^{-1}(L_0)$ has size*

$$\begin{cases} 1 & \text{if } G = C_4, \\ 2 & \text{if } G = D_4, \\ 3 & \text{if } G = V_4. \end{cases}$$

Proof. It is easy to see that

$$\Phi_m^{-1}(L_0) = \{(E, L) : E \in \text{Ext}^{\hookrightarrow L_0}_{2/F}, L \in \text{Twist}_F(L_0/E)\},$$

and the result follows from Lemma 9.1. □

Corollary 9.3. *For every integer m, we have*

$$\#\text{Ét}^{C_4/F}_{(1^4)/F,m} + 2 \cdot \#\text{Ét}^{D_4/F}_{(1^4)/F,m} + 3 \cdot \#\text{Ét}^{V_4/F}_{(1^4)/F,m} = \#\text{Tow}_m.$$

Proof. This is immediate from Lemma 9.2. □

Lemma 9.4. *If* Tow_m *is nonempty, then one of the following three statements is true:*

(1) m is an even integer with $6 \le m \le 8e_F + 2$.
(2) $m \equiv 1 \pmod 4$ and $4e_F + 5 \le m \le 8e_F + 1$.
(3) $m = 8e_F + 3$.

For even m with $6 \le m \le 8e_F + 2$, we have

$$\#\text{Tow}_m = 4(q-1)q^{\frac{m}{2}-2}\big(\mathbb{1}_{m \ge 4e_F+4} \cdot q^{-e_F} + \mathbb{1}_{m \le 8e_F} \cdot \big(q^{\min\{0, e_F+1-\lceil \frac{m}{4} \rceil\}} - q^{-\min\{\lfloor \frac{m-2}{4} \rfloor, e_F\}}\big)\big).$$

For $m \equiv 1 \pmod 4$ with $4e_F + 5 \le m \le 8e_F + 1$, we have

$$\#\text{Tow}_m = 4(q-1)q^{e_F + \frac{m-1}{4} - 1}.$$

We also have

$$\#\text{Tow}_{8e_F+3} = 4q^{3e_F}.$$

Proof. Let m be an integer such that Tow_m is nonempty. Let $(E, L) \in \text{Tow}_m$, and let $m_1 = v_F(d_{E/F})$ and $m_2 = v_E(d_{L/E})$, so that $m = 2m_1 + m_2$ by the tower law for discriminant. By Lemma 8.15, either m_1 is even with $2 \le m_1 \le 2e_F$, or $m_1 = 2e_F + 1$. Similarly, either m_2 is even with $2 \le m_2 \le 4e_F$, or $m_2 = 4e_F + 1$. If m_2 is even, then m is even and $6 \le m \le 8e_F + 2$. If $m_2 = 4e_F + 1$ and m_1 is even, then $m \equiv 1 \pmod 4$ and $4e_F + 5 \le m \le 8e_F + 1$. Finally, if m_1 and m_2 are both odd, then $m = 8e_F + 3$. Now that we have identified the possibilities, we can enumerate Tow_m in each case.

Suppose first that m is even with $6 \le m \le 8e_F + 2$. Then each $(E, L) \in \text{Tow}_m$ has m_2 even, so $\#\text{Tow}_m$ is the sum of the following two quantities:

(1)
$$\sum_{\substack{\max\{2, \frac{m}{2} - 2e_F\} \le m_1 \le \min\{\frac{m}{2} - 1, 2e_F\} \\ m_1 \text{ even}}} \ \sum_{E \in \text{Ext}_{2/F,m_1}} \#\text{Ext}_{2/E,m-2m_1}.$$

(2)
$$\mathbb{1}_{m \ge 4e_F+4} \cdot \sum_{E \in \text{Ext}_{2/F,2e_F+1}} \#\text{Ext}_{2/E,m-4e_F-2}.$$

By Lemma 8.15, the first of these quantities is equal to

$$\begin{aligned}
\#\text{Ext}_{2/E,m-2m_1} &= \sum_{\substack{\max\{2, \frac{m}{2} - 2e_F\} \le m_1 \le \min\{\frac{m}{2} - 1, 2e_F\} \\ m_1 \text{ even}}} 4(q-1)^2 q^{\frac{m-m_1}{2} - 2} \\
&= 4(q-1)^2 q^{\frac{m}{2}-2} \sum_{k=a}^{b} q^{-k} \\
&= 4(q-1)^2 q^{\frac{m}{2}-2} \cdot \mathbb{1}_{a \le b} \cdot \frac{q^{1-a} - q^{-b}}{q-1} \\
&= \mathbb{1}_{6 \le m \le 8e_F} \cdot 4(q-1)q^{\frac{m}{2}-2}(q^{1-a} - q^{-b}),
\end{aligned}$$

where

$$a := \max\left\{1, \left\lceil\frac{m}{4}\right\rceil - e_F\right\}, \quad b := \min\left\{\left\lfloor\frac{m-2}{4}\right\rfloor, e_F\right\}.$$

For $m = 2, 4$ we have $q^{1-a} - q^{-b} = 0$, so we may drop the "$6 \leq m$" from the indicator function, giving

$$\#\mathrm{Ext}_{2/E, m-2m_1} = \mathbb{1}_{m \leq 8e_F} \cdot 4(q-1)q^{\frac{m}{2}-2}(q^{1-a} - q^{-b}).$$

Similarly, the second quantity is equal to

$$\mathbb{1}_{m \geq 4e_F+4} \cdot 4(q-1)q^{\frac{m}{2}-e_F-2},$$

and we obtain the desired expression for $\#\mathrm{Tow}_m$. Now suppose that $m \equiv 1 \pmod 4$ and $4e_F + 5 \leq m \leq 8e_F + 1$. Then each $(E, L) \in \mathrm{Tow}_m$ has $m_2 = 4e_F + 1$ and $m_1 = \frac{m-1}{2} - 2e_F$, so Lemma 8.15 gives us

$$\begin{aligned} \#\mathrm{Tow}_m &= \sum_{E \in \mathrm{Ext}_{2/F, \frac{m-1}{2}-2e_F}} \#\mathrm{Ext}_{2/E, 4e_F+1} \\ &= 4(q-1)q^{e_F + \frac{m-1}{4} - 1}. \end{aligned}$$

Finally, if $m = 8e_F + 3$, then each $(E, L) \in \mathrm{Tow}_m$ has $m_1 = 2e_F + 1$ and $m_2 = 4e_F + 1$, so

$$\begin{aligned} \#\mathrm{Tow}_m &= \sum_{E \in \mathrm{Ext}_{2/F, 2e_F+1}} \#\mathrm{Ext}_{2/E, 4e_F+1} \\ &= 4q^{3e_F}, \end{aligned}$$

by Lemma 8.15. □

Proof of Theorem 5.7. This is immediate from Corollary 9.3 and Lemma 9.4. □

Lemma 9.5. *We have*

$$\frac{1}{4} \cdot \sum_m q^{-m} \#\mathrm{Tow}_m = \frac{1}{q^2+q+1}(q^{-3e_F-3} + q^{-3e_F-1} + q^{-2}).$$

Proof. Lemma 9.4 tells us that $\frac{1}{4}\sum_m q^{-m}\#\mathrm{Tow}_m$ is the sum of the following four quantities:

(1) $\sum_{\substack{4e_F+4 \leq m \leq 8e_F+2 \\ m \text{ even}}} (q-1)q^{-\frac{m}{2}-e_F-2}$.
(2) $\sum_{\substack{6 \leq m \leq 8e_F \\ m \text{ even}}} (q-1)q^{\min\{0, e_F+1-\lceil\frac{m}{4}\rceil\}-\frac{m}{2}-2}$.
(3) $-\sum_{\substack{6 \leq m \leq 8e_F \\ m \text{ even}}} (q-1)q^{-\frac{m}{2}-2-\min\{\lfloor\frac{m-2}{4}\rfloor, e_F\}}$.
(4) $\sum_{\substack{4e_F+5 \leq m \leq 8e_F+1 \\ m \equiv 1 \pmod 4}} (q-1)q^{e_F+\frac{-3m-1}{4}-1}$.
(5) q^{-5e_F-3}.

We can simplify this as the sum of the following quantities:

(1) $(q-1)q^{-e_F-2} \cdot \sum_{k=2e_F+2}^{4e_F+1} q^{-k}$.
(2) (a) $(q-1)q^{-2} \cdot \sum_{k=3}^{2e_F+2} q^{-k}$.
   (b) $(q-1)q^{e_F-1} \cdot \sum_{k=2e_F+3}^{4e_F} q^{-\lceil\frac{3k}{2}\rceil}$.
(3) (a) $-(q-1)q^{-e_F-2} \cdot \sum_{k=2e_F+1}^{4e_F} q^{-k}$.
   (b) $-(q-1)q^{-2} \cdot \sum_{k=3}^{2e_F} q^{-\lfloor\frac{3k-1}{2}\rfloor}$.
(4) $(q-1)q^{e_F-2} \cdot \sum_{k=e_F+1}^{2e_F} q^{-3k}$.
(5) q^{-5e_F-3}.

We put the pieces together to obtain the contributions to the final sum:

- (1) and (3)(a) cancel to give a contribution of
$$(q-1)(q^{-5e_F-3}-q^{-3e_F-3}).$$
- (2)(a) simplifies to a contribution of
$$q^{-4}-q^{-2e_F-4}.$$
- We have
$$\sum_{k=2e_F+3}^{4e_F} q^{-\lceil \frac{3k}{2}\rceil} = \frac{q+1}{q^3-1}(q^{-3e_F-3}-q^{-6e_F}),$$
so (2)(b) gives a contribution of
$$\frac{q+1}{q^2+q+1}(q^{-2e_F-4}-q^{-5e_F-1}).$$
- We have
$$\sum_{k=3}^{2e_F} q^{-\lfloor \frac{3k-1}{2}\rfloor} = \frac{q+1}{q^3-1}(q^{-2}-q^{1-3e_F}),$$
so (3)(b) gives a contribution of
$$-\frac{q+1}{q^2+q+1}(q^{-4}-q^{-1-3e_F}).$$
- We have
$$\sum_{k=e_F+1}^{2e_F} q^{-3k} = \frac{q^{-3e_F}-q^{-6e_F}}{q^3-1},$$
so (4) gives a contribution of
$$\frac{1}{q^2+q+1}(q^{-2e_F-2}-q^{-5e_F-2}).$$
- Finally, (5) obviously gives a contribution of
$$q^{-5e_F-3}.$$

So far, we have shown that $\frac{1}{4}\sum_m q^{-m}\#\mathrm{Tow}_m$ is the sum of the following six quantities:

(A) $(q-1)(q^{-5e_F-3}-q^{-3e_F-3})$.
(B) $q^{-4}-q^{-2e_F-4}$.
(C) $\frac{q+1}{q^2+q+1}(q^{-2e_F-4}-q^{-5e_F-1})$.
(D) $-\frac{q+1}{q^2+q+1}(q^{-4}-q^{-3e_F-1})$.
(E) $\frac{1}{q^2+q+1}(q^{-2e_F-2}-q^{-5e_F-2})$.
(F) q^{-5e_F-3}.

The sum of $(C), (D)$ and (E) is
$$q^{-2e_F-4}-q^{-5e_F-2}+\frac{q+1}{q^2+q+1}(q^{-3e_F-1}-q^{-4}),$$
so we have shown that $\sum_m q^{-m}\#\mathrm{Tow}_m$ is the sum of the following four quantities:

(1) $(q-1)(q^{-5e_F-3}-q^{-3e_F-3})$.
(2) $q^{-4}-q^{-2e_F-4}$.
(3) $q^{-2e_F-4}-q^{-5e_F-2}+\frac{q+1}{q^2+q+1}(q^{-3e_F-1}-q^{-4})$.

(4) q^{-5e_F-3}.

It is easy to check that this sum simplifies to

$$\frac{1}{q^2+q+1}(q^{-3e_F-3}+q^{-3e_F-1}+q^{-2}),$$

so we are done. □

Proof of Corollary 5.12. This follows easily from Corollary 9.3, Lemma 9.5, and the definition of mass. □

Part 4. Asymptotic counts for generic extensions with prescribed norms

10. Introduction

As we saw in Part 2, the community has devoted much attention to counting families of S_n-n-ic extensions of a fixed base field k. One way of obtaining such a family is to "prescribe" certain norms. That is, we choose elements $\alpha_1, \dots, \alpha_r \in k^\times$ and count S_n-n-ic extensions K/k such that $\alpha_i \in N_{K/k}K^\times$ for every i. Equivalently, we choose a finitely generated subgroup $\mathcal{A} \subseteq k^\times$ and count S_n-n-ic extensions K/k with $\mathcal{A} \subseteq N_{K/k}K^\times$. The latter formulation is more convenient to work with, so we will use it from now on.

Write $N_{k,n}(X; \mathcal{A})$ for the number of S_n-n-ic extensions K/k such that $\mathcal{A} \subseteq N_{K/k}K^\times$ with $\mathrm{Nm}(\mathrm{disc}(K/k)) \leq X$. It turns out ([Vos88, Corollary to Theorem 4]) that an S_n-n-ic extension K/k has $\mathcal{A} \subseteq N_{K/k}K^\times$ if and only if

$$\mathcal{A} \subseteq N_{K_v/k_v}K_v^\times$$

for every place v of k, where K_v is the completion of K over v, as in Definition 3.29. For each place v of k, define

$$\text{Ét}^{\mathcal{A}}_{n/k_v} = \left\{ L \in \text{Ét}_{n/k_v} : \mathcal{A} \subseteq N_{L/k_v}L^\times \right\}.$$

Then $\left(\text{Ét}^{\mathcal{A}}_{n/k_v}\right)_v$ is a collection of local conditions, in the sense of Definition 3.31, and we will see (Lemma 11.3) that it is in fact *acceptable*, so that we may apply Theorem 3.53 and Conjecture 3.54 to prove results for $n \in \{3,4,5\}$ and make conjectures for $n \geq 6$. In the rest of Section 10, we state the key results of Part 4, postponing all proofs.

10.1. Qualitative results.

In Section 11, we will start by exploring our problem in as much generality as possible, namely for all $n \geq 3$. We will obtain qualitative statements for all n, which are theorems for $n \in \{3,4,5\}$, and conjectures contingent on the Malle–Bhargava Heuristics (i.e. Conjecture 3.54) for $n \geq 6$. Specialising to the known cases, $n \in \{3,4,5\}$, we isolate the following headline result:

Theorem 10.1. *Let $n \in \{3,4,5\}$. For every finitely generated subgroup $\mathcal{A} \subseteq k^\times$, we have*

$$0 < \lim_{X \to \infty} \frac{N_{k,n}(X; \mathcal{A})}{N_{k,n}(X)} \leq 1,$$

with equality if and only if $\mathcal{A} \subseteq k^{\times n}$.

Corollary 10.2. *Let $n \in \{3,4,5\}$. For every finitely generated subgroup $\mathcal{A} \subseteq k^\times$, there are infinitely many S_n-n-ic extensions K/k with $\mathcal{A} \subseteq N_{K/k}K^\times$.*

For $n \geq 6$, there is a natural conjectural analogue of Theorem 10.1. This analogue is a little too fiddly to state in this introductory section, but we refer the reader to Theorems 11.10 and 11.12.

Let us unpack the content of Theorem 10.1. It tells us that, for $n \in \{3,4,5\}$, any finitely generated subgroup $\mathcal{A} \subseteq k^\times$ is contained in the norm group of a positive proportion of S_n-n-ic extensions. Moreover, it tells us that $\mathcal{A}$ can only be contained in 100% of such norm groups if it is contained in *every* such norm group.

Remark 10.3. In the special case where $\mathcal{A}$ is generated by one element, Corollary 10.2 can be obtained by classical methods, using Hilbert's irreducibility theorem. See [FLN22, Example 1.13] for details. For general subgroups $\mathcal{A}$, ours is the first proof we are aware of.

10.2. **Quantitative results: mass computations.** As discussed above, our methods rely upon the fact that, for S_n-n-ic K/k, we have $\mathcal{A} \subseteq N_{K/k}K^\times$ if and only if K satisfies the acceptable family $\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big)_v$ of local conditions. Thus, by the Malle–Bhargava heuristics, we have (certainly for $n \in \{3,4,5\}$ and conjecturally for $n \geq 6$)

$$\lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{X} = \frac{1}{2} \cdot \operatorname{Res}_{s=1} \zeta_k(s) \cdot \prod_{v \in \Pi_k} m\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big),$$

where the product is over all places of k, both finite and infinite. Thus, we may express this density explicitly as an Euler product if we can find the mass $m\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big)$ for each place v of k. We will study these masses in the following two cases:

(1) $n = \ell$ is an odd prime.
(2) $n = 4$.

Our motivation for considering these two cases is that they include each of $n = 3$, $n = 4$, and $n = 5$, which are the degrees for which the Malle–Bhargava heuristics are known (Theorem 3.53).

We start by stating the masses at archimedean places, which are easy to compute for all n:

Theorem 10.4. *Let v be an archimedean (i.e. infinite) place of k, and let $f : k \to \mathbb{C}$ be the corresponding embedding. The following two statements are true:*

- *If f is a real embedding, then*

$$m\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big) = \begin{cases} \sum_{s=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{s!(n-2s)!2^s} & \text{if } f(\alpha) > 0 \text{ for all } \alpha \in \mathcal{A}, \\ \sum_{s=0}^{\lceil \frac{n}{2} \rceil - 1} \frac{1}{s!(n-2s)!2^s} & \text{otherwise.} \end{cases}$$

- *If f is a complex embedding, then*

$$m\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big) = \frac{1}{n!}.$$

For finite primes $\mathfrak{p}$, we will state the pre-masses $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{n/k_{\mathfrak{p}}}\big)$ instead of the corresponding masses. This is just for notational convenience, as it is trivial to pass from pre-mass to mass. Our next result, Theorem 10.8, states the masses explicitly whenever $n = \ell$ for an odd prime ℓ. Before we can state the result, we need a few definitions. For a p-adic field F, a finitely generated subgroup $\mathcal{A} \subseteq F^\times$, and a positive integer n, define

$$\overline{\mathcal{A}}^n = \mathcal{A}F^{\times n}/F^{\times n}.$$

For each nonnegative integer t, write

$$\overline{\mathcal{A}}^n_t = \overline{\mathcal{A}}^n \cap \big(U_F^{(t)} F^{\times n}/F^{\times n}\big),$$

where $U_F^{(t)}$ is the t^{th} term of the unit filtration, given by $U_F^{(t)} = 1 + \mathfrak{p}_F^t$, and we adopt the convention that $U_F^{(0)} = \mathcal{O}_F^\times$.

Remark 10.5. In the special case $n = 2$, we already saw the groups $\overline{\mathcal{A}}^n$ and $\overline{\mathcal{A}}^n_t$ in Section 8.2. Indeed, in Section 12.2, we will generalise the results of Section 8.2, using more sophisticated proof techniques.

Definition 10.6. Let F be a p-adic field, let n be a positive integer, and let $\overline{\mathcal{A}}$ be a subgroup of $F^\times/F^{\times n}$. A *stratified generating set* for $\overline{\mathcal{A}}$ is a collection $(A_i)_{i\geq 0}$, indexed by nonnegative integers, where each A_i is a subset of $F^\times$, such that the following three conditions hold:

(1) For each i and each $\alpha \in A_i$, we have $v_F(\alpha) = i$.
(2) For $\alpha, \beta \in \bigcup_i A_i$, if $\alpha \neq \beta$ then $[\alpha] \neq [\beta]$ in $F^\times/F^{\times n}$.
(3) The image of $\bigcup_i A_i$ under the natural map $F^\times \to F^\times/F^{\times n}$ is a minimal generating set for the group $\overline{\mathcal{A}}$.

Lemma 10.7. *Let F be a p-adic field, let n be a positive integer, and let $\overline{\mathcal{A}}$ be a subgroup of $F^\times/F^{\times n}$. Write $\mathcal{D}$ for the set of proper divisors of n. There exists a stratified generating set $(A_i)_{i\geq 0}$ for $\overline{\mathcal{A}}$, such that $A_i = \varnothing$ unless $i = 0$ or $i \in \mathcal{D}$.*

Proof. Let $(A_i)_{i\geq 0}$ be any stratified generating set for $\overline{\mathcal{A}}$ (it is clear that such an object exists and is finite). Suppose that there is at least one element $x \in \bigcup_i A_i$ such that $v_F(x) \neq 0$ and $v_F(x) \notin \mathcal{D}$. We will show that $(A_i)_{i\geq 0}$ can be replaced by another stratified generating set with strictly fewer such elements, thus proving the result by induction.

Without loss of generality, we may assume that $1 \leq v_F(x) < n$. Let $a = v_F(x)$, and let g be the greatest common divisor of a and n. By Bézout's Lemma, there exist integers k and l such that $ka + ln = g$. Let $a' = a/g$ and $n' = n/g$, so that a' and n' are coprime. It is easy to see that $v_F(x^k) \equiv g \pmod{n}$ and $v_F(x^{n'}) \equiv 0 \pmod{n}$. Thus, there are elements $\beta_1, \beta_2 \in F^\times$ with $[x]^k = [\beta_1]$ and $[x]^{n'} = [\beta_2]$ in $F^\times/F^{\times n}$, such that $v_F(\beta_1) = g$ and $v_F(\beta_2) = 0$. It is easy to see that k and n' are coprime, so another application of Bézout's Lemma tells us that $\langle [x] \rangle = \langle [\beta_1], [\beta_2] \rangle$, and the result follows. □

Lemma 10.7 tells us that when n is prime, any subgroup of $F^\times/F^{\times n}$ has a stratified generating set of the form (A_0, A_1). Similarly, in the case $n = 4$, any subgroup of $F^\times/F^{\times 4}$ has a stratified generating set of the form (A_0, A_1, A_2). We will use these special cases without reference throughout the rest of the thesis.

We are now ready to state our main result for the case where $n = \ell$ is an odd prime:

Theorem 10.8. *Let p be a rational prime, let F be a p-adic field with residue field of size q, and let ℓ be a rational prime. Let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. Let (A_0, A_1) be a stratified generating set for $\overline{\mathcal{A}}^\ell$. The following four statements are true:*

(1) We have

$$\widetilde{m}(\text{Ét}^{\mathcal{A}}_{\ell/F}) = \widetilde{m}(\text{Ét}^{\mathcal{A}}_{(\ell)/F}) + \widetilde{m}(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}) + (1 - \ell^{-1}) + \sum_{d=1}^{\ell-2} \frac{\operatorname{Part}(d, \ell - d)}{q^d},$$

where $\operatorname{Part}(d, m)$ is the partition function defined in Section 11.

(2) We have

$$\widetilde{m}(\text{Ét}^{\mathcal{A}}_{(\ell)/F}) = \begin{cases} \frac{1}{\ell} & \text{if } A_1 = \varnothing, \\ 0 & \text{otherwise.} \end{cases}$$

(3) Suppose that $p \neq \ell$. Then we have

$$\widetilde{m}(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}) = \begin{cases} \frac{1}{q^{\ell-1}} & \text{if } q \not\equiv 1 \pmod{\ell} \text{ or } \mathcal{A} \subseteq F^{\times \ell}, \\ \frac{1}{\ell q^{\ell-1}} & \text{if } q \equiv 1 \pmod{\ell} \text{ and } A_0 = \varnothing \text{ and } \# A_1 = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(4) *Suppose that $p = \ell$. Then we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^p)/F}\big) = \frac{1}{q^{p-1}} - \widetilde{m}\big(\text{Ét}^{C_p/F}_{(1^p)/F}\big) + \widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big).$$

The two missing ingredients, $\widetilde{m}\big(\text{Ét}^{C_p/F}_{(1^p)/F}\big)$ and $\widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big)$, are as follows. We have

$$\widetilde{m}\big(\text{Ét}^{C_p/F}_{(1^p)/F}\big) = \frac{q-1}{p-1}\cdot q^{-2}\cdot\Big(\mathbb{1}_{e_F \geq p-1}\cdot A\Big(\Big\lceil\frac{pe_F}{p-1}\Big\rceil\Big)+\mathbb{1}_{(p-1)\nmid e_F}\cdot B\Big(\Big\lceil\frac{pe_F}{p-1}\Big\rceil\Big)\Big)+\mathbb{1}_{\mu_p\subseteq F}\cdot q^{-(p-1)(e_F+1)},$$

where A and B are the explicit functions defined in Appendix B, and

$$\widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big) = \mathbb{1}_{\mu_p\subseteq F}\cdot\mathbb{1}_{\overline{\mathcal{A}}^p_{\frac{pe_F}{p-1}}=0}\cdot\frac{q^{-(p-1)(e_F+1)}}{\#\overline{\mathcal{A}}^p}+\frac{1}{(p-1)\#\overline{\mathcal{A}}^p}\cdot q^{-2}\cdot\sum_{\substack{1\leq c\leq\lceil\frac{pe_F}{p-1}\rceil\\ c\not\equiv 1 \pmod p}}\frac{q\cdot\#\overline{\mathcal{A}}^p_c-\#\overline{\mathcal{A}}^p_{c-1}}{q^{(p-2)c+\lfloor\frac{c-2}{p}\rfloor}}.$$

Since the sizes $\#\overline{\mathcal{A}}^p_c$ can all be different, the series for $\widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big)$ does not have a closed form. In the special case where $\mathcal{A}$ is generated by one element, we can write down such a closed form, which is stated in Theorem 12.37. Along the way, we find the exact number of extensions $L \in \text{Ét}^{C_p/F}_{(1^p)/F}$ with each possible discriminant, which we state in Theorem 12.24.

We now turn our attention to the final case of particular interest, $n = 4$. When $\mathfrak{p}$ is a prime of k not lying over 2, the pre-masses $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{4/k_\mathfrak{p}}\big)$ are described explicitly by the following result:

Theorem 10.9. *Let p be a rational prime and let F be a p-adic field with residue field of size q. For any choice of p, we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{4/F}\big) = \frac{5q^2+8q+8}{8q^2} + \sum_{\sigma\in\{(4),(22),(1^21^2),(2^2),(1^4)\}}\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{\sigma/F}\big).$$

Moreover, the following statements are true:

(1) *For any choice of p, we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(4)/F}\big) = \begin{cases}\frac{1}{4} & \textit{if } 4 \mid v_F(\alpha) \textit{ for all } \alpha\in\mathcal{A},\\ 0 & \textit{otherwise,}\end{cases}$$

and

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(22)/F}\big) = \begin{cases}\frac{1}{8} & \textit{if } 2 \mid v_F(\alpha) \textit{ for all } \alpha\in\mathcal{A},\\ 0 & \textit{otherwise.}\end{cases}$$

(2) *Suppose that $p \neq 2$. Let (A_0, A_1) be a stratified generating set for $\overline{\mathcal{A}}^2$. Then we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^21^2)/F}\big) = \begin{cases}\frac{1}{2q^2} & \textit{if } \mathcal{A}\subseteq F^{\times 2},\\ \frac{3}{8q^2} & \textit{else if } A_0 = \varnothing \textit{ and } \#A_1 = 1,\\ \frac{1}{4q^2} & \textit{otherwise.}\end{cases}$$

(3) *Suppose that $p \neq 2$. Let (A_0, A_1, A_2) be a stratified generating set for $\overline{\mathcal{A}}^4$. Then we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(2^2)/F}\big) = \begin{cases}\frac{1}{2q^2} & \textit{if } A_0\subseteq F^{\times 2} \textit{ and } A_1 = A_2 = \varnothing,\\ \frac{1}{4q^2} & \textit{else if } A_0\subseteq F^{\times 2} \textit{ and } A_1 = \varnothing \textit{ and } \frac{\alpha_i}{\alpha_j}\in F^{\times 2} \textit{ for all } \alpha_i,\alpha_j\in A_2,\\ 0 & \textit{otherwise.}\end{cases}$$

If $q \equiv 1 \pmod 4$, then we have

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^4)/F}\big) = \begin{cases} \frac{1}{q^3} & \textit{if } \mathcal{A} \subseteq F^{\times 4}, \\ \frac{1}{2q^3} & \textit{if } A_0 = A_1 = \varnothing \textit{ and } \#A_2 = 1 \textit{ and } A_2 \subseteq F^{\times 2}, \\ \frac{1}{4q^3} & \textit{if } A_0 = A_2 = \varnothing \textit{ and } \#A_1 = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

If $q \equiv 3 \pmod 4$, then

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^4)/F}\big) = \begin{cases} \frac{1}{q^3} & \textit{if } \mathcal{A} \subseteq F^{\times 2}, \\ \frac{1}{2q^3} & \textit{if } A_0 = A_2 = \varnothing \textit{ and } \#A_1 = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

So our problem is completely solved for $\mathfrak{p} \nmid 2$. Since there are only finitely many primes $\mathfrak{p} \mid 2$, it suffices to have a practicable method for computing $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{4/k_{\mathfrak{p}}}\big)$ for each such $\mathfrak{p}$. In principle, this can be done by brute-force, since there are finitely many isomorphism classes of quartic étale algebras over $k_{\mathfrak{p}}$, and we can find all of them e.g. by adapting the methods of [PR01]. Unfortunately, [Kra66, Theorem 2] tells us that $\#\text{Ét}_{4/k_{\mathfrak{p}}}$ is on the order of $2^{3[k_{\mathfrak{p}}:\mathbb{Q}_2]}$, which becomes very large very quickly, so the brute-force approach is unfeasible in many cases.

For $\mathfrak{p} \mid 2$, Theorem 10.9 tells us the value of $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{\sigma/k_{\mathfrak{p}}}\big)$ for all $\sigma \notin \{(1^21^2), (2^2), (1^4)\}$, so it remains to address these three cases. For $\sigma = (1^21^2)$ and $\sigma = (2^2)$, we state the required masses in Theorems 10.10 and 10.11, respectively.

For each integer m, define the explicit function $N^{\neq}_{(1^21^2)}$ by

$$N^{\neq}_{(1^21^2)}(m) = \begin{cases} 2(q-1)^2 q^{\frac{m}{2}-2}(\frac{m}{2}-1) - \mathbb{1}_{4\mid m}(q-1)q^{\frac{m}{4}-1} & \text{if } 4 \leq m \leq 2e_F \text{ and } m \text{ is even}, \\ 2(q-1)^2 q^{\frac{m}{2}-2}(2e_F - \frac{m}{2}+1) - \mathbb{1}_{4\mid m}(q-1)q^{\frac{m}{4}-1} & \text{if } 2e_F+2 \leq m \leq 4e_F \text{ and } m \text{ is even}, \\ 4(q-1)q^{\frac{m-1}{2}-1} & \text{if } 2e_F+3 \leq m \leq 4e_F+1 \text{ and } m \text{ is odd}, \\ q^{e_F}(2q^{e_F}-1) & \text{if } m = 4e_F+2, \\ 0 & \text{otherwise.} \end{cases}$$

For the reader's convenience, we will also state the definition of $N^{\neq}_{(1^21^2)}(m)$ in Appendix B.

Theorem 10.10. *Let F be a 2-adic field with residue field of size q and absolute ramification index e_F. The pre-mass $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^21^2)/F}\big)$ is equal to the sum of the following quantities:*

(1)

$$\frac{1}{8} \cdot \sum_{4 \leq m \leq 4e_F+2} q^{-m} \#\text{Ét}^{\mathcal{A}}_{(1^2)/F, \frac{m}{2}},$$

which can be stated explicitly using Corollary 8.13.

(2)

$$\frac{1}{4} \cdot \sum_{4 \leq m \leq 4e_F+2} q^{-m} N^{\neq}_{(1^21^2)}(m),$$

where $N^{\neq}_{(1^21^2)}$ is the explicit function defined in Appendix B.

In order to address the symbols (2^2) and (1^4), and specifically to understand the C_4-extensions, we need some further definitions. Let F be a 2-adic field, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. Let $\mathcal{G}_4(\mathcal{A}) \subseteq F^\times$ be a subset whose image in $F^\times/F^{\times 4}$ generates the group $\overline{\mathcal{A}}^4$. We will assume that a choice of $\mathcal{G}_4(\mathcal{A})$ is fixed implicitly in the definition of $\mathcal{A}$; all results dependent on $\mathcal{G}_4(\mathcal{A})$ will be independent of this choice. Recall from Part 3 that a C_4-*extendable extension* of F is a quadratic field extension E/F that can be embedded into a C_4-extension of F. The set of isomorphism classes of C_4-extendable extensions is denoted by $\mathrm{Ext}_{2/F}^{\uparrow C_4}$. Let $E \in \mathrm{Ext}_{2/F}^{\uparrow C_4,\mathcal{A}}$, and let $\omega \in E^\times$ be such that $E(\sqrt{\omega})$ is an element of $\mathrm{Ext}_{2/E}^{C_4/F}$ with minimal discriminant valuation. For each $\alpha \in F^\times$, write

$$N_\alpha = N_{F(\sqrt{\alpha})/F} F(\sqrt{\alpha})^\times,$$

and similarly write

$$N_\omega = N_{E(\sqrt{\omega})/F} E(\sqrt{\omega})^\times.$$

Define

$$N_\omega^{\mathcal{A}} = \bigcap_{\alpha \in \mathcal{G}_4(\mathcal{A}) \cap N_\omega} \overline{N}_\alpha^2 \setminus \bigcup_{\alpha \in \mathcal{G}_4(\mathcal{A}) \setminus N_\omega} \overline{N}_\alpha^2 \subseteq F^\times/F^{\times 2}.$$

For each $E \in \mathrm{Ext}_{2/F}^{\uparrow C_4,\mathcal{A}}$, fix once and for all a choice of element ω as defined above, and write

$$N_E^{\mathcal{A}} = N_\omega^{\mathcal{A}}.$$

For each nonnegative integer c, write

$$N_{E,c}^{\mathcal{A}} = N_E^{\mathcal{A}} \cap \big(U_F^{(c)} F^{\times 2}/F^{\times 2}\big).$$

Theorem 10.11. *Let F be a 2-adic field, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. If $2 \nmid v_F(\alpha)$ for some $\alpha \in \mathcal{A}$, then $\text{Ét}_{(2^2)/F}^{\mathcal{A}} = \varnothing$. Otherwise, the following four statements are true:*

(1) For $G \in \{S_4, A_4\}$, we have $\text{Ét}_{(2^2)/F}^{G/F} = \varnothing$, so

$$\widetilde{m}\big(\text{Ét}_{(2^2)/F}^{G/F,\mathcal{A}}\big) = 0.$$

(2) We have

$$\widetilde{m}\big(\text{Ét}_{(2^2)/F}^{D_4/F,\mathcal{A}}\big) = \frac{1}{2} \cdot \Big(q^{-2} - q^{-2e_F-2} - \frac{1}{q^2+q+1}\Big(q^{-1} - q^{-3e_F-1}\Big) + q^{-3e_F-2}\Big(q^{e_F} - 1\Big)\Big).$$

(3) We have

$$\widetilde{m}\big(\text{Ét}_{(2^2)/F}^{V_4/F,\mathcal{A}}\big) = \frac{1}{4\#\overline{\mathcal{A}}^2}\Big(\mathbb{1}_{\overline{\mathcal{A}}^2_{2e_F}=0} \cdot q^{-3e_F-2} + \sum_{c=1}^{e_F} q^{-3c-1}\Big(q \cdot \#\overline{\mathcal{A}}^2_{2c} - \#\overline{\mathcal{A}}^2_{2c-1}\Big)\Big).$$

(4) Let E be the unique unramified quadratic extension of F. If $2 \mid v_F(\alpha)$ for all $\alpha \in \mathcal{A}$, then $\widetilde{m}\big(\text{Ét}_{(2^2)/F}^{C_4/F,\mathcal{A}}\big)$ is the sum of the following two quantities:

(a)

$$\frac{1}{8} \cdot \sum_{c=1}^{e_F} q^{-4c}(\#N_{E,2e_F-2c}^{\mathcal{A}} - \#N_{E,2e_F-2c+2}^{\mathcal{A}}),$$

(b)

$$\frac{1}{8} \cdot q^{-4e_F-2}(\#N_E^{\mathcal{A}} - N_{E,0}^{\mathcal{A}}).$$

Otherwise, we have $\widetilde{m}\big(\text{Ét}_{(2^2)/F}^{C_4/F,\mathcal{A}}\big) = 0$.

For $\sigma = (1^4)$, the actual mass is too cumbersome to state in closed form, so we instead study the quantities $\#\text{Ét}_{(1^4)/F,m}^{G/F,\mathcal{A}}$ for each G. For $G \neq C_4$, we state these quantities explicitly. For $G = C_4$, we give a formula for $\#\text{Ét}_{(1^2)/E,m_2}^{C_4/F,\mathcal{A}}$, whenever E is a totally ramified quadratic extension of F and m_2 is an integer.

Let m_1 be either $2e_F+1$ or an even integer with $2 \le m_1 \le 2e_F$. Define

$$N^{V_4}(m_1,m_2) = \begin{cases} 2(q-1)q^{\frac{m_2}{2}-1} & \text{if } 2 \le m_2 < m_1 \text{ and } m_2 \text{ is even,} \\ (q-2)q^{\frac{m_1}{2}-1} & \text{if } m_2 = m_1 \text{ and } m_1 \text{ is even,} \\ (q-1)q^{\frac{m_1+m_2}{4}-1} & \text{if } m_1 < m_2 \le 4e_F - m_1 \text{ and } m_1 \equiv m_2 \pmod 4, \\ q^{e_F} & \text{if } m_2 > m_1 \text{ and } m_1+m_2 = 4e_F+2, \\ 0 & \text{otherwise.} \end{cases}$$

Define $N^{V_4}(m_1,m_2)=0$ for all other pairs of integers (m_1,m_2). For each integer m_2, define

$$N^{C_2}(m_2) = \begin{cases} 2(q-1)q^{\frac{m_2}{2}-1} & \text{if } 0 \le m_2 \le 4e_F \text{ and } m_2 \text{ is even,} \\ 2q^{2e_F} & \text{if } m_2 = 4e_F+1, \\ 0 & \text{otherwise.} \end{cases}$$

For the reader's convenience, we will also state the definitions of $N^{V_4}(m_1,m_2)$ and $N^{C_2}(m_2)$ in Appendix B.

Theorem 10.12. *Let F be a 2-adic field, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. The following four statements are true:*

(1) For $G \in \{S_4, A_4\}$, we have

$$\widetilde{m}\big(\text{Ét}^{G/F,\mathcal{A}}_{(1^4)/F}\big) = \widetilde{m}\big(\text{Ét}^{G/F}_{(1^4)/F}\big),$$

which is known from Corollaries 5.8 and 5.9.

(2) For each positive integer m, we have

$$\#\text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m} = \frac{1}{2}\sum_{0<m_1<m/2} \#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1} \cdot \Big(N^{C_2}(m_2) - N^{C_4}(m_1,m_2) - N^{V_4}(m_1,m_2)\Big),$$

where N^{C_2}, N^{C_4}, and N^{V_4} are the functions defined in Appenix B. We can compute this quantity explicitly using Corollary 12.31.

(3) Let m be a positive integer. The quantity $\#\text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m}$ is the sum of the following two quantities:

(a)

$$\frac{1}{2}\cdot\sum_{\substack{m_1<m_2\\ m_1+2m_2=m}} (\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1})(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_2}).$$

(b)

$$\mathbb{1}_{3|m}\cdot\frac{2}{3(\#\overline{\mathcal{A}}^2)^2}\cdot q^{\frac{m}{6}-2}\Big(q\#\overline{\mathcal{A}}^2_{m/3} - \#\overline{\mathcal{A}}^2_{m/3-1}\Big)\Big(q\#\overline{\mathcal{A}}^2_{m/3} - 2\#\overline{\mathcal{A}}^2_{m/3-1}\Big).$$

This expression can be made explicit using Corollary 12.31.

(4) Let $E \in \text{Ét}^{\mathcal{A}}_{(1^2)/F}$ be a C_4-extendable extension, let $m_1 = v_F(d_{E/F})$, and let m_2 be a positive integer. If $m_1 > e_F$, then

$$\text{Ét}^{C_4/F,\mathcal{A}}_{(1^2)/E,m_2} = \begin{cases} \frac{1}{2}\cdot\#N^{\mathcal{A}}_E & \textit{if } m_2 = m_1+2e_F, \\ 0 & \textit{otherwise.} \end{cases}$$

Suppose instead that $m_1 \le e_F$. For each even integer t, define

$$c(t) = 2e_F - 2\Big\lfloor\frac{m_1+t}{4}\Big\rfloor.$$

Then we have

$$\#\text{Ét}^{C_4/F,\mathcal{A}}_{(1^2)/E,m_2} = \begin{cases} \frac{1}{2}\cdot \#N^{\mathcal{A}}_{E,c(m_2)} & \textit{if } m_2 = 3m_1 - 2, \\ \frac{1}{2}\cdot \left(\#N^{\mathcal{A}}_{E,c(m_2)} - \#N^{\mathcal{A}}_{E,c(m_2-2)}\right) & \textit{if } 3m_1 \le m_2 \le 4e_F - m_1 + 1 \textit{ and } m_2 \textit{ is even}, \\ \frac{1}{2}\cdot \left(\#N^{\mathcal{A}}_{E} - \#N^{\mathcal{A}}_{E,c(m_2-2)}\right) & \textit{if } m_2 = 4e_F - m_1 + 2, \\ 0 & \textit{otherwise.} \end{cases}$$

Using the formula in Theorem 10.12, we are able to formulate an efficient algorithm for computing $\#\text{Ét}^{C_4/k_{\mathfrak{p}},\mathcal{A}}_{(1^4)/k_{\mathfrak{p}},m}$ for each m. We will state the time complexity of this algorithm in Theorem 10.13, but first we need some notation.

Let F be a p-adic field for some rational prime p. In most computer algebra packages, p-adic fields are defined up to a certain *precision*, which refers to the length of p-adic series representations stored. We will be working with field extensions E/F with $[E:F] \le 4$, and we need enough precision to construct the quotient $E^\times/E^{\times 4}$ of units modulo fourth powers. It follows that we need precision on the order of e_F. Suppose that we are working with precision m. In any sensible implementation, the computation time for a field operation in F will be polynomial in $[F:\mathbb{Q}_p]$ and m. Since for our applications we have $m = O(e_F)$, a field operation in F can be performed with time complexity $O(t([F:\mathbb{Q}_p]))$, for some polynomial function t. Moreover, since we are bounding the degree by a constant, any field operation in any extension E/F with $[E:F] \le 4$ can also be performed with time complexity $O(t([F:\mathbb{Q}_p]))$. Given a function f in unspecified variables, we write

$$O_F(f) = O(f \cdot t([F:\mathbb{Q}_p])).$$

Thus, the notation O_F should be thought of as Big O notation, where we are suppressing the polynomial $t([F:\mathbb{Q}_2])$ to account for field operations in F, and quadratic and quartic extensions thereof. By the discussion above, the brute-force computation of $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{4/k_{\mathfrak{p}}}\big)$ has time complexity at least $O_{k_{\mathfrak{p}}}\big(\#\mathcal{G}_4(\mathcal{A}) \cdot 2^{3[k_{\mathfrak{p}}:\mathbb{Q}_2]}\big)$. We present the following improvements:

Theorem 10.13. *Let $\mathfrak{p}$ be a prime of k lying over 2, and choose a set $\mathcal{G}_4(\mathcal{A})$ as above. There are two algorithms for computing $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{4/k_{\mathfrak{p}}}\big)$, whose time complexities respectively are as follows:*

(1)
$$O_{k_{\mathfrak{p}}}\big(e_{k_{\mathfrak{p}}} \cdot \#\mathcal{G}_4(\mathcal{A}) \cdot 2^{2[k_{\mathfrak{p}}:\mathbb{Q}_2]} \cdot [k_{\mathfrak{p}}:\mathbb{Q}_2]^3\big).$$

(2)
$$O_{k_{\mathfrak{p}}}\big(e_{k_{\mathfrak{p}}} \cdot 2^{\#\mathcal{G}_4(\mathcal{A})} \cdot 2^{[k_{\mathfrak{p}}:\mathbb{Q}_2]} \cdot [k_{\mathfrak{p}}:\mathbb{Q}_2]^3\big).$$

Remark 10.14. The first time complexity in Theorem 10.13 is unconditionally a big improvement over the brute-force algorithm. The second time complexity is a significantly bigger improvement, conditional on the number of generators of $\overline{\mathcal{A}}^4$ being kept reasonably small. Thus, the algorithms are both useful, and the choice between them will depend on the application.

11. Results for general n

The main goal of this section is to prove Theorem 10.1, along with its conjectural generalisations in Theorems 11.10 and 11.12. We start by proving Theorem 10.4, which addresses the case where v is an archimedean place.

Proof of Theorem 10.4. Suppose that f is a real embedding. Then

$$\text{Ét}_{n/k_v} = \{\mathbb{R}^r \times \mathbb{C}^s : r + 2s = n \text{ and } r, s \geq 0\}.$$

If $L = \mathbb{R}^r \times \mathbb{C}^s$, then we have

$$N_{L/k_v} L^\times = \begin{cases} \mathbb{R}^\times & \text{if } r > 0, \\ \mathbb{R}_{>0} & \text{if } r = 0, \end{cases}$$

and

$$\#\operatorname{Aut}(L/k_v) = 2^s \cdot r! \cdot s!.$$

The result for real f follows. If f is a complex embedding, then the only element of $\text{Ét}_{n/k_v}$ is $\mathbb{C}^n$, which has $n!$ automorphisms and norm group $\mathbb{C}^\times$, so we are done. □

11.1. **Expressing our problem in terms of local conditions.** As we discussed in Section 10, for each place v of k, we may view $\mathcal{A}$ as a subgroup of $k_v^\times$, so it makes sense to write $\text{Ét}_{n/k_v}^{\mathcal{A}}$, which is the set of degree n étale algebras L/k_v with $\mathcal{A} \subseteq N_{L/k_v} L^\times$. In particular, we have a system of local conditions $\big(\text{Ét}_{n/k_v}^{\mathcal{A}}\big)_v$.

The following theorem says that for an extension K/k, we have $\mathcal{A} \subseteq N_{K/k} K^\times$ if and only if K satisfies the system of local conditions $\big(\text{Ét}_{n/k_v}^{\mathcal{A}}\big)_v$:

Theorem 11.1 (Hasse Norm Principle holds for S_n-n-ics)**.** *Let n be a positive integer, let K/k be an S_n-n-ic extension of number fields, and let $\mathcal{A} \subseteq k^\times$ be a finitely generated subgroup. Then $\mathcal{A} \subseteq N_{K/k} K^\times$ if and only if K/k satisfies the system $\big(\text{Ét}_{n/k_v}^{\mathcal{A}}\big)_v$ of local conditions.*

Proof. This is [Vos88, Corollary to Theorem 4]. □

Remark 11.2 (The Hasse norm principle is a special case of the Hasse principle)**.** Theorem 11.1 says that being a norm globally is equivalent to being a norm everywhere locally. On the surface, the result looks quite different from the usual Hasse principle, since the former is about norms of field extensions, while the latter is about roots of polynomials. However, given a k-basis $\{e_1, \ldots, e_n\}$ for K, we have a homogeneous degree n polynomial

$$f(x_1, \ldots, x_n) = N_{K/k}(x_1 e_1 + \ldots + x_n e_n) \in k[x_1, \ldots, x_n].$$

The Hasse norm principle then says that the polynomial $f(\mathbf{x}) - \alpha$ has a root in k if and only if it has a root in k_v for every place v of k. Thus, Theorem 11.1 says precisely that the Hasse principle holds for so-called "norm equations".

Lemma 11.3. *Let k be a number field, let n be an integer with $n \geq 3$, and let $\mathcal{A} \subseteq k^\times$ be a finitely generated subgroup. Then the system $\big(\text{Ét}_{n/k_v}^{\mathcal{A}}\big)_v$ of local conditions is acceptable.*

Proof. Let $\mathfrak{p}$ be a finite prime such that $\gcd(\operatorname{Nm}(\mathfrak{p}), n) = 1$ and $v_\mathfrak{p}(\alpha) = 0$ for all $\alpha \in \mathcal{A}$. Note that all but finitely many primes satisfy these conditions. Let $L \in \text{Ét}_{n/k_\mathfrak{p}}$ such that $v_{k_\mathfrak{p}}(d_{L/k_\mathfrak{p}}) \leq 1$. Writing $L = L_1 \times \ldots \times L_r$ for field extensions $L_i/k_\mathfrak{p}$, at most one of the extensions $L_i/k_\mathfrak{p}$ is ramified, so either $L = L_1$ or $L_i/k_\mathfrak{p}$ is unramified for some i. Suppose that $L = L_1$. Let $(L, k_\mathfrak{p}) = (f^e)$. Since $\operatorname{Nm}(\mathfrak{p})$ is coprime to n, the field extension $L/k_\mathfrak{p}$ is tamely ramified, so Lemma 3.11 tells us that $v_{k_\mathfrak{p}}(d_{L/k_\mathfrak{p}}) = f(e-1)$, and therefore $f = 1$ and $e \leq 2$, so $n \leq 2$, contradicting the assumption that $n \geq 3$. Therefore, $L_i/k_\mathfrak{p}$ is unramified for some i, so $\mathcal{O}_{k_\mathfrak{p}}^\times \subseteq N_{L/k_\mathfrak{p}} L^\times$, and hence $L \in \text{Ét}_{n/k_\mathfrak{p}}^{\mathcal{A}}$. The result follows. □

Corollary 11.4. *For $n \in \{3,4,5\}$, we have*

$$\lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{X} = \frac{1}{2} \cdot \operatorname*{Res}_{s=1}\big(\zeta_k(s)\big) \cdot \prod_{v\in\Pi_k} m\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big),$$

and the same result holds conjecturally for $n \geq 6$, subject to the Malle–Bhargava heuristics.

Proof. This is immediate from Theorem 3.53, Theorem 11.1, and Lemma 11.3. □

Recall the notion of *splitting symbols* from Section 3. Call a splitting symbol $(f_1^{e_1}\dots f_r^{e_r})$ *predictable* if the integers e_i are mutually coprime. Call a symbol $(f_1^{e_1}\dots f_r^{e_r})$ *epimorphic* if it is predictable and the integers f_i are mutually coprime. For a p-adic field F, write $\text{Ét}^{\text{pred}}_{n/F}$ and $\text{Ét}^{\text{epi}}_{n/F}$ for the sets of $L \in \text{Ét}_{n/F}$ such that (L,F) is predictable and epimorphic, respectively. Write $\text{Split}^{\text{pred}}_n$ and $\text{Split}^{\text{epi}}_n$ for the sets of predictable and epimorphic degree n splitting symbols, respectively. The following lemma justifies the terminology; it says that predictable splitting symbols have "predictable" norm groups, and epimorphic splitting symbols have surjective norm maps.

Lemma 11.5. *Let F be a p-adic field and let σ be a predictable splitting symbol. Write $\sigma = (f_1^{e_1}\dots f_r^{e_r})$ and let $L \in \text{Ét}_{\sigma/F}$. Let $g = \gcd(f_1,\dots,f_r)$. Then we have*

$$N_{L/F}L^\times = \big\{x \in F^\times : g \mid v_F(x)\big\}.$$

In particular, if $L \in \text{Ét}^{\text{epi}}_{n/F}$, then

$$N_{L/F}L^\times = F^\times.$$

Proof. Write $L = L_1 \times \ldots \times L_r$, where each L_i/F is a field extension with ramification index e_i and inertia degree f_i. For each i, let L_i^{ur} be the maximal unramified subextension of L_i/F. By considering the towers $L_i/L_i^{\text{ur}}/F$, it is easy to see that we have

$$\mathcal{O}_F^{\times e_i} \subseteq N_{L_i/F}L_i^\times$$

for each i. Moreover, for each i, there is some $x_i \in N_{L_i/F}L_i^\times$ with $v_F(x_i) = f_i$. Since the e_i are mutually coprime, there exist integers r_i such that $\sum_i r_i e_i = 1$, so for each $\alpha \in \mathcal{O}_F^\times$, we have

$$\alpha = \prod_i (\alpha^{e_i})^{r_i} \in \prod_i N_{L_i/F}L_i^\times = N_{L/F}L^\times.$$

Therefore, $\mathcal{O}_F^\times \subseteq N_{L/F}L^\times$. On the other hand, there are integers s_i such that $\sum_i s_i f_i = g$. Setting

$$x = \prod_i x_i^{s_i} \in N_{L/F}L^\times,$$

we obtain $v_F(x) = g$, so

$$\{x \in F^\times : g \mid v_F(x)\} \subseteq N_{L/F}L^\times.$$

Conversely, we have

$$N_{L_i/F}L_i^\times \subseteq N_{L_i^{\text{ur}}/F}L_i^{\text{ur},\times} = \{x \in F^\times : f_i \mid v_F(x)\} \subseteq \{x \in F^\times : g \mid v_F(x)\}$$

for each i, so we are done. □

Corollary 11.6. *Let F be a p-adic field and let $\mathcal{A} = \langle \alpha_1,\dots,\alpha_d\rangle$ be a finitely generated subgroup of $F^\times$. Let n be a positive integer and suppose that $n \mid v_F(\alpha_i)$ for each i. For every finite prime $\mathfrak{p}$ of k, we have*

$$\text{Ét}^{\text{pred}}_{n/k_{\mathfrak{p}}} \subseteq \text{Ét}^{\mathcal{A}}_{n/k_{\mathfrak{p}}}.$$

Proof. This is immediate from Lemma 11.5. □

Lemma 11.7. *Let n be an integer with $n \geq 3$, let p be a rational prime with $p > n$, let F be a p-adic field, and let $L \in \text{Ét}_{n/F} \setminus \text{Ét}^{\text{pred}}_{n/F}$. Then $v_F(d_{L/F}) \geq 2$.*

Proof. Let $(L, F) = (f_1^{e_1} \ldots f_r^{e_r})$. Since $p > n$, we have $p \nmid e_i$ for each i, so by Lemma 3.11 we have

$$v_F(d_{L/F}) = \sum_i f_i(e_i - 1).$$

Since (L, F) is not predictable, the e_i are not mutually coprime, so there is some $d \geq 2$ with $d \mid e_i$ for all i, and therefore $e_i \geq 2$ for each i. If any of the integers e_i is at least 3, then we are done. On the other hand, if $e_i = 2$ for every i, then

$$v_F(d_{L/F}) = \sum_i f_i = \frac{n}{2} > 1,$$

so we are done. □

Lemma 11.8. *For $n \geq 3$, we have*

$$\prod_{v \in \Pi_k} \frac{\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big)}{\widetilde{m}\big(\text{Ét}_{n/k_v}\big)} > 0.$$

Proof. Since the factor

$$\frac{\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{n/k_v}\big)}{\widetilde{m}\big(\text{Ét}_{n/k_v}\big)}$$

is strictly positive for each v, without loss of generality we may assume that $v = \mathfrak{p}$ is a finite prime with $\text{char}(\mathcal{O}_k/\mathfrak{p}) > n$ and $v_{\mathfrak{p}}(\alpha_i) = 0$ for all i. Then all degree n étale algebras $L/k_{\mathfrak{p}}$ are tamely ramified, so Lemma 3.11 tells us that[1]

$$v_{k_{\mathfrak{p}}}(d_{L/k_{\mathfrak{p}}}) = d_{(L,k_{\mathfrak{p}})},$$

for each $L \in \text{Ét}_{n/k_{\mathfrak{p}}}$. For $0 \leq d \leq n-1$, let $a_d = \text{Part}(d, n-d)$. Corollary 3.10, Corollary 11.6, and Lemma 11.7 tell us that

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{n/k_{\mathfrak{p}}}\big) \geq \widetilde{m}\big(\text{Ét}^{\text{pred}}_{n/k_{\mathfrak{p}}}\big) \geq a_0 + a_1 q^{-1}$$

and

$$\widetilde{m}\big(\text{Ét}_{n/k_{\mathfrak{p}}}\big) = a_0 + a_1 q^{-1} + \ldots + a_{n-1} q^{-(n-1)},$$

where we write q as shorthand for $\text{Nm}(\mathfrak{p})$. It is easy to write down a positive real number a, independent of $\mathfrak{p}$, such that

$$1 - a q^{-2} \leq \frac{\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{n/k_{\mathfrak{p}}}\big)}{\widetilde{m}\big(\text{Ét}_{n/k_{\mathfrak{p}}}\big)} \leq 1,$$

and the result follows. □

Lemma 11.9. *Let F be a local field and let n be any positive integer. Then*

$$\bigcap_{L \in \text{Ét}_{n/F}} N_{L/F} L^\times = F^{\times n}.$$

[1] Recall that $d_{(L,k_{\mathfrak{p}})}$ was defined in Definition 3.8.

Proof. If F is $\mathbb{R}$ or $\mathbb{C}$, then the result is easy to see. Therefore, we will assume that F is p-adic. By the structure theorem for finitely generated abelian groups, we may write

$$F^\times/F^{\times n} = \bigoplus_{i=1}^{r} (\mathbb{Z}/d_i\mathbb{Z})e_i,$$

for basis elements $e_i \in F^\times/F^{\times n}$ and integers $d_i \geq 2$ with $d_i \mid n$. For each i, let

$$A_i = \bigoplus_{j\neq i} (\mathbb{Z}/d_j\mathbb{Z})e_j,$$

and let E_i/F be the degree d_i abelian field extension with

$$\big(N_{E_i/F}E_i^\times\big)/F^{\times n} = A_i.$$

For each i, let L_i/E_i be any field extension of degree $\frac{n}{d_i}$, so that

$$\big(N_{L_i/F}L_i^\times\big)/F^{\times n} \subseteq A_i.$$

The result follows since $\bigcap_i A_i = 0$. □

Theorem 11.10. *Let $n \geq 3$, let k be a number field, and let $\mathcal{A} \subseteq k^\times$ be a finitely generated subgroup. Assuming Conjecture 3.54 is true for n (as is the case for $n \leq 5$), we have*

$$0 < \lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{N_{k,n}(X)} \leq 1,$$

with equality if and only if

$$\mathcal{A} \subseteq \ker\Big(k^\times \to \prod_{v\in\Pi_k} k_v^\times/k_v^{\times n}\Big).$$

Proof. Since we are assuming that Conjecture 3.54 holds for n, Lemma 11.8 and Corollary 11.4 tell us that

$$0 < \lim_{X\to\infty} \frac{N_{k,n}(X;\mathcal{A})}{N_{k,n}(X)} \leq 1,$$

with equality if and only if $\text{Ét}_{n/k_v}^{\mathcal{A}} = \text{Ét}_{n/k_v}$ for all $v \in \Pi_k$. The result then follows from Lemma 11.9. □

Definition 11.11. Given a number field k, we say that a positive integer n is *power-pathological in k* if the following three statements are true:

(1) $n = 2^r n'$ for an odd integer n' and an integer $r \geq 3$.
(2) The extension $k(\mu_{2^r})/k$ is not cyclic.
(3) All primes $\mathfrak{p}$ of k lying over 2 decompose in $k(\mu_{2^r})/k$.

Theorem 11.12 (Hasse principle for n^{th} powers)**.** *For any number field k, we have*

$$\#\ker\Big(k^\times/k^{\times n} \to \prod_{v\in\Pi_k} k_v^\times/k_v^{\times n}\Big) = \begin{cases} 1 & \text{if } n \text{ is not power-pathological in } k, \\ 2 & \text{if } n \text{ is power-pathological in } k. \end{cases}$$

Proof. This is the special case $T = \Pi_k$ of [NSW00, Theorem 9.1.11]. □

Corollary 11.13. *If n is not power-pathological in k, then*

$$\ker\Big(k^\times \to \prod_{v\in\Pi_k} k_v^\times/k_v^{\times n}\Big) = k^{\times n}.$$

If n is power-pathological in k, then

$$\ker\Big(k^\times \to \prod_{v\in\Pi_k} k_v^\times/k_v^{\times n}\Big) = k^{\times n}\cup uk^{\times n},$$

for some $u \in k^{\times(n/2)}\setminus k^{\times n}$.

Proof of Theorem 10.1. This is immediate from Theorems 3.53, 11.10, and 11.12. □

Corollary 11.14. *If n is not power-pathological in k and Conjecture 3.54 is true for n, then $\mathcal{A}$ is in the norm group of* 100% *of S_n-n-ics if and only if $\mathcal{A}$ is in the norm group of all S_n-n-ics.*

12. Prime degree extensions

The main purpose of this section is to prove Theorem 10.8, which states the mass $\widetilde{m}\big(\text{Ét}_{\ell/F}^{\mathcal{A}}\big)$ whenever ℓ is an odd prime, F is a p-adic field, and $\mathcal{A}\subseteq F^\times$ is a finitely generated subgroup. We start by fixing some notation: Let p and ℓ be rational primes; let F be a p-adic field with residue field of size q; let π_F be a uniformiser of F; let $\mathcal{A}\subseteq F^\times$ be a finitely generated subgroup.

Lemma 12.1. *We have*

$$\text{Split}_\ell = \{(1^\ell),(\ell)\}\sqcup \text{Split}_\ell^{\text{epi}}.$$

Proof. Let $\sigma\in\text{Split}_\ell\setminus\{(1^\ell),(\ell)\}$. Writing $\sigma=(f_1^{e_1}\dots f_r^{e_r})$, we have $\ell=\sum_i f_ie_i$, so the e_i (respectively the f_i) are mutually coprime, and therefore $\sigma\in\text{Split}_\ell^{\text{epi}}$. □

Corollary 12.2. *We have*

$$\widetilde{m}\big(\text{Ét}_{\ell/F}^{\mathcal{A}}\big) = \widetilde{m}\big(\text{Ét}_{(1^\ell)/F}^{\mathcal{A}}\big)+\widetilde{m}\big(\text{Ét}_{(\ell)/F}^{\mathcal{A}}\big)+\widetilde{m}\big(\text{Ét}_{\ell/F}^{\text{epi}}\big).$$

Proof. This follows easily from Lemmas 11.5 and 12.1. □

Lemma 12.3. *We have*

$$\widetilde{m}\big(\text{Ét}_{\ell/F}^{\text{epi}}\big) = \Big(1-\frac{1}{\ell}\Big)+\sum_{d=1}^{\ell-2}\frac{\text{Part}(d,\ell-d)}{q^d}.$$

Proof. Since (1^ℓ) is the only degree ℓ splitting symbol σ with $d_\sigma=\ell-1$, we have

$$\widetilde{m}\big(\text{Ét}_{\ell/F}^{\text{epi}}\big) = \sum_{d=0}^{\ell-2}\widetilde{m}\big(\{L\in\text{Ét}_{\ell/F}^{\text{epi}} : d_{(L,F)}=d\}\big).$$

Since $d_{(\ell)}=0$, it follows from Lemma 12.1 that

$$\{L\in\text{Ét}_{\ell/F}^{\text{epi}} : d_{(L,F)}=d\} = \{L\in\text{Ét}_{\ell/F} : d_{(L,F)}=d\}$$

whenever $1\le d\le \ell-2$. The result follows from Corollary 3.10. □

Recall from Section 10 that for each positive integer n, we write $\overline{\mathcal{A}}^n$ for the group $\mathcal{A}F^{\times n}/F^{\times n}$. Recall the notion of a stratified generating set from Definition 10.6.

Lemma 12.4. *Let (A_0,A_1) be a stratified generating set for $\overline{\mathcal{A}}^\ell$. Then we have*

$$\widetilde{m}\big(\text{Ét}_{(\ell)/F}^{\mathcal{A}}\big) = \begin{cases}\frac{1}{\ell} & \textit{if } A_1=\varnothing,\\ 0 & \textit{otherwise.}\end{cases}$$

Proof. This follows from the fact that the unramified degree ℓ extension of F has norm group $\mathcal{O}_F^\times F^{\times\ell}$. □

Because of Corollary 12.2 and Lemmas 12.3 and 12.4, it remains only to find the pre-mass $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}\big)$ of totally ramified degree ℓ extensions with $\mathcal{A}$ in their norm group. We address the tamely ramified case $p \neq \ell$ and the wildly ramified case $p = \ell$ separately.

12.1. Finding $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}\big)$ when $p \neq \ell$.

For each positive integer m, fix a primitive m^{th} root of unity ζ_m in the algebraic closure of F.

Lemma 12.5. *Let e be a positive integer coprime to q and define $g = \gcd(e, q-1)$. For $0 \leq j \leq g-1$, define*

$$L_j = F\Big(\sqrt[e]{\zeta_{q-1}^j \pi_F}\Big).$$

The extensions L_j/F are all nonisomorphic, and

$$\text{Ét}_{(1^e)/F} = \big\{L_j : j = 0, 1, \ldots, g-1\big\}.$$

Proof. This is essentially [PR01, Theorem 7.2], where we replace the polynomial $X^e + \zeta_{q-1}^j \pi_F$ with $X^e - \zeta_{q-1}^j \pi_F$. The modifications to the proof are trivial. □

Lemma 12.6. *Suppose that $p \neq \ell$. The following two statements are true:*

1. *If $\ell \mid q-1$, then $\text{Ét}_{(1^\ell)/F} = \{L_0, \ldots, L_{\ell-1}\}$, where $L_j = F\Big(\sqrt[\ell]{\zeta_{q-1}^j \pi_F}\Big)$. Moreover, for each j we have $\operatorname{Aut}(L_j/F) \cong C_\ell$ and*

$$N_{L_j/F} L_j^\times = \big\{u^\ell((-1)^{\ell+1}\zeta_{q-1}^j \pi_F)^m : u \in \mathcal{O}_F^\times, m \in \mathbb{Z}\big\}.$$

2. *If $\ell \nmid q-1$, then $\text{Ét}_{(1^\ell)/F} = \{L\}$, where $L = F(\sqrt[\ell]{\pi_F})$. Moreover, we have $\operatorname{Aut}(L/F) = 1$ and $N_{L/F} L^\times = F^\times$.*

Proof. In both cases, the classification of extensions comes from Lemma 12.5. To prove the statements about norms and automorphisms, we consider the two cases separately.

(1) Suppose that $\ell \mid q-1$, so that $\zeta_\ell \in F^\times$. Since the elements $\zeta_\ell^j \pi_F$ are all uniformisers of F, and π_F is an arbitrary uniformiser, we only need to prove the result for $L_0 = F(\sqrt[\ell]{\pi_F})$. The element $\sqrt[\ell]{\pi_F}$ has minimal polynomial $X^\ell - \pi_F$ over F, which splits in L_0, so L_0/F is Galois, hence cyclic. By class field theory, we have

$$[F^\times : N_{L_0/F} L_0^\times] = \ell.$$

Moreover, it is clear that

$$\big\{u^\ell((-1)^{\ell+1}\pi_F)^m : u \in \mathcal{O}_F^\times, m \in \mathbb{Z}\big\} \subseteq N_{L_0/F} L_0^\times.$$

By [Neu13, Part II, Proposition 3.7], we have

$$[\mathcal{O}_F^\times : \mathcal{O}_F^{\times\ell}] = \#\mu_\ell(F) = \ell.$$

It follows that

$$\big[F^\times : \big\{u^\ell((-1)^{\ell+1}\pi_F)^m : u \in \mathcal{O}_F^\times, m \in \mathbb{Z}\big\}\big] = \ell,$$

and the result follows.

(2) Suppose that $\ell \nmid q-1$. Since $\ell \neq p$ and $\ell \nmid q-1$, the result [NS13, Page 140, Proposition 5.7] tells us that $\zeta_\ell \notin L$. It follows that the polynomial $X^\ell - \pi_F$ has only one root in L, and therefore L/F is not Galois, hence it has only one automorphism. The maximal abelian subextension of L/F is F, so it has trivial norm group.

□

Lemma 12.7. *Suppose that $p \neq \ell$ and $\ell \mid q-1$. Let (A_0, A_1) be a stratified generating set for $\overline{\mathcal{A}}^\ell$. Then*

$$\#\text{Ét}^{\mathcal{A}}_{(1^\ell)/F} = \begin{cases} \ell & \textit{if } \mathcal{A} \subseteq F^{\times \ell}, \\ 1 & \textit{if } A_0 = \varnothing \textit{ and } \#A_1 = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Lemmas 12.5 and 12.6. □

Corollary 12.8. *Suppose that $p \neq \ell$, and let (A_0, A_1) be a stratified generating set for $\overline{\mathcal{A}}^\ell$. The following two statements are true:*

(1) If $\ell \nmid q-1$, then

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}\big) = \frac{1}{q^{\ell-1}}.$$

(2) If $\ell \mid q-1$, then

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}\big) = \begin{cases} \frac{1}{q^{\ell-1}} & \textit{if } \mathcal{A} \subseteq F^{\times \ell}, \\ \frac{1}{\ell q^{\ell-1}} & \textit{if } A_0 = \varnothing \textit{ and } \#A_1 = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This is immediate from Lemmas 3.11, 12.6 and 12.7. □

12.2. Finding $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^\ell)/F}\big)$ when $p = \ell$.

In the current subsection, we will address the wildly ramified case $p = \ell$.

Lemma 12.9. *We have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^p)/F}\big) = \widetilde{m}\big(\text{Ét}_{(1^p)/F}\big) - \widetilde{m}\big(\text{Ét}^{C_p/F}_{(1^p)/F}\big) + \widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big).$$

Proof. Let $L \in \text{Ét}_{(1^p)/F} \setminus \text{Ét}^{C_p/F}_{(1^p)/F}$. Then the maximal abelian subextension of L/F is F, so by class field theory we have $N_{L/F}L^\times = F^\times$. Therefore, we have

$$\text{Ét}^{\mathcal{A}}_{(1^p)/F} = \text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F} \cup \Big(\text{Ét}_{(1^p)/F} \setminus \text{Ét}^{C_p/F}_{(1^p)/F}\Big),$$

and the result follows. □

Let L/F be an abelian extension of p-adic fields, and let $G = \text{Gal}(L/F)$. Write $\mathfrak{f}(L/F)$ for the conductor of the extension L/F, defined to be the smallest integer m such that $U_F^{(m)} \subseteq N_{L/F}L^\times$. For a character $\chi : G \to \mathbb{C}^\times$, the *Artin conductor* of χ is defined to be

$$\mathfrak{f}(\chi) = \sum_{i \geq 0} \frac{|G_i|}{|G_0|}\Big(\chi(1) - \chi(G_i)\Big),$$

where $(G_i)_i$ is the ramification filtration of G, defined by

$$G_i = \Big\{\varphi \in G : v_L\Big(\frac{\varphi(\pi_L) - \pi_L}{\pi_L}\Big) \geq i\Big\},$$

and $\chi(G_i)$ is the average value of $\chi(g)$ as g ranges over G_i. Write $G^\vee$ for the set of characters $\chi : G \to \mathbb{C}^\times$.

Theorem 12.10. *Let L/F be an abelian extension of p-adic fields, and let $G = \mathrm{Gal}(L/F)$. We have*

(1) $\mathfrak{f}(L/F) = \max_{\chi \in G^\vee} \mathfrak{f}(\chi)$.
(2) $v_F(d_{L/F}) = \sum_{\chi \in G^\vee} \mathfrak{f}(\chi)$.

Proof. The first item is [AT68, Page 135, Corollary to Theorem 14]. The second is [Keu23, Theorem 17.50]. □

Lemma 12.11. *Let L/F be a C_p-extension of p-adic fields. Then*

$$\mathfrak{f}(L/F) = \frac{v_F(d_{L/F})}{p-1}.$$

Proof. Take $G = \mathrm{Gal}(L/F) = \langle g \rangle$, and write c for the unique integer with $G_{c-1} \neq G_c$. Writing ω for the complex number $e^{\frac{2\pi i}{p}}$, we have

$$G^\vee = \{\chi_j : j = 0, 1, 2, \ldots, p-1\},$$

where $\chi_j(g) = \omega^j$. We have

$$\mathfrak{f}(\chi_j) = \begin{cases} 0 & \text{if } j = 0, \\ c & \text{otherwise,} \end{cases}$$

so Theorem 12.10 tells us that $\mathfrak{f}(L/F) = c$ and $v_F(d_{L/F}) = (p-1)c$, and the result follows. □

Given a set $\text{Ét}^{\bullet}_{\bullet/F}$ of étale algebras over F, write $\text{Ét}^{\bullet}_{\bullet/F,m}$ and $\text{Ét}^{\bullet}_{\bullet/F,\leq m}$ for the sets of $L \in \text{Ét}^{\bullet}_{\bullet/F}$ with $v_F(d_{L/F}) = m$ and $v_F(d_{L/F}) \leq m$, respectively. Given a field F and vector spaces V and W over F, write $\mathrm{Epi}_F(V, W)$ for the set of surjective F-linear maps $V \to W$.

Lemma 12.12. *Let m be a positive integer. There is a surjective* $(p-1)$*-to-*1 *map*

$$\mathrm{Epi}_{\mathbb{F}_p}\left(F^\times/U_F^{(\lfloor \frac{m}{p-1} \rfloor)} F^{\times p}, \mathbb{F}_p\right) \to \text{Ét}^{C_p/F}_{p/F,\leq m},$$

where the map $\chi : F^\times/U_F^{(\lfloor \frac{m}{p-1} \rfloor)} F^{\times p} \twoheadrightarrow \mathbb{F}_p$ is sent to the unique abelian extension L/F with

$$N_{L/F} L^\times = \ker\left(F^\times \to F^\times/U_F^{(\lfloor \frac{m}{p-1} \rfloor)} F^{\times p} \xrightarrow{\chi} \mathbb{F}_p\right).$$

Proof. This follows from Lemma 12.11 by basic class field theory. □

Corollary 12.13. *For every positive integer m, we have*

$$\#\text{Ét}^{C_p/F}_{p/F,\leq m} = \frac{1}{p-1}\Big(\#\Big(F^\times/U_F^{(\lfloor \frac{m}{p-1} \rfloor)} F^{\times p}\Big) - 1\Big).$$

Proof. This is immediate from Lemma 12.12. □

Lemma 12.14. *Let $u \in \mathcal{O}_F^\times$, and let n be an integer with $n > \frac{pe_F}{p-1}$. Then $U_F^{(n)} F^{\times p} = U_F^{(n+1)} F^{\times p}$.*

Proof. Let $u \in U_F^{(n)} F^{\times p}$. Then there exist elements $a \in F^\times$ and $x \in \mathfrak{p}_F^n$ with $u = a^p(1+x)$. Since $v_F(x) \geq n$ and $n > \frac{pe_F}{p-1}$, it is easy to see that

$$\left(1 + \frac{x}{p}\right)^p \equiv 1 + x \pmod{\mathfrak{p}_F^{n+1}},$$

and it follows that $u \in U_F^{(n+1)} F^{\times p}$, as required. □

Corollary 12.15. *We have* $U_F^{(\lfloor \frac{pe_F}{p-1} \rfloor + 1)} \subseteq F^{\times p}$.

Proof. This follows from Lemma 12.14 by Hensel's lemma. □

Lemma 12.16. *For* $0 \leq i \leq \lfloor \frac{pe_F}{p-1} \rfloor$, *let* $W_i = U_F^{(i)} F^{\times p} / U_F^{(i+1)} F^{\times p}$. *For each positive integer* c, *there is a group isomorphism*

$$F^\times / U_F^{(c)} F^{\times p} \cong \left(F^\times / U_F^{(0)} F^{\times p}\right) \oplus \bigoplus_{i=0}^{\min\{c-1, \lfloor \frac{pe_F}{p-1} \rfloor\}} W_i.$$

Proof. Corollary 12.15 tells us that

$$F^\times / U_F^{(c)} F^{\times p} = F^\times / U_F^{(\lfloor \frac{pe_F}{p-1} \rfloor + 1)} F^{\times p}$$

whenever $c \geq \lfloor \frac{pe_F}{p-1} \rfloor + 1$, so we only need to prove the result for $c \leq \lfloor \frac{pe_F}{p-1} \rfloor + 1$.

The left- and right-hand sides have the same cardinality by definition of the W_i. Moreover, both are p-torsion groups, hence $\mathbb{F}_p$-vector spaces, so they are isomorphic as groups. □

Lemma 12.17. *We have*

$$U_F^{(0)} F^{\times p} = U_F^{(1)} F^{\times p}.$$

Proof. The p-power map

$$\mathbb{F}_F^\times \to \mathbb{F}_F^\times, \quad x \mapsto x^p$$

is injective, hence bijective. Thus, every element of $U_F^{(0)}$ is congruent to a p^{th} power modulo $\mathfrak{p}_F$, and the result follows. □

Lemma 12.18. *Let* $0 \leq i \leq \lfloor \frac{pe_F}{p-1} \rfloor$, *and let* $m \in U_F^{(i)}$.

(1) If $p \nmid i$, *then* $m \in U_F^{(i+1)} F^{\times p}$ *if and only if* $m \in U_F^{(i+1)}$.

(2) If $p \mid i$, *then* $m \in U_F^{(i+1)} F^{\times p}$ *if and only if there is some* $x \in \mathfrak{p}_F^{\frac{i}{p}}$ *such that* $(1+x)^p \equiv m \pmod{\mathfrak{p}_F^{i+1}}$.

(3) If $p \mid i$ *and* $i < \frac{pe_F}{p-1}$, *then* $m \in U_F^{(i+1)} F^{\times p}$, *and in particular*

$$m \equiv \left(1 + \pi_F^{\frac{i}{p}} y\right)^p \pmod{\mathfrak{p}_F^{i+1}},$$

where $[y] \in \mathcal{O}_F/\mathfrak{p}_F$ *is the unique element with* $[y]^p = \left[\frac{m-1}{\pi_F^i}\right]$, *which exists by Lemma 12.17.*

(4) If $i = \frac{pe_F}{p-1}$, *then* $m \in U_F^{(i+1)} F^{\times p}$ *if and only if* $\left[\frac{m-1}{\pi_F^{e_F/(p-1)} p}\right] \in \mathcal{O}_F/\mathfrak{p}_F$ *is in the image of the map*

$$\mathcal{O}_F/\mathfrak{p}_F \to \mathcal{O}_F/\mathfrak{p}_F, \quad y \mapsto y + \frac{\pi_F^{e_F}}{p} y^p,$$

and in that case $m \equiv \left(1 + \pi_F^{\frac{i}{p}} y\right)^p \pmod{\mathfrak{p}_F^{i+1}}$, *for each* y *in the preimage.*

Proof. By Lemma 12.17, the case $i = 0$ is trivial, so we assume that $i \geq 1$. For the first two statements, the "if" directions are trivial, so we focus on the "only if".

Suppose that $m \in U_F^{(i+1)} F^{\times p} \setminus U_F^{(i+1)}$, so $v_F(m-1) = i$. We will show that this implies $p \mid i$ and there is some $x \in \mathfrak{p}_F^{\frac{i}{p}}$ with $(1+x)^p \equiv m \pmod{\mathfrak{p}_F^{i+1}}$, proving the first two statements.

Since $m \in U_F^{(i+1)} F^{\times p}$, there is some $c \in F^\times$ such that $v_F(c) = 0$ and $m \equiv c^p \pmod{\mathfrak{p}_F^{i+1}}$. Write $c = 1 + x$ for $x \in \mathcal{O}_F$, so that

$$m - 1 \equiv \sum_{j=1}^{p-1} \binom{p}{j} x^j + x^p \pmod{\mathfrak{p}_F^{i+1}}.$$

Since $v_F(m-1) > 0$, we have $v_F(x) > 0$, so

$$\begin{cases} v_F\Big(\sum_{j=1}^{p-1} \binom{p}{j} x^j\Big) = e_F + v_F(x), \\ v_F(x^p) = p v_F(x). \end{cases} \tag{9}$$

Suppose for contradiction that $v_F(x) > \frac{e_F}{p-1}$. Then $v_F(x) + e_F < p v_F(x)$, so

$$i = v_F(m-1) = v_F(x) + e_F > \frac{p e_F}{p-1},$$

which is impossible since by assumption $i \leq \frac{p e_F}{p-1}$.

Therefore, $v_F(x) \leq \frac{e_F}{p-1}$. We will consider the cases $v_F(x) = \frac{e_F}{p-1}$ and $v_F(x) < \frac{e_F}{p-1}$ separately. Suppose first that $v_F(x) = \frac{e_F}{p-1}$. Then $p v_F(x) = e_F + v_F(x) = \frac{p e_F}{p-1}$, so Equation (9) tells us that

$$i = v_F(m-1) \geq \frac{p e_F}{p-1},$$

and therefore $i = \frac{p e_F}{p-1}$ and $v_F(x) \geq \frac{i}{p}$, as required.

Suppose instead that $v_F(x) < \frac{e_F}{p-1}$. Then $p v_F(x) < v_F(x) + e_F$, so Equation (9) tells us that

$$i = v_F(m-1) = p v_F(x),$$

and therefore $p \mid i$ and $v_F(x) \geq \frac{i}{p}$. Thus we have proved Statements (1) and (2).

Suppose that $p \mid i$ and $i < \frac{p e_F}{p-1}$. By Lemma 12.17, there is a $y \in \mathcal{O}_F$ with $y^p \equiv \frac{m-1}{\pi_F^i} \pmod{\mathfrak{p}_F}$. Let $x = \pi_F^{\frac{i}{p}} y$. Then we have

$$(1+x)^p \equiv 1 + x^p \equiv m \pmod{\mathfrak{p}_F^{i+1}},$$

so Statement (3) follows from Statement (2).

Suppose that $i = \frac{p e_F}{p-1}$. Statement (2) tells us that $m \in U_F^{(i+1)} F^{\times p}$ if and only if there is some $x \in \mathfrak{p}_F^{\frac{e_F}{p-1}}$ with

$$m - 1 \equiv px + x^p \pmod{\mathfrak{p}_F^{\frac{p e_F}{p-1}+1}},$$

and Statement (4) follows easily. □

We note the following algorithm as an immediate consequence of Lemma 12.18:

Algorithm 12.19.

Input: $\alpha \in \mathcal{O}_F^\times$.

Output: Returns a pair (i, λ). If $\alpha \in F^{\times p}$, then $i = \infty$ and $\lambda \in \mathcal{O}_F^\times$ is such that

$$\alpha \equiv \lambda^p \pmod{\mathfrak{p}_F^{\lfloor \frac{pe_F}{p-1} \rfloor + 1}}.$$

Otherwise, i is the largest integer with $\alpha \in U_F^{(i)} F^{\times p}$, and $\lambda \in \mathcal{O}_F^\times$ is an element such that $\alpha \equiv \lambda^p \pmod{\mathfrak{p}_F^i}$.

Algorithm:

(1) Set $m_0 = \alpha$ and $\lambda_0 = 1$.

(2) For $0 \le i \le \frac{pe_F}{p-1}$, do the following:

   If $p \nmid i$, then:
   - If $m_i \equiv 1 \pmod{\mathfrak{p}_F^{i+1}}$, then set $m_{i+1} = m_i$ and $\lambda_{i+1} = \lambda_i$.
   - Otherwise, return (i, λ_i) and break the for loop.

   If $p \mid i$ and $i < \frac{pe_F}{p-1}$, then:
   - Let $[y] \in \mathcal{O}_F/\mathfrak{p}_F$ be the unique element with $[y]^p = \left[\frac{m_i - 1}{\pi_F^i}\right]$, and set $\lambda_{i+1} = \lambda_i(1 + \pi_F^{i/p} y)$ and $m_{i+1} = \frac{m_i}{(1+\pi_F^{i/p} y)^p}$.

   If $i = \frac{pe_F}{p-1}$, then:
   - If $\left[\frac{m_i - 1}{\pi_F^{e_F/(p-1)} p}\right] \in \mathcal{O}_F/\mathfrak{p}_F$ is in the image of the map
   $$\mathcal{O}_F/\mathfrak{p}_F \to \mathcal{O}_F/\mathfrak{p}_F, \quad y \mapsto y + \frac{\pi_F^{e_F}}{p} y^p,$$
   then take y in the preimage and set $\lambda_{i+1} = \lambda_i(1 + \pi_F^{i/p} y)$ and $m_{i+1} = \frac{m_i}{(1+\pi_F^{i/p} y)^p}$.
   - Otherwise, return $(\frac{pe_F}{p-1}, \lambda_{\frac{pe_F}{p-1}})$.

   By Lemma 12.18, we see inductively that $m_i \equiv 1 \pmod{\mathfrak{p}_F^i}$ and $\alpha = \lambda_i^p m_i$ for all i that it is defined.

(3) If the for loop from the previous step finishes, then return $(\infty, \lambda_{\frac{pe_F}{p-1}+1})$.

Lemma 12.20. *Suppose that $(p-1) \mid e_F$. Define φ to be the map*

$$\varphi : \mathcal{O}_F/\mathfrak{p}_F \to \mathcal{O}_F/\mathfrak{p}_F, \quad y \mapsto y + \frac{\pi_F^{e_F}}{p} y^p.$$

We have

$$\#\operatorname{im}\varphi = \begin{cases} q/p & \text{if } \mu_p \subseteq F, \\ q & \text{if } \mu_p \not\subseteq F. \end{cases}$$

Proof. The map is $\mathbb{F}_p$-linear, and its kernel consists of the roots of the polynomial

$$X\left(X^{p-1} + \frac{\pi_F^{e_F}}{p}\right) \in \mathbb{F}_F[X].$$

Since $\mathbb{F}_F$ contains all $(p-1)^{\text{st}}$ roots of unity, the polynomial has either 1 or p roots. By Hensel's lemma, any root of $X^{p-1} + \frac{\pi_F^{e_F}}{p}$ in $\mathbb{F}_F$ lifts to a root in F, which exists if and only if $-p \in F^{\times(p-1)}$. The result [Was97, Lemma 14.6] states that $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$, and the result follows. □

Recall from Lemma 12.16 that we are interested in the groups $W_i = U_F^{(i)} F^{\times p} / U_F^{(i+1)} F^{\times p}$, for integers i with $0 \le i \le \lfloor \frac{pe_F}{p-1} \rfloor$.

Corollary 12.21. *Let i be an integer with $0 \leq i \leq \frac{pe_F}{p-1}$. We have group isomorphisms*

$$W_i \cong \begin{cases} \mathbb{F}_F & \textit{if } i < \frac{pe_F}{p-1} \textit{ and } p \nmid i, \\ \mathbb{F}_p & \textit{if } i = \frac{pe_F}{p-1} \textit{ and } \mu_p \subseteq F, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Suppose first that $p \nmid i$. Then Lemma 12.18(1) tells us that the natural sequence

$$1 \to U_F^{(i+1)} \to U_F^{(i)} \to W_i \to 1,$$

is exact, so $W_i \cong \mathbb{F}_F$. If $p \mid i$ and $i < \frac{pe_F}{p-1}$, then Lemma 12.18(3) tells us that $W_i = 0$. Finally, suppose that $i = \frac{pe_F}{p-1}$. Write φ for the map

$$\varphi : \mathcal{O}_F/\mathfrak{p}_F \to \mathcal{O}_F/\mathfrak{p}_F, \quad y \mapsto y + \frac{\pi_F^{e_F}}{p} y^p.$$

By Lemma 12.18(4), we have an exact sequence

$$1 \to \operatorname{im} \varphi \to U_F^{(i)}/U_F^{(i+1)} \to W_i \to 1,$$

where the map $\operatorname{im} \varphi \to U_F^{(i)}/U_F^{(i+1)}$ is given by $[x] \mapsto [1 + \pi_F^{\frac{e_F}{p-1}} px]$. The result then follows by Lemma 12.20. □

Corollary 12.22. *Let c be a nonnegative integer. If $0 \leq c \leq \lceil \frac{pe_F}{p-1} \rceil$, then we have*

$$\#\big(F^\times / U_F^{(c)} F^{\times p}\big) = pq^{c-1-\lfloor \frac{c-1}{p} \rfloor}.$$

If $c > \lceil \frac{pe_F}{p-1} \rceil$, then we have

$$\#\big(F^\times / U_F^{(c)} F^{\times p}\big) = \begin{cases} p^2 q^{e_F} & \textit{if } \mu_p \subseteq F, \\ pq^{e_F} & \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Lemma 12.16 and Corollary 12.21. □

Corollary 12.23. *Let $L \in \mathrm{\acute{E}t}_{p/F}^{C_p/F}$. Then we have $v_F(d_{L/F}) = (p-1)c$ for some integer c with $0 \leq c \leq \lfloor \frac{pe_F}{p-1} \rfloor + 1$.*

If $1 \leq c \leq \lceil \frac{pe_F}{p-1} \rceil$, then we have

$$\#\mathrm{\acute{E}t}_{p/F, \leq (p-1)c}^{C_p/F} = \frac{1}{p-1}\Big(pq^{c-1-\lfloor \frac{c-1}{p} \rfloor} - 1\Big).$$

If $(p-1) \mid e_F$, then we have

$$\#\mathrm{\acute{E}t}_{p/F, \leq pe_F + p - 1}^{C_p/F} = \begin{cases} \frac{1}{p-1}\Big(p^2 q^{e_F} - 1\Big) & \textit{if } \mu_p \subseteq F, \\ \frac{1}{p-1}\Big(pq^{e_F} - 1\Big) & \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Corollaries 12.13 and 12.22. □

Theorem 12.24. *If $\mathrm{\acute{E}t}_{(1^p)/F,m}^{C_p/F}$ is nonempty, then we have $m = (p-1)c$ for an integer c with $1 \leq c \leq \lfloor \frac{pe_F}{p-1} \rfloor + 1$, and*

$$\#\mathrm{\acute{E}t}_{(1^p)/F,m}^{C_p/F} = \begin{cases} \frac{p(q-1)}{p-1} \cdot q^{c-2-\lfloor \frac{c-2}{p} \rfloor} & \textit{if } c \not\equiv 1 \pmod{p}, \\ pq^{e_F} & \textit{if } c = \frac{pe_F}{p-1} + 1 \textit{ and } \mu_p \subseteq F, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Corollary 12.23. □

With p and q fixed implicitly, we define functions $A(t)$ and $B(t)$ as follows. For integers t with $t \geq 2$, define

$$A(t) = \begin{cases} q^{1-\lfloor \frac{t}{2} \rfloor} \cdot \frac{q^{\lfloor \frac{t}{2} \rfloor}-1}{q-1} & \text{if } p = 2, \\ q^{-p(p-2)} \cdot \frac{q^{(p-1)(p-2)}-1}{q^{p-2}-1} \cdot \frac{q^{-(p-1)^2 \cdot \lfloor \frac{t}{p} \rfloor}-1}{q^{-(p-1)^2}-1} & \text{if } p \neq 2, \end{cases}$$

and

$$B(t) = \begin{cases} 0 & \text{if } p = 2, \\ q^{-\lfloor \frac{t}{p} \rfloor} \cdot \frac{q^{-(p-2)(t+1)}-q^{-(p-2)(\lfloor \frac{t}{p} \rfloor p+2)}}{q^{-(p-2)}-1} & \text{if } p \neq 2. \end{cases}$$

For the reader's convenience, we will also state the definitions of $A(t)$ and $B(t)$ in Appendix B.

Lemma 12.25. *Let p be an integer with $p \geq 2$ and let q be a positive rational number. For any integer t with $t \geq 2$, we have*

$$\sum_{\substack{1 \leq c \leq t \\ c \not\equiv 1 \pmod{p}}} q^{-(p-2)c-\lfloor \frac{c-2}{p} \rfloor} = \mathbb{1}_{t \geq p} \cdot A(t) + \mathbb{1}_{t \not\equiv 0,1 \pmod{p}} \cdot B(t),$$

where $A(t)$ and $B(t)$ are the functions defined above.

Proof. The proof is a straightforward computation. To eliminate the possibility of a manipulation error, we have checked the identity numerically (see the Python notebook in the Github repository `https://github.com/Sebastian-Monnet/Sn-n-ics-paper-checks`). □

Corollary 12.26. *Recall the explicit functions $A(t)$ and $B(t)$ from Appendix B. We have*
$$\widetilde{m}\big(\text{Ét}^{C_p/F}_{(1^p)/F}\big) = \frac{q-1}{p-1} q^{-2} \Big(\mathbb{1}_{e_F \geq p-1} \cdot A\Big(\Big\lceil \frac{pe_F}{p-1} \Big\rceil \Big) + \mathbb{1}_{(p-1) \nmid e_F} \cdot B\Big(\Big\lceil \frac{pe_F}{p-1} \Big\rceil \Big) \Big) + \mathbb{1}_{\mu_p \subseteq F} \cdot q^{-(p-1)(e_F+1)}.$$

Proof. By Theorem 12.24, the mass $\widetilde{m}\big(\text{Ét}^{C_p/F}_{(1^p)/F}\big)$ is the sum of the following two quantities:

(1)
$$\frac{q-1}{p-1} \cdot q^{-2} \cdot \sum_{\substack{1 \leq c < \frac{pe_F}{p-1}+1 \\ c \not\equiv 1 \pmod{p}}} q^{-\left((p-2)c + \lfloor \frac{c-2}{p} \rfloor\right)}.$$

(2)
$$\mathbb{1}_{\mu_p \subseteq F} \cdot q^{-(p-1)(e_F+1)}.$$

For $c \in \mathbb{Z}$, we have $c < \frac{pe_F}{p-1} + 1$ if and only if $c \leq \lceil \frac{pe_F}{p-1} \rceil$. Setting $t = \lceil \frac{pe_F}{p-1} \rceil$, Lemma 12.25 tells us that

$$\sum_{\substack{1 \leq c < \frac{pe_F}{p-1}+1 \\ c \not\equiv 1 \pmod{p}}} q^{-\left((p-2)c + \lfloor \frac{c-2}{p} \rfloor\right)} = \mathbb{1}_{\lceil \frac{pe_F}{p-1} \rceil \geq p} \cdot A\Big(\Big\lceil \frac{pe_F}{p-1} \Big\rceil \Big) + \mathbb{1}_{\lceil \frac{pe_F}{p-1} \rceil \not\equiv 0,1 \pmod{p}} \cdot B\Big(\Big\lceil \frac{pe_F}{p-1} \Big\rceil \Big).$$

It is easy to see that $\lceil \frac{pe_F}{p-1} \rceil \geq p$ if and only if $e_F \geq p-1$. We claim that $\lceil \frac{pe_F}{p-1} \rceil \equiv 0, 1 \pmod{p}$ if and only if $(p-1) \mid e_F$. To see this, write $e_F = m(p-1) + r$ for integers m and r with $0 \leq r \leq p-2$. Then
$$\Big\lceil \frac{pe_F}{p-1} \Big\rceil = pm + \Big\lceil \frac{pr}{p-1} \Big\rceil.$$
If $(p-1) \mid e_F$, then $r = 0$, so $\lceil \frac{pe_F}{p-1} \rceil \equiv 0 \pmod{p}$. Otherwise, we have $r \geq 1$, so $1 < \frac{pr}{p-1} \leq p-1$, hence $\lceil \frac{pe_F}{p-1} \rceil \not\equiv 0, 1 \pmod{p}$. The result follows. □

Recall that, given nonnegative integers n and t with $n \geq 1$ and $t \geq 0$, we write

$$\overline{\mathcal{A}}^n = \mathcal{A}F^{\times n}/F^{\times n}$$

and

$$\overline{\mathcal{A}}^n_t = \overline{\mathcal{A}}^n \cap \Big(U_F^{(t)}F^{\times n}/F^{\times n}\Big).$$

Lemma 12.27. *Let c be an integer with $0 \leq c \leq \frac{pe_F}{p-1}+1$. We have*

$$\#\text{Ét}^{C_p/F,\mathcal{A}}_{p/F,\leq(p-1)c} = \frac{1}{p-1}\cdot\Big(\frac{\#\overline{\mathcal{A}}^p_c}{\#\overline{\mathcal{A}}^p}\cdot\#\big(F^\times/U_F^{(c)}F^{\times p}\big)-1\Big).$$

Proof. By Lemma 12.12, we need to count $\mathbb{F}_p$-linear transformations

$$\chi : F^\times/F^{\times p} \to \mathbb{F}_p$$

such that

$$\chi\big(\overline{\mathcal{A}}^p\big) = \chi\big(U_F^{(c)}F^{\times p}/F^{\times p}\big) = 0.$$

In other words, we need to compute the size of the annihilator

$$\Big(\overline{\mathcal{A}}^p + \Big(U_F^{(c)}F^{\times p}/F^{\times p}\Big)\Big)^\perp.$$

It is easy to see that

$$\dim_{\mathbb{F}_p}\Big(\big(\overline{\mathcal{A}}^p + (U_F^{(c)}F^{\times p}/F^{\times p})\big)^\perp\Big) = \dim_{\mathbb{F}_p}\Big(F^\times/U_F^{(c)}F^{\times p}\Big) - \dim_{\mathbb{F}_p}\big(\overline{\mathcal{A}}^p/\overline{\mathcal{A}}^p_c\big),$$

so

$$\#\Big(\overline{\mathcal{A}}^p + (U_F^{(c)}F^{\times p}/F^{\times p})\Big)^\perp = \frac{\#\overline{\mathcal{A}}^p_c}{\#\overline{\mathcal{A}}^p}\cdot\#\Big(F^\times/U_F^{(c)}F^{\times p}\Big).$$

The result then follows by Lemma 12.12. □

Corollary 12.28. *Let c be an integer with $0 \leq c \leq \frac{pe_F}{p-1}+1$. We have*

$$\#\text{Ét}^{C_p/F,\mathcal{A}}_{p/F,\leq(p-1)c} = \frac{1}{p-1}\cdot\Big(\frac{\#\overline{\mathcal{A}}^p_c}{\#\overline{\mathcal{A}}^p}\Big(1+(p-1)\#\text{Ét}^{C_p/F}_{p/F,\leq(p-1)c}\Big)-1\Big).$$

Proof. This is immediate from Corollary 12.13 and Lemma 12.27. □

Remark 12.29. Taking $p = 2$ in Corollary 12.28 yields the same result we proved earlier in Corollary 8.13.

Corollary 12.30. *Let c be an integer with $1 \leq c \leq \frac{pe_F}{p-1}+1$. We have*

$$\#\text{Ét}^{C_p/F,\mathcal{A}}_{p/F,(p-1)c} = \frac{\#\big(F^{\times p}/U_F^{(c-1)}F^{\times p}\big)}{(p-1)\#\overline{\mathcal{A}}^p}\cdot\Big(\#\overline{\mathcal{A}}^p_c\cdot\#W_{c-1} - \#\overline{\mathcal{A}}^p_{c-1}\Big)$$

Proof. This follows immediately from Lemma 12.27, together with the definition of the groups W_i. □

Corollary 12.31. *For $1 \leq c \leq \frac{pe_F}{p-1}+1$, we have*

$$\#\text{Ét}^{C_p/F,\mathcal{A}}_{p/F,(p-1)c} = \begin{cases} \frac{p}{(p-1)\#\overline{\mathcal{A}}^p}q^{c-2-\lfloor\frac{c-2}{p}\rfloor}\Big(q\cdot\#\overline{\mathcal{A}}^p_c - \#\overline{\mathcal{A}}^p_{c-1}\Big) & \textit{if } c \not\equiv 1 \pmod{p}, \\ \frac{pq^{e_F}}{\#\overline{\mathcal{A}}^p} \quad \textit{if } c = \frac{pe_F}{p-1}+1 \textit{ and } \mu_p \subseteq F \textit{ and } \overline{\mathcal{A}}^p_{\frac{pe_F}{p-1}} = 0, \\ 0 \quad \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Corollary 12.22, Theorem 12.24, and Lemma 12.27. □

Corollary 12.32. *The mass $\widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big)$ is given by*

$$\widetilde{m}\big(\text{Ét}^{C_p/F,\mathcal{A}}_{(1^p)/F}\big) = \mathbb{1}_{\mu_p\subseteq F}\cdot\mathbb{1}_{\overline{\mathcal{A}}^p_{\frac{pe_F}{p-1}}=0}\cdot\frac{q^{-(p-1)(e_F+1)}}{\#\overline{\mathcal{A}}^p}+\frac{1}{(p-1)\#\overline{\mathcal{A}}^p}\cdot q^{-2}\cdot\sum_{\substack{1\leq c\leq\lceil\frac{pe_F}{p-1}\rceil\\ c\not\equiv 1 \pmod p}}\frac{q\#\overline{\mathcal{A}}^p_c-\#\overline{\mathcal{A}}^p_{c-1}}{q^{(p-2)c+\lfloor\frac{c-2}{p}\rfloor}}.$$

Proof. This is immediate from Theorem 12.24 and Corollary 12.31. □

Proof of Theorem 10.8. We prove the statements one by one.

(1) This is immediate from Corollary 12.2 and Lemma 12.3.
(2) This is precisely Lemma 12.4.
(3) This is precisely Corollary 12.8.
(4) Serre's mass formula [Ser78, Theorem 2] tells us that

$$\widetilde{m}\big(\text{Ét}_{(1^p)/F}\big)=\frac{1}{q^{p-1}},$$

and the first part of the statement follows from Lemma 12.9. The rest of the theorem is given by Corollaries 12.26 and 12.32.

□

Definition 12.33. Let $\alpha\in F^\times$. We define $c_\alpha\in\mathbb{Z}\cup\{\infty\}$ as follows:

- If $\alpha\in F^{\times p}$, then $c_\alpha=\infty$.
- Otherwise, adopting the convention that $U_F^{(-1)}=F^\times$, we define c_α to be the largest integer c such that $\alpha\in U_F^{(c)}F^{\times p}$.

Remark 12.34. We can compute c_α using Algorithm 12.19. We will state the time complexity of this computation in Lemma 13.35.

Lemma 12.35. *Let $\alpha\in F^\times\setminus F^{\times p}$. Then we have $-1\leq c_\alpha\leq\lfloor\frac{pe_F}{p-1}\rfloor$. Moreover, if $c_\alpha<\frac{pe_F}{p-1}$ then $p\nmid c_\alpha$, and if $c_\alpha=\frac{pe_F}{p-1}$ then $\mu_p\subseteq F$.*

Proof. This follows from Corollaries 12.15 and 12.21. □

Lemma 12.36. *Let $\alpha\in F^\times$ and let c be an integer with $1\leq c\leq\frac{pe_F}{p-1}+1$. Then we have*

(1) If $c\leq c_\alpha$, then we have

$$\#\text{Ét}^{C_p/F,\alpha}_{p/F,(p-1)c}=\begin{cases}\frac{p(q-1)}{p-1}\cdot q^{c-2-\lfloor\frac{c-2}{p}\rfloor} & \textit{if } c\not\equiv 1 \pmod p,\\ pq^{e_F} & \textit{if } c=\frac{pe_F}{p-1}+1 \textit{ and } \mu_p\subseteq F,\\ 0 & \textit{otherwise.}\end{cases}$$

(2) If $1\leq c_\alpha<\frac{pe_F}{p-1}$, then

$$\#\text{Ét}^{C_p/F,\alpha}_{p/F,(p-1)(c_\alpha+1)}=\frac{q-p}{p-1}\cdot q^{c_\alpha-1-\lfloor\frac{c_\alpha}{p}\rfloor}.$$

(3) If $c_\alpha=\frac{pe_F}{p-1}$, then

$$\#\text{Ét}^{C_p/F,\alpha}_{p/F,(p-1)(c_\alpha+1)}=0.$$

(4) If $c_\alpha + 2 \leq c \leq \frac{pe_F}{p-1} + 1$, then

$$\#\text{Ét}_{p/F,(p-1)c}^{C_p/F,\alpha} = \begin{cases} \frac{q-1}{p-1} q^{c-2-\lfloor \frac{c-2}{p} \rfloor} & \textit{if } c \not\equiv 1 \pmod{p}, \\ q^{e_F} \quad \textit{if } c = \frac{pe_F}{p-1} + 1 \textit{ and } \mu_p \subseteq F, \\ 0 \quad \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Corollary 12.21, Corollary 12.22, Corollary 12.30, and Lemma 12.35. □

Theorem 12.37. *Let $\alpha \in F^\times \setminus F^{\times p}$. If $p \nmid v_F(\alpha)$, then*

$$\widetilde{m}\big(\text{Ét}_{(1^p)/F}^{C_p/F,\alpha}\big) = \frac{1}{p} \cdot \widetilde{m}\big(\text{Ét}_{(1^p)/F}^{C_p/F}\big).$$

If $p \mid v_F(\alpha)$, then $\widetilde{m}\big(\text{Ét}_{(1^p)/F}^{C_p/F,\alpha}\big)$ is the sum of the following seven quantities:

(1)

$$\mathbb{1}_{c_\alpha \geq p} \cdot \frac{q-1}{p-1} \cdot q^{-2} \cdot A(c_\alpha).$$

(2)

$$\mathbb{1}_{c_\alpha \not\equiv 0,1 \pmod{p}} \cdot \frac{q-1}{p-1} \cdot q^{-2} \cdot B(c_\alpha).$$

(3)

$$\mathbb{1}_{c_\alpha < \frac{pe_F}{p-1}} \cdot \frac{q-p}{p-1} \cdot \frac{1}{p} \cdot q^{-2-(p-2)(c_\alpha+1)-\lfloor \frac{c_\alpha}{p} \rfloor}.$$

(4)

$$\mathbb{1}_{c_\alpha < \frac{pe_F}{p-1} - 1} \cdot \frac{q-1}{pq^2(p-1)} \cdot \Big(\mathbb{1}_{e_F \geq p-1} \cdot A\Big(\Big\lceil \frac{pe_F}{p-1} \Big\rceil\Big) - \mathbb{1}_{c_\alpha \geq p-1} \cdot A(c_\alpha + 1)\Big).$$

(5)

$$\mathbb{1}_{c_\alpha < \frac{pe_F}{p-1} - 1} \cdot \mathbb{1}_{(p-1) \nmid e_F} \cdot \frac{q-1}{pq^2(p-1)} \cdot B\Big(\Big\lceil \frac{pe_F}{p-1} \Big\rceil\Big).$$

(6)

$$-\mathbb{1}_{c_\alpha < \frac{pe_F}{p-1} - 1} \cdot \mathbb{1}_{c_\alpha \not\equiv -1,0 \pmod{p}} \cdot \frac{q-1}{pq^2(p-1)} \cdot B(c_\alpha + 1).$$

(7)

$$\mathbb{1}_{c_\alpha < \frac{pe_F}{p-1}} \cdot \mathbb{1}_{\mu_p \subseteq F} \cdot \frac{1}{p} \cdot q^{-(p-1)(e_F+1)}.$$

Proof. If $p \nmid v_F(\alpha)$, then the result follows from Corollary 12.28, so we will assume that $p \mid v_F(\alpha)$. Lemma 12.35 tells us that $c_\alpha \geq 1$. By Lemma 12.36, the pre-mass is the sum of the following four quantities:

(1)

$$\frac{q-1}{p-1} \cdot q^{-2} \cdot \sum_{\substack{1 \leq c \leq c_\alpha \\ c \not\equiv 1 \pmod{p}}} q^{-(p-2)c-\lfloor \frac{c-2}{p} \rfloor}.$$

(2)

$$\mathbb{1}_{c_\alpha < \frac{pe_F}{p-1}} \cdot \frac{q-p}{p-1} \cdot \frac{1}{p} \cdot q^{-2-(p-2)(c_\alpha+1)-\lfloor \frac{c_\alpha}{p} \rfloor}.$$

(3)
$$\frac{q-1}{p-1}\cdot\frac{1}{p}\cdot q^{-2}\cdot \sum_{\substack{c_\alpha+2\le c<\frac{pe_F}{p-1}+1 \\ c\not\equiv 1 \pmod p}} q^{-(p-2)c-\lfloor\frac{c-2}{p}\rfloor}.$$

(4)
$$\mathbb{1}_{(p-1)\mid e_F}\cdot \mathbb{1}_{c_\alpha<\frac{pe_F}{p-1}}\cdot \mathbb{1}_{\mu_p\subseteq F}\cdot\frac{1}{p}\cdot q^{-(p-1)(e_F+1)}.$$

By Lemma 12.25, the first three quantities rearrange to:

(1)
$$\frac{q-1}{p-1}\cdot q^{-2}\cdot(\mathbb{1}_{c_\alpha\ge p}\cdot A(c_\alpha)+\mathbb{1}_{c_\alpha\not\equiv 0,1 \pmod p}B(c_\alpha)).$$

(2)
$$\mathbb{1}_{c_\alpha<\frac{pe_F}{p-1}}\cdot\frac{q-p}{p-1}\cdot\frac{1}{p}\cdot q^{-2-(p-2)(c_\alpha+1)-\lfloor\frac{c_\alpha}{p}\rfloor}.$$

(3)
$$\mathbb{1}_{c_\alpha<\frac{pe_F}{p-1}-1}\cdot\frac{q-1}{p-1}\cdot\frac{1}{p}\cdot q^{-2}\cdot\Big(\mathbb{1}_{e_F\ge p-1}\cdot A\Big(\Big\lceil\frac{pe_F}{p-1}\Big\rceil\Big)-\mathbb{1}_{c_\alpha\ge p-1}A(c_\alpha+1)$$
$$+\mathbb{1}_{\lceil\frac{pe_F}{p-1}\rceil\not\equiv 0,1 \pmod p}B\Big(\Big\lceil\frac{pe_F}{p-1}\Big\rceil\Big)-\mathbb{1}_{c_\alpha\not\equiv -1,0 \pmod p}B(c_\alpha+1)\Big).$$

We saw in the proof of Corollary 12.26 that $\lceil\frac{pe_F}{p-1}\rceil\equiv 0,1 \pmod p$ if and only if $(p-1)\mid e_F$, so
$$\mathbb{1}_{\lceil\frac{pe_F}{p-1}\rceil\not\equiv 0,1 \pmod p}=\mathbb{1}_{(p-1)\nmid e_F}.$$
Since the extension $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally ramified[1] of degree $p-1$, we have
$$\mathbb{1}_{(p-1)\mid e_F}\cdot\mathbb{1}_{\mu_p\subseteq F}=\mathbb{1}_{\mu_p\subseteq F},$$
and the result follows. □

13. S_4-quartic extensions

The goal of Section 13 is to prove Theorems 10.9, 10.10, 10.11, and 10.12, which concern the pre-mass $\widetilde{m}(\text{Ét}^{\mathcal{A}}_{4/F})$, for p-adic fields F. Throughout the section, let p be a rational prime, let F be a p-adic field, and let $\mathcal{A}\subseteq F^\times$ be a finitely generated subgroup. With F fixed, write q for the size $\#\mathbb{F}_F$ of the residue field of F.

13.1. Tamely ramified parts.

The goal of this subsection is to prove Theorem 10.9.

Lemma 13.1. *We have*
$$\text{Split}_4^{\text{epi}}=\{(13),(1^22),(112),(1^211),(1^31),(1111)\}$$
and
$$\text{Split}_4=\{(4),(22),(1^21^2),(2^2),(1^4)\}\cup\text{Split}_4^{\text{epi}}.$$

Proof. The eleven possible splitting symbols are listed on [Bha04, Page 1353], and it is clear that the epimorphic ones are as stated. □

[1] Since the polynomial $x^{p-1}+\ldots+x+1$ becomes Eisenstein after the substitution $x\mapsto x+1$.

Lemma 13.2. *For all p, we have*

$$\widetilde{m}\big(\text{Ét}^{\text{epi}}_{4/F}\big) = \frac{5q^2+8q+8}{8q^2}.$$

Proof. This follows from Theorem 3.9(2), and Lemma 13.1. □

Lemma 13.3. *For all p, we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(4)/F}\big) = \begin{cases} \frac{1}{4} & \text{if } 4 \mid v_F(\alpha) \text{ for all } \alpha \in \mathcal{A}, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(22)/F}\big) = \begin{cases} \frac{1}{8} & \text{if } 2 \mid v_F(\alpha) \text{ for all } \alpha \in \mathcal{A}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This follows easily from Lemma 11.5. □

Lemma 13.4. *Suppose that p is odd. Let (A_0, A_1) be a stratified generating set for $\overline{\mathcal{A}}^2$. Then we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^21^2)/F}\big) = \begin{cases} \frac{1}{2q^2} & \text{if } \mathcal{A} \subseteq F^{\times 2}, \\ \frac{3}{8q^2} & \text{if } A_0 = \varnothing \text{ and } \#A_1 = 1, \\ \frac{1}{4q^2} & \text{otherwise.} \end{cases}$$

Proof. By Lemma 12.5, we have

$$\text{Ét}_{(1^21^2)/F} = \{L_0 \times L_0, L_0 \times L_1, L_1 \times L_1\},$$

where

$$L_j = F\Big(\sqrt{\zeta_{q-1}^j \pi_F}\Big), \quad j = 0, 1.$$

Lemma 3.11 tells us that $v_F(d_{L_j/F}) = 1$ for each j. It follows that, for $i, j \in \{0,1\}$, we have

$$\widetilde{m}\big(\{L_i \times L_j\}\big) = \begin{cases} \frac{1}{8q^2} & \text{if } i = j, \\ \frac{1}{4q^2} & \text{if } i \neq j. \end{cases}$$

The result then follows from the fact that

$$N_{L_j/F} L_j^\times = \langle \mathcal{O}_F^{\times 2}, -\zeta_{q-1}^j \pi_F \rangle.$$

□

Lemma 13.5. *Suppose that p is odd. Let (A_0, A_1, A_2) be a stratified generating set for $\overline{\mathcal{A}}^4$. Then we have*

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(2^2)/F}\big) = \begin{cases} \frac{1}{2q^2} & \text{if } A_0 \subseteq F^{\times 2} \text{ and } A_1 = A_2 = \varnothing, \\ \frac{1}{4q^2} & \text{else if } A_0 \subseteq F^{\times 2} \text{ and } A_1 = \varnothing \text{ and } \frac{\alpha_i}{\alpha_j} \in F^{\times 2} \text{ for all } \alpha_i, \alpha_j \in A_2, \\ 0 & \text{otherwise.} \end{cases}$$

If $q \equiv 1 \pmod 4$, then we have

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^4)/F}\big) = \begin{cases} \frac{1}{q^3} & \text{if } \mathcal{A} \subseteq F^{\times 4}, \\ \frac{1}{2q^3} & \text{if } A_0 = A_1 = \varnothing \text{ and } \#A_2 = 1 \text{ and } A_2 \subseteq F^{\times 2}, \\ \frac{1}{4q^3} & \text{if } A_0 = A_2 = \varnothing \text{ and } \#A_1 = 1, \\ 0 & \text{otherwise.} \end{cases}$$

If $q \equiv 3 \pmod 4$, then we have

$$\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(1^4)/F}\big) = \begin{cases} \frac{1}{q^3} & \textit{if } \mathcal{A} \subseteq F^{\times 2}, \\ \frac{1}{2q^3} & \textit{else if } A_0 = A_2 = \varnothing \textit{ and } \# A_1 = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let E/F be the quadratic unramified extension. Lemma 12.5 tells us that

$$\text{Ét}_{(1^2)/E} = \{L_0, L_1\},$$

where

$$L_j = E\Big(\sqrt{\zeta_{q^2-1}^j \pi_F}\Big),$$

for each j. On the other hand, we have two index 4 subgroups

$$\langle \mathcal{O}_F^{\times 2}, \pi_F^2 \rangle, \quad \langle \mathcal{O}_F^{\times 2}, \zeta_{q-1}\pi_F^2 \rangle$$

of $F^\times$. Clearly the quartic abelian extensions corresponding to these subgroups have splitting symbol (2^2), so they must be equal to L_0 and L_1 in some order, which implies that L_0 and L_1 are nonisomorphic abelian extensions of F. Lemma 3.11 tells us that $v_F(d_{L_j/F}) = 2$ for each j, so $\widetilde{m}(\{L_j\}) = \frac{1}{4q^2}$, and the formula for $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{(2^2)/F}\big)$ follows.

Lemma 12.5 tells us that

$$\text{Ét}_{(1^4)/F} = \begin{cases} \{L_0, L_1, L_2, L_3\} & \text{if } q \equiv 1 \pmod 4, \\ \{L_0, L_1\} & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

where

$$L_j = F\Big(\sqrt[4]{\zeta_{q-1}^j \pi_F}\Big).$$

Suppose first that $q \equiv 1 \pmod 4$. Then the minimal polynomial of $\sqrt[4]{\pi_F}$ over F splits in L_0, so L_0/F is Galois. Since π_F is an arbitrary choice of uniformiser, it follows that L_j/F is Galois for each j, and therefore

$$N_{L_j/F} L_j^\times = \langle \mathcal{O}_F^{\times 4}, -\zeta_{q-1}^j \pi_F \rangle.$$

Lemma 3.11 tells us that $\widetilde{m}(\{L_j\}) = \frac{1}{4q^3}$ for each j, and the result follows. Finally, suppose that $q \equiv 3 \pmod 4$. Then $\mu_4 \not\subseteq F$, so $\sqrt[4]{\pi_F}$ has only two conjugates in L_0, and therefore L_0 is non-Galois with a maximal abelian subextension $F(\sqrt{\pi_F})$, so

$$N_{L_0/F} L_0^\times = \langle \mathcal{O}_F^{\times 2}, -\pi_F \rangle,$$

and similarly L_1/F is non-Galois with

$$N_{L_1/F} L_1^\times = \langle \mathcal{O}_F^{\times 2}, -\zeta_{q-1}\pi_F \rangle.$$

By Lemma 3.11, we have $v_F(d_{L_j/F}) = 3$ for each j, and the result follows. □

Proof of Theorem 10.9. This is immediate from Lemmas 13.1 to 13.5 inclusive. □

13.2. **2-adic fields.** In this subsection, we specialise to the case $p = 2$, so that F is a 2-adic field. Recall that, for an integer m, the decorators $\text{Ét}^{\bullet}_{\bullet/F,m}$ and $\text{Ét}^{\bullet}_{\bullet/F,\leq m}$ denote the sets of $L \in \text{Ét}^{\bullet}_{\bullet/F}$ with $v_F(d_{L/F}) = m$ and $v_F(d_{L/F}) \leq m$, respectively. By Theorem 10.9, in order to compute $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{4/F}\big)$, all we need is to compute $\widetilde{m}\big(\text{Ét}^{\mathcal{A}}_{\sigma/F}\big)$ for each $\sigma \in \{(1^2 1^2), (2^2), (1^4)\}$. The goal of Section 13.2 is to address the first two of these cases, by proving Theorems 10.10 and 10.11.

Lemma 13.6. *We have*

$$\mathrm{\acute{E}t}^{\mathcal{A}}_{(1^21^2)/F} = \big\{L_1 \times L_2 \in \mathrm{\acute{E}t}_{(1^21^2)/F} : L_1 \not\cong L_2\big\} \cup \big\{L_1 \times L_1 : L_1 \in \mathrm{\acute{E}t}^{\mathcal{A}}_{(1^2)/F}\big\}.$$

Proof. It is clear that the left-hand side is contained inside the right-hand side, and also that

$$\{L_1 \times L_1 : L_1 \in \mathrm{\acute{E}t}^{\mathcal{A}}_{(1^2)/F}\} \subseteq \mathrm{\acute{E}t}^{\mathcal{A}}_{(1^21^2)/F}.$$

Finally, for distinct elements $L_1, L_2 \in \mathrm{\acute{E}t}_{(1^2)/F}$, the norm groups $N_{L_i/F}L_i^\times$ are distinct index 2 subgroups of $F^\times$, and therefore $\mathrm{Nm}(L_1 \times L_2) = F^\times$, so $L_1 \times L_2 \in \mathrm{\acute{E}t}^{\mathcal{A}}_{(1^21^2)/F}$. □

Lemma 13.7. *Let m be an integer. We have*

$$\#\{L_1 \times L_2 \in \mathrm{\acute{E}t}_{(1^21^2)/F,m} : L_1 \not\cong L_2\} = N^{\neq}_{(1^21^2)}(m),$$

where $N^{\neq}_{(1^21^2)}(m)$ is the explicit function defined in Appendix B.

Proof. Theorem 12.24 tells us that, for all m_1, we have

$$\#\mathrm{\acute{E}t}_{(1^2)/F,m_1} = \begin{cases} 2(q-1)q^{\frac{m_1}{2}-1} & \text{if } m_1 \text{ is even with } 2 \le m_1 \le 2e_F, \\ 2q^{e_F} & \text{if } m_1 = 2e_F + 1, \\ 0 & \text{otherwise.} \end{cases}$$

We will use this fact without reference for the rest of this proof. For any m, the number we are looking for is equal to

$$\frac{1}{2} \cdot \Big(\sum_{m_1+m_2=m} \Big(\#\mathrm{\acute{E}t}_{(1^2)/F,m_1} \cdot \#\mathrm{\acute{E}t}_{(1^2)/F,m_2}\Big) - \#\mathrm{\acute{E}t}_{(1^2)/F,m/2}\Big). \tag{10}$$

It is easy to see that this is 0 unless one of the following is true:

- $4 \le m \le 4e_F$ and m is even.
- $2e_F + 3 \le m \le 4e_F + 1$ and m is odd.
- $m = 4e_F + 2$.

The result follows by considering these cases separately. □

Proof of Theorem 10.10. This is immediate from Lemmas 13.6 and 13.7. □

Lemma 13.8. *For each nonnegative integer m, we have*

$$\#\mathrm{\acute{E}t}^{V_4/F,\mathcal{A}}_{(2^2)/F,m} = \begin{cases} \frac{1}{2} \cdot \#\mathrm{\acute{E}t}^{\mathcal{A}}_{(1^2)/F,m/2} & \text{if } 2 \mid v_F(\alpha) \text{ for all } \alpha \in \mathcal{A}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Write E_{ur} for the unramified quadratic extension of F. Let $L \in \mathrm{\acute{E}t}^{V_4/F}_{(2^2)/F,m}$. It follows from Lemma 6.19 that there are exactly two elements $E \in \mathrm{\acute{E}t}_{(1^2)/F,m/2}$ with $L = E_{\mathrm{ur}}E$. For such E, we have

$$\mathrm{Nm}\, L = \mathrm{Nm}\, E_{ur} \cap \mathrm{Nm}\, E = \{x \in \mathrm{Nm}\, E : 2 \mid v_F(x)\}.$$

Therefore, if there is some $\alpha \in \mathcal{A}$ with $2 \nmid v_F(\alpha)$, then $\mathrm{\acute{E}t}^{V_4/F,\mathcal{A}}_{(2^2)/F} = \varnothing$. On the other hand, if $2 \mid v_F(\alpha)$ for all $\alpha \in \mathcal{A}$, then we have a 2-to-1 surjection

$$\mathrm{\acute{E}t}^{\mathcal{A}}_{(1^2)/F,m/2} \to \mathrm{\acute{E}t}^{V_4/F,\mathcal{A}}_{(2^2)/F,m}, \quad E \mapsto E_{\mathrm{ur}}E,$$

and the result follows. □

Lemma 13.9. *We have*

$$\text{Ét}_{(2^2)/F}^{D_4/F,\mathcal{A}} = \begin{cases} \text{Ét}_{(2^2)/F}^{D_4/F} & \text{if } 2 \mid v_F(\alpha) \text{ for all } \alpha \in \mathcal{A}, \\ \varnothing & \text{otherwise.} \end{cases}$$

Proof. Let E/F be the unramified quadratic extension. By class field theory, every element $L \in \text{Ét}_{(2^2)/F}^{D_4/F}$ has $N_{L/F}L^\times = N_{E/F}E^\times$, and the result follows. □

Lemma 13.10. *Let E/F be the unique unramified quadratic extension. For each nonnegative integer m, we have*

$$\#\text{Ét}_{(2^2)/F,m}^{D_4/F} = \frac{1}{2} \cdot \left(\#\text{Ét}_{(1^2)/E,m/2} - \#\text{Ét}_{(1^2)/E,m/2}^{C_4/F} - \#\text{Ét}_{(1^2)/E,m/2}^{V_4/F}\right).$$

Proof. Using the tower law for discriminant, it is easy to see that there is a well-defined surjection

$$\text{Ét}_{(1^2)/E,\frac{m}{2}} \setminus \left(\text{Ét}_{(1^2)/E,\frac{m}{2}}^{C_4/F} \cup \text{Ét}_{(1^2)/E,\frac{m}{2}}^{V_4/F}\right) \to \text{Ét}_{(2^2)/F,m}^{D_4/F}.$$

Moreover, Lemma 9.1(2) tells us that this surjection is 2-to-1. □

Lemma 13.11. *Let E/F be the unique unramified quadratic extension. For each nonnegative integer m, we have*

$$\#\text{Ét}_{(1^2)/E,m}^{C_4/F} = \frac{1}{2} \cdot \#\text{Ét}_{(1^2)/F,m}.$$

Proof. If $\text{Ext}_{2/E,m}^{C_4/F} \neq \varnothing$, then either m is even with $0 \leq m \leq 2e_F$, or $m = 2e_F + 1$. Suppose that m is an even integer with $0 \leq m \leq 2e_F$. Let $\omega \in E^\times$ be such that $E(\sqrt{\omega})/E$ is unramified, hence a C_4-extension of F. By Lemma 8.19, we have

$$U_E^{(2e_E-m)}E^{\times 2} \cap F^\times = U_F^{(2e_F-m)}F^{\times 2},$$

so Lemma 8.18 gives a 2-to-1 surjection

$$U_F^{(2e_F-m)}F^{\times 2}/F^{\times 2} \to \text{Ext}_{2/E,\leq m}^{C_4/F}, \quad t \mapsto E(\sqrt{\omega t}).$$

But Lemma 8.5 and Corollary 8.6 tell us that, for $u \in F^\times/F^{\times 2}$, we have

$$v_F(d_{F(\sqrt{u})/F}) \leq m \iff u \in U_F^{(2e_F-m)}F^{\times 2}/F^{\times 2},$$

and therefore

$$\#\text{Ext}_{2/F,\leq m} = \#(U_F^{(2e_F-m)}F^{\times 2}/F^{\times 2}) - 1,$$

so

$$\#\text{Ext}_{2/E,\leq m}^{C_4/F} = \frac{1}{2}\#\text{Ext}_{2/F,\leq m} + \frac{1}{2},$$

and the result follows for $2 \leq m \leq 2e_F$. By Lemmas 8.18 and 8.5, there is a 2-to-1 surjection

$$\{[x] \in F^\times/F^{\times 2} : v_F(x) = 1\} \to \text{Ét}_{(1^2)/E,2e_F+1}^{C_4/F}, \quad x \mapsto E(\sqrt{\omega x}),$$

and a bijection

$$\{[x] \in F^\times/F^{\times 2} : v_F(x) = 1\} \to \text{Ét}_{(1^2)/F,2e_F+1}, \quad x \mapsto F(\sqrt{x}),$$

and the result for $m = 2e_F + 1$ follows. □

Lemma 13.12. *Let E/F be the unique unramified quadratic extension. For each nonnegative integer m, we have*

$$\#\text{Ét}_{(1^2)/E,m}^{V_4/F} = \frac{1}{2} \cdot \#\text{Ét}_{(1^2)/F,m}.$$

Proof. This follows easily from Lemma 9.1 and Lemma 13.8. □

Lemma 13.13. *If $\text{Ét}^{D_4/F,\mathcal{A}}_{(2^2)/F,m}$ is nonempty, then either m is a multiple of 4 with $4 \leq m \leq 4e_F$, or $m = 4e_F + 2$. If m is a multiple of 4 with $4 \leq m \leq 4e_F$, then*

$$\#\text{Ét}^{D_4/F,\mathcal{A}}_{(2^2)/F,m} = \begin{cases} (q-1)\Big((q+1)q^{\frac{m}{2}-2} - q^{\frac{m}{4}-1}\Big) & \textit{if } 2 \mid v_F(\alpha) \textit{ for all } \alpha \in \mathcal{A}, \\ 0 \quad \textit{otherwise.} \end{cases}$$

If $m = 4e_F + 2$, then

$$\#\text{Ét}^{D_4/F,\mathcal{A}}_{(2^2)/F,m} = \begin{cases} q^{e_F}(q^{e_F}-1) & \textit{if } 2 \mid v_F(\alpha) \textit{ for all } \alpha \in \mathcal{A}, \\ 0 \quad \textit{otherwise.} \end{cases}$$

Proof. This follows easily from Theorem 12.24 and Lemmas 13.9, 13.10, 13.11, and 13.12. □

Lemma 13.14. *If $2 \mid v_F(\alpha)$ for all $\alpha \in \mathcal{A}$, then*

$$\widetilde{m}\big(\text{Ét}^{D_4/F,\mathcal{A}}_{(2^2)/F}\big) = \frac{1}{2} \cdot \Big(q^{-2} - q^{-2e_F-2} - \frac{1}{q^2+q+1}\big(q^{-1} - q^{-3e_F-1}\big) + q^{-3e_F-2}\big(q^{e_F}-1\big)\Big).$$

Proof. This follows easily from Lemma 13.13. To eliminate the possibility of a manipulation error, we have checked the required summation numerically in the Python notebook in the Github repository `https://github.com/Sebastian-Monnet/Sn-n-ics-paper-checks`. □

Lemma 13.15. *Let $M/L/K$ be a tower of quadratic extensions of p-adic fields. Suppose that M/K is Galois and let $\beta \in L^\times$. Let $\alpha = N_{L/K}\beta$. Then*

$$\alpha \in N_{M/K}M^\times \iff \beta \in N_{M/L}M^\times.$$

Proof. The ($\Leftarrow$) direction is obvious. For ($\Rightarrow$), suppose that $\alpha \in N_{M/K}M^\times$. Then $\alpha = N_{L/K}\theta$ for some $\theta \in N_{M/L}M^\times$. Since $N_{L/K}(\theta/\beta) = 1$, Hilbert's theorem 90 tells us that $\theta = \beta\frac{x}{\bar{x}}$ for some $x \in L^\times$. Writing $M = L(\sqrt{d})$ for $d \in L^\times$, we have

$$\begin{aligned}(\beta, d)_L &= (d, \theta)_L(d, x)_L(d, \bar{x})_L \\ &= (d, x)_L(\bar{d}, x)_L \\ &= 1,\end{aligned}$$

where the final equality comes from the fact that M/K is Galois, so $L(\sqrt{d}) = L(\sqrt{\bar{d}}) = M$. □

Next, we want to understand the sets $\text{Ét}^{C_4/F,\mathcal{A}}_{(2^2)/F,m}$, for positive integers m. Recall from Section 10 that, given a C_4-extendable extension E/F, we defined a certain subset $N_E^{\mathcal{A}}$ of $F^\times/F^{\times 2}$. We would suggest rereading this definition, which is just before the statement of Theorem 10.11, before tackling the next lemma.

Lemma 13.16. *Let $E \in \text{Ext}^{\mathcal{A}}_{2/F}$ be C_4-extendable, and let m_2 be an integer such that $\text{Ext}^{C_4/F}_{2/E,\leq m_2}$ is nonempty. If $m_2 \leq 2e_E$, then we have*

$$\#\text{Ext}^{C_4/F,\mathcal{A}}_{2/E,\leq m_2} = \frac{1}{2} \cdot \#\Bigg(\Big(U_E^{(2e_E - 2\lfloor\frac{m_2}{2}\rfloor)}E^{\times 2} \cap F^\times\Big)/F^{\times 2} \cap N_E^{\mathcal{A}}\Bigg).$$

If $m_2 \geq 2e_E + 1$, then we have

$$\#\text{Ext}^{C_4/F,\mathcal{A}}_{2/E,\leq m_2} = \frac{1}{2} \cdot \#N_E^{\mathcal{A}}.$$

Proof. Let $\omega \in E^\times$ be the element we fixed in the definition of $N_E^{\mathcal{A}}$. If $m_2 \leq 2e_E$, then Lemma 8.18 gives us a 2-to-1 surjection

$$\left(U_E^{(2e_E - 2\lfloor \frac{m_2}{2} \rfloor)} E^{\times 2} \cap F^\times\right)/F^{\times 2} \to \operatorname{Ext}_{2/E,\leq m_2}^{C_4/F}, \quad t \mapsto E(\sqrt{\omega t}).$$

If $m_2 \geq 2e_E + 1$, then Lemma 8.18 gives a 2-to-1 surjection

$$F^\times/F^{\times 2} \to \operatorname{Ext}_{2/E,\leq m_2}^{C_4/F}, \quad t \mapsto E(\sqrt{\omega t}).$$

Let $t \in F^\times$ and let $L = E(\sqrt{\omega t})$. Let $\alpha \in \mathcal{A}$, and let $\widetilde{\alpha} \in E^\times$ be such that $N_{E/F}\widetilde{\alpha} = \alpha$. Lemma 13.15 tells us that $\alpha \in N_{L/F}L^\times$ if and only if $\widetilde{\alpha} \in N_{L/E}L^\times$. By Lemma 13.15 and properties of quadratic Hilbert symbols, we have

$$\begin{aligned}
\widetilde{\alpha} \in N_{L/E}L^\times &\iff (\widetilde{\alpha}, \omega t)_E = 1 \\
&\iff (\widetilde{\alpha}, t)_E = (\widetilde{\alpha}, \omega)_E \\
&\iff (\alpha, t)_F = \begin{cases} 1 & \text{if } \alpha \in N_{E(\sqrt{\omega})/F}E(\sqrt{\omega})^\times, \\ -1 & \text{otherwise.} \end{cases} \\
&\iff \begin{cases} t \in N_\alpha & \text{if } \alpha \in N_\omega, \\ t \notin N_\alpha & \text{otherwise.} \end{cases}
\end{aligned}$$

It follows that $\mathcal{A} \subseteq N_{L/F}L^\times$ if and only if $t \in N_E^{\mathcal{A}}$, and the result follows. □

Lemma 13.17. *Let E be the unramified quadratic extension of F, and let m be a nonnegative integer. If $m \leq 4e_F + 1$, then*

$$\#\text{Ét}_{(2^2)/F,\leq m}^{C_4/F,\mathcal{A}} = \begin{cases} \frac{1}{2} \cdot \#N_{E,2e_F - 2\lfloor \frac{m}{4} \rfloor}^{\mathcal{A}} - 1 & \textit{if } v_F(\alpha) \equiv 0 \pmod 4 \textit{ for all } \alpha \in \mathcal{A}, \\ \frac{1}{2} \cdot \#N_{E,2e_F - 2\lfloor \frac{m}{4} \rfloor}^{\mathcal{A}} & \textit{else if } 2 \mid v_F(\alpha) \textit{ for all } \alpha \in \mathcal{A}, \\ 0 & \textit{otherwise.} \end{cases}$$

If $m \geq 4e_F + 2$, then

$$\#\text{Ét}_{(2^2)/F,\leq m}^{C_4/F,\mathcal{A}} = \begin{cases} \frac{1}{2} \cdot \#N_E^{\mathcal{A}} - 1 & \textit{if } v_F(\alpha) \equiv 0 \pmod 4 \textit{ for all } \alpha \in \mathcal{A}, \\ \frac{1}{2} \cdot \#N_E^{\mathcal{A}} & \textit{else if } 2 \mid v_F(\alpha) \textit{ for all } \alpha \in \mathcal{A}, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Clearly, if $2 \nmid v_F(\alpha)$ for any $\alpha \in \mathcal{A}$, then $\text{Ét}_{(2^2)/F,\leq m}^{C_4/F,\mathcal{A}} = \varnothing$. Therefore, we will assume that $2 \mid v_F(\alpha)$ for all $\alpha \in \mathcal{A}$. By Lemma 9.1, the natural map

$$\text{Ét}_{(1^2)/E,\leq \lfloor \frac{m}{2} \rfloor}^{C_4/F} \to \text{Ét}_{(2^2)/F,\leq m}^{C_4/F}$$

is a bijection. Let $m_2 = \lfloor \frac{m}{2} \rfloor$. Suppose that $m \leq 4e_F + 1$. Then Lemmas 8.19 and 13.16 tell us that

$$\#\operatorname{Ext}_{2/E,\leq m_2}^{C_4/F,\mathcal{A}} = \frac{1}{2} \cdot \#N_{E,2e_F - 2\lfloor \frac{m_2}{2} \rfloor}^{\mathcal{A}}.$$

It is easy to see that $\lfloor \frac{m_2}{2} \rfloor = \lfloor \frac{m}{4} \rfloor$, and also that $\operatorname{Ext}_{2/E,\leq m_2}^{C_4/F,\mathcal{A}}$ contains the unramified quadratic extension if and only if $v_F(\alpha) \equiv 0 \pmod 4$ for all $\alpha \in \mathcal{A}$. The result for $m \leq 4e_F + 1$ follows.

The argument for $m \geq 4e_F + 2$ is similar but easier, so we omit it. □

Corollary 13.18. *For each nonnegative integer m, we have*

$$\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(2^2)/F,m} = \begin{cases} \frac{1}{2}\cdot\left(\#N^{\mathcal{A}}_{E,2e_F-\frac{m}{2}} - \#N^{\mathcal{A}}_{E,2e_F-\frac{m}{2}+2}\right) & \text{if } 4 \mid m \text{ and } 4 \le m \le 4e_F, \\ \frac{1}{2}\cdot\left(\#N^{\mathcal{A}}_{E} - \#N^{\mathcal{A}}_{E,0}\right) & \text{if } m = 4e_F+2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This follows easily from Lemma 13.17. □

Proof of Theorem 10.11. We address the statements one by one.

1. An S_4- or A_4-quartic extension has no proper intermediate fields, so it cannot have splitting symbol (2^2).
2. This is precisely Lemma 13.14.
3. This follows from Corollary 12.31 and Lemma 13.8.
4. This follows from Corollary 13.18.

□

In the special case where $\mathcal{A}$ is generated by a single element, we can write down a simple description of the sizes $\#N^{\mathcal{A}}_{E,c}$, and hence of the counts $\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(2^2)/F,m}$. We note these descriptions in Lemma 13.19 and Corollary 13.20.

Lemma 13.19. *Let $\alpha \in F^\times \backslash F^{\times 2}$, let $d_\alpha = v_F(d_{F(\sqrt{\alpha})/F})$, and let E/F be the unique unramified quadratic extension of F. For each nonnegative integer c, we have*

$$\#N^{\langle\alpha\rangle}_{E,c} = \begin{cases} q^{e_F - \lceil\frac{c-1}{2}\rceil} & \text{if } c < d_\alpha, \\ 2q^{e_F-\lceil\frac{c-1}{2}\rceil} & \text{if } d_\alpha \le c \le 2e_F \text{ and } v_F(\alpha) \equiv 0 \pmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. From the definition of $N^{\mathcal{A}}_E$, it is easy to see that

$$N^{\langle\alpha\rangle}_{E} = \begin{cases} \overline{N}^2_\alpha & \text{if } v_F(\alpha) \equiv 0 \pmod 4, \\ (F^\times/F^{\times 2}) \setminus \overline{N}^2_\alpha & \text{otherwise.} \end{cases}$$

By Lemma 12.11, we have $U^{(c)}_F F^{\times 2}/F^{\times 2} \subseteq \overline{N}^2_\alpha$ if and only if $c \ge d_\alpha$. By elementary linear algebra, it follows that

$$\#N^{\langle\alpha\rangle}_{E,c} = \begin{cases} \frac{1}{2}\cdot\#\left(U^{(c)}_F F^{\times 2}/F^{\times 2}\right) & \text{if } c < d_\alpha, \\ \#\left(U^{(c)}_F F^{\times 2}/F^{\times 2}\right) & \text{if } c \ge d_\alpha \text{ and } v_F(\alpha) \equiv 0 \pmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

The result follows by Corollary 12.22. □

Corollary 13.20. *Let $\alpha \in F^\times \setminus F^{\times 2}$, and let m be an integer. If $\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\langle\alpha\rangle}_{(2^2)/F,m}$ is nonempty, then $v_F(\alpha)$ is even and either $m = 4e_F + 2$ or m is a multiple of 4 with $4 \le m \le 4e_F$. If $v_F(\alpha) \equiv 0 \pmod 4$ and m is a multiple of 4 with $4 \le m \le 4e_F$, then*

$$\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\langle\alpha\rangle}_{(2^2)/F,m} = \begin{cases} \frac{1}{2}q^{\frac{m}{4}-1}(q-1) & \text{if } m > 4e_F - 2d_\alpha + 4, \\ \frac{1}{2}q^{\frac{m}{4}-1}(q-2) & \text{if } m = 4e_F - 2d_\alpha + 4, \\ q^{\frac{m}{4}-1}(q-1) & \text{if } m < 4e_F - 2d_\alpha + 4. \end{cases}$$

If $v_F(\alpha) \equiv 2 \pmod 4$ and m is a multiple of 4 with $4 \leq m \leq 4e_F$, then

$$\#\text{Ét}^{C_4/F,\langle\alpha\rangle}_{(2^2)/F,m} = \begin{cases} \frac{1}{2}q^{\frac{m}{4}-1}(q-1) & \textit{if } m > 4e_F - 2d_\alpha + 4, \\ \frac{1}{2}q^{\frac{m}{4}} & \textit{if } m = 4e_F - 2d_\alpha + 4, \\ 0 & \textit{if } m < 4e_F - 2d_\alpha + 4. \end{cases}$$

If $v_F(\alpha)$ is even and $m = 4e_F + 2$, then

$$\#\text{Ét}^{C_4/F,\langle\alpha\rangle}_{(2^2)/F,4e_F+2} = \begin{cases} \frac{1}{2}q^{e_F} & \textit{if } d_\alpha > 0, \\ q^{e_F} & \textit{if } v_F(\alpha) \equiv 2 \pmod 4 \textit{ and } d_\alpha = 0, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. By Lemma 8.5, if $v_F(\alpha)$ is even then d_α is even. The result follows from Corollary 13.18 and Lemma 13.19. □

Lemma 13.21. *For $G \in \{S_4, A_4\}$, we have*

$$\text{Ét}^{G/F,\mathcal{A}}_{(1^4)/F} = \text{Ét}^{G/F}_{(1^4)/F}.$$

Proof. Let $L \in \text{Ét}^{G/F}_{(1^4)/F}$, for $G \in \{S_4, A_4\}$. Then L/F has no intermediate fields, so class field theory tells us that $N_{L/F}L^\times = F^\times$. □

Lemma 13.22. *We have*

$$\#\text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m} = \frac{1}{2}\sum_{\substack{2m_1+m_2=m\\ m_1,m_2>0}}\ \sum_{E\in\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}} \Big(\#\text{Ét}_{(1^2)/E,m_2} - \#\text{Ét}^{C_4/F}_{(1^2)/E,m_2} - \#\text{Ét}^{V_4/F}_{(1^2)/E,m_2}\Big).$$

Proof. We will construct a 2-to-1 surjection

$$\bigsqcup_{\substack{2m_1+m_2=m\\ m_1,m_2>0}}\ \bigsqcup_{E\in\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}} \big\{L \in \text{Ét}_{(1^2)/E,m_2} : L/F \text{ not Galois}\big\} \to \text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m},$$

thus proving the result. An element of the left-hand side may be written as a pair (E, L), where $E \in \text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}$ and $L \in \text{Ét}_{(1^2)/E,m_2}$. Using the tower law for discriminant, it is easy to see that there is a well-defined map

$$\Phi : \bigsqcup_{\substack{2m_1+m_2=m\\ m_1,m_2>0}}\ \bigsqcup_{E\in\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}} \big\{L \in \text{Ét}_{(1^2)/E,m_2} : L/F \text{ not Galois}\big\} \to \text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m}, \quad (E, L) \mapsto L.$$

Let $L \in \text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m}$. Since L/F has Galois closure group D_4, it has a unique quadratic intermediate field E. It is easy to see that the pair (E, L) is in the domain of Φ, so Φ is surjective. Let $L \in \text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m}$. It is easy to see that

$$\Phi^{-1}(L) = \{(E, E(\sqrt{\alpha})), (E, E(\sqrt{\bar\alpha}))\},$$

where E/F is the unique quadratic subextension of L/F, and $\alpha \in E^\times$ is an element with $L = E(\sqrt{\alpha})$. Since L/F is non-Galois, we have $E(\sqrt{\alpha}) \ncong E(\sqrt{\bar\alpha})$ as extensions of E, and therefore the preimage $\Phi^{-1}(L)$ has exactly two elements, so we are done. □

Lemma 13.23. *Let $E \in \text{Ét}_{(1^2)/F,m_1}$ for some integer m_1. For each nonnegative integer m_2, we have*

$$\#\text{Ét}^{V_4/F}_{(1^2)/E,m_2} = N^{V_4}(m_1, m_2),$$

where N^{V_4} is the function defined in Appendix B.

Proof. By the tower law for discriminant, every $L \in \text{Ét}^{V_4/F}_{(1^2)/E,m_2}$ has $v_F(d_{L/F}) = 2m_1 + m_2$. We will use this fact without reference throughout the proof. Suppose that $m_2 < m_1$. By Lemma 6.19, we have a bijection

$$\text{Ét}_{(1^2)/F,m_2} \to \text{Ét}^{V_4/F}_{(1^2)/E,m_2}, \quad E' \mapsto EE'.$$

If $m_2 > m_1$, then similarly we obtain a 2-to-1 surjection

$$\text{Ét}_{(1^2)/F,\frac{m_1+m_2}{2}} \to \text{Ét}^{V_4/F}_{(1^2)/E,m_2}, \quad E \mapsto EE'.$$

Using these two maps, the result for $m_1 \neq m_2$ follows from Theorem 12.24. Finally, suppose that $m_1 = m_2$. Suppose that $L \in \text{Ét}^{V_4/F}_{(1^2)/E,m_2}$ and $L = EE'$ for some quadratic extension E'/F. Let $\chi, \chi' : F^\times/F^{\times 2} \to \mathbb{F}_2$ be the quadratic characters associated to E and E' respectively. By Theorem 12.10 and Lemma 12.11, we have

$$\mathfrak{f}(\chi) = v_F(d_{E/F}) = \min\left\{c : U_F^{(c)}F^{\times 2}/F^{\times 2} \subseteq \ker\chi\right\},$$

and similarly for χ' and E'. By Lemma 6.19, we have

$$m_1 + \mathfrak{f}(\chi') + \mathfrak{f}(\chi\chi') = v_F(d_{L/F}) = 2m_1 + m_2 = 3m_1,$$

so

$$\mathfrak{f}(\chi') + \mathfrak{f}(\chi\chi') = 2m_1.$$

If $\mathfrak{f}(\chi') \neq m_1$, then Lemma 6.19 tells us that

$$\mathfrak{f}(\chi\chi') = \max\{m_1, \mathfrak{f}(\chi')\},$$

so

$$\mathfrak{f}(\chi') + \max\{m_1, \mathfrak{f}(\chi')\} = 2m_1,$$

which is impossible. It follows that $\mathfrak{f}(\chi') = \mathfrak{f}(\chi\chi') = m_1$, so

$$\#\text{Ét}^{V_4/F}_{(1^2)/E,m_1} = \frac{1}{2}\cdot\#\left\{\chi' : F^\times/U_F^{(m_1)}F^{\times 2} \to \mathbb{F}_2 \;\middle|\; \chi'|_{W_{m_1-1}} \notin \{0, \chi|_{W_{m_1-1}}\}\right\}.$$

If $m_1 = 2e_F + 1$, then $W_{m_1-1} \cong C_2$ by Corollary 12.21, so $\text{Ét}^{V_4/F}_{(1^2)/E,m_1} = \varnothing$. If m_1 is even with $2 \leq m_1 \leq 2e_F$, then Corollary 12.21 tells us that $\#W_{m_1-1} = q$, so there are $q-2$ possible restrictions $\chi'|_{W_{m_1-1}}$. Each such restriction lifts to

$$\#(F^\times/U_F^{(m_1-2)}F^{\times 2}) = 2q^{\frac{m_1}{2}-1}$$

characters, so we have

$$\#\left\{\chi' : F^\times/U_F^{(m_1)}F^{\times 2} \to \mathbb{F}_2 \;\middle|\; \chi'|_{W_{m_1-1}} \notin \{0, \chi|_{W_{m_1-1}}\}\right\} = 2q^{\frac{m_1}{2}-1}(q-2),$$

and the result for $m_1 = m_2$ follows. □

Lemma 13.24. *We have*

$$\#\text{Ét}^{D_4/F,\mathcal{A}}_{(1^4)/F,m} = \frac{1}{2}\cdot\sum_{0<m_1<m/2}\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}\cdot\Big(N^{C_2}(m-2m_1) - N^{C_4}(m_1, m-2m_1) - N^{V_4}(m_1, m-2m_1)\Big),$$

where the functions N^{C_2}, N^{C_4}, and N^{V_4} are as defined in Appendix B. We can compute this quantity explicitly using Corollary 12.31.

Proof. This follows easily from Lemma 8.3, Theorem 12.24, Lemma 13.22, and Lemma 13.23. □

Lemma 13.25. *Let m be an integer. If $\text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m}$ is nonempty, then m is an even integer with $6 \leq m \leq 6e_F + 2$. In that case, the number $\#\text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m}$ is the sum of the following two quantities:*

(1)

$$\frac{1}{2} \cdot \sum_{\substack{m_1 < m_2 \\ m_1 + 2m_2 = m}} \Big(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}\Big)\Big(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_2}\Big).$$

(2)

$$\mathbb{1}_{3|m} \cdot \frac{2}{3(\#\overline{\mathcal{A}}^2)^2} \cdot q^{\frac{m}{3}-2}\Big(q\#\overline{\mathcal{A}}^2_{m/3} - \#\overline{\mathcal{A}}^2_{m/3-1}\Big)\Big(q\#\overline{\mathcal{A}}^2_{m/3} - 2\#\overline{\mathcal{A}}^2_{m/3-1}\Big).$$

Proof. The necessary conditions on m, namely that m is even with $6 \leq m \leq 6e_F + 2$, come from Lemma 5.5. Assume that m satisfies these conditions. Define the map

$$\Phi : \bigsqcup_{\substack{m_1 < m_2 \\ m_1 + 2m_2 = m}} \text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1} \times \text{Ét}^{\mathcal{A}}_{(1^2)/F,m_2} \to \text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m}, \quad (E_1, E_2) \mapsto E_1E_2.$$

By Lemma 6.19, this map is well-defined and 2-to-1, so

$$\#\operatorname{im}\Phi = \frac{1}{2} \cdot \sum_{\substack{m_1 < m_2 \\ m_1 + 2m_2 = m}} \Big(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}\Big)\Big(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_2}\Big).$$

If $3 \nmid m$, then Φ is surjective, so we are done. Suppose that $3 \mid m$. Let S be the set of $L \in \text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m}$ such that every intermediate quadratic field E of L has $v_F(d_{E/F}) = m/3$. Then

$$\text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m} = S \sqcup \operatorname{im}\Phi,$$

so

$$\#\text{Ét}^{V_4/F,\mathcal{A}}_{(1^4)/F,m} = \#S + \frac{1}{2} \cdot \sum_{\substack{m_1 < m_2 \\ m_1 + 2m_2 = m}} \Big(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}\Big)\Big(\#\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_2}\Big).$$

Let Σ be the set of pairs (χ_1, χ_2), where:

(1) χ_1 and χ_2 are quadratic characters $\chi_i : F^\times/U_F^{(m/3)}F^{\times 2} \to \mathbb{F}_2$.
(2) The restrictions of χ_1 and χ_2 to $U_F^{(m/3-1)}F^{\times 2}/U_F^{(m/3)}F^{\times 2}$ are nonzero and distinct.
(3) For $i = 1, 2$, we have

$$\chi_i\Big(\mathcal{A}U_F^{(m/3)}F^{\times 2}/F^{\times 2}U_F^{(m/3)}\Big) = 0.$$

Then there is a natural 6-to-1 surjection $\Sigma \to S$, so

$$\#S = \frac{1}{6} \cdot \#\Sigma.$$

Evaluating $\#S$ amounts to a simple linear algebra problem. To emphasise this simplicity, we define:

(1)

$$V = F^\times/U_F^{(m/3)}F^{\times 2}.$$

(2)

$$M = U_F^{(m/3-1)}F^{\times 2}/U_F^{(m/3)}F^{\times 2}.$$

(3)
$$N = \mathcal{A}U_F^{(m/3)}F^{\times 2}/U_F^{(m/3)}F^{\times 2}.$$

Then V is an $\mathbb{F}_2$-vector space, M and N are subspaces of V, and we are looking for pairs of linear transformations $\chi_1, \chi_2 : V \to \mathbb{F}_2$ such that the following two statements are true:

(1) $\chi_i(N) = 0$ for $i = 1, 2$.
(2) The restrictions $\chi_1|_M$ and $\chi_2|_M$ are nonzero and distinct.

These correspond bijectively to pairs $\overline{\chi}_1, \overline{\chi}_2 : V/N \to \mathbb{F}_2$ such that the restrictions $\overline{\chi}_1|_{(M+N)/N}$ and $\overline{\chi}_2|_{(M+N)/N}$ are nonzero and distinct. There are
$$\Big(\#\Big(\frac{M+N}{N}\Big) - 1\Big)\Big(\#\Big(\frac{M+N}{N}\Big) - 2\Big)$$
possibilities for the pair $(\overline{\chi}_1|_{(M+N)/N}, \overline{\chi}_2|_{(M+N)/N})$. Each of these lifts to
$$\Big(\#\Big(\frac{V}{M+N}\Big)\Big)^2$$
pairs $(\overline{\chi}_1, \overline{\chi}_2)$, so we have
$$\#\Sigma = \Big(\#\Big(\frac{V}{M+N}\Big)\Big)^2 \cdot \Big(\#\Big(\frac{M+N}{N}\Big) - 1\Big)\Big(\#\Big(\frac{M+N}{N}\Big) - 2\Big).$$
We evaluate the sizes of the relevant vector spaces.

(1) Corollary 12.22 tells us that
$$\#V = 2q^{\frac{m}{6}}.$$
(2) By the second and third isomorphism theorems for groups, we have
$$N = \frac{\mathcal{A}U_F^{(m/3)}F^{\times 2}}{U_F^{(m/3)}F^{\times 2}} \cong \frac{\overline{\mathcal{A}}^2}{\overline{\mathcal{A}}^2_{m/3}},$$
so
$$\#N = \frac{\#\overline{\mathcal{A}}^2}{\#\overline{\mathcal{A}}^2_{m/3}}.$$
(3) We have
$$M + N = \frac{\mathcal{A}U_F^{(m/3-1)}F^{\times 2}}{U_F^{(m/3)}F^{\times 2}},$$
so
$$\#(M+N) = \Big[\mathcal{A}U_F^{(m/3-1)}F^{\times 2} : U_F^{(m/3-1)}F^{\times 2}\Big] \cdot \#W_{m/3-1}.$$
By the second and third isomorphism theorems for groups, we have
$$\frac{\mathcal{A}U_F^{(m/3-1)}F^{\times 2}}{U_F^{(m/3-1)}F^{\times 2}} \cong \frac{\overline{\mathcal{A}}^2}{\overline{\mathcal{A}}^2_{m/3-1}},$$
so Corollary 12.21 tells us that
$$\#(M+N) = q \cdot \frac{\#\overline{\mathcal{A}}^2}{\#\overline{\mathcal{A}}^2_{m/3-1}}.$$

It follows that
$$\#\Sigma = \frac{4q^{\frac{m}{3}-2}}{(\#\overline{\mathcal{A}}^2)^2} \cdot \Big(q\#\overline{\mathcal{A}}^2_{m/3} - \#\overline{\mathcal{A}}^2_{m/3-1}\Big)\Big(q\#\overline{\mathcal{A}}^2_{m/3} - 2\#\overline{\mathcal{A}}^2_{m/3-1}\Big).$$

□

13.3. **Totally wildly ramified C_4-extensions.** Our goal in this subsection is to prove Theorem 10.12, which gives us algorithms for computing $\widetilde{m}\big(\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(1^4)/F}\big)$, and analyse the time complexity of those algorithms to prove Theorem 10.13.

Lemma 13.26. *Let m_1 and m_2 be integers, with m_1 even. Then*

$$\Big\lfloor \frac{m_1}{4} + \frac{1}{2}\Big\lfloor\frac{m_2}{2}\Big\rfloor\Big\rfloor = \Big\lfloor\frac{m_1+m_2}{4}\Big\rfloor.$$

Proof. This is easy to see by writing $m_1 = 2k_1$ and $m_2 = 2k_2 + r$, for $r \in \{0, 1\}$. □

Lemma 13.27. *Let F be a 2-adic field and let $E \in \acute{\mathrm{E}}\mathrm{t}^{\mathcal{A}}_{(1^2)/F}$. If $-1 \notin N_{E/F}E^\times$, then*

$$\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^2)/E} = \varnothing.$$

For the rest of the lemma, assume that $-1 \in N_{E/F}E^\times$. Let $m_1 = v_F(d_{E/F})$, and let m_2 be an integer. Let

$$c(m_2) = 2e_F - 2\Big\lfloor\frac{m_1+m_2}{4}\Big\rfloor.$$

If $m_1 \le e_F$, then

$$\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(1^2)/E,\le m_2} = \begin{cases} 0 & \text{if } m_2 < 3m_1 - 2,\\ \frac{1}{2}\cdot \#N^{\mathcal{A}}_{E,c(m_2)} & \text{if } 3m_1 - 2 \le m_2 \le 4e_F - m_1 + 1,\\ \frac{1}{2}\cdot\#N^{\mathcal{A}}_E & \text{if } m_2 \ge 4e_F - m_1 + 2.\end{cases}$$

If $m_1 > e_F$, then

$$\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(1^2)/E,\le m_2} = \begin{cases} 0 & \text{if } m_2 < m_1 + 2e_F,\\ \frac{1}{2}\cdot\#N^{\mathcal{A}}_E & \text{if } m_2 \ge m_1 + 2e_F.\end{cases}$$

Proof. If $-1 \notin N_{E/F}E^\times$, then $\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^2)/E} = \varnothing$ by Corollary 8.8. Suppose that $-1 \in N_{E/F}E^\times$. Then Corollary 8.8 and Lemma 8.17 tell us that $\acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^2)/E,\le m_2}$ is nonempty if and only if

$$m_2 \ge \begin{cases} 3m_1 - 2 & \text{if } m_1 \le e_F,\\ 2e_F + m_1 & \text{if } m_1 > e_F.\end{cases}$$

Suppose that $m_1 \le e_F$ and $m_2 \ge 3m_1 - 2$. If $m_2 \le 4e_F - m_1 + 1$, then Lemmas 8.19, 13.16, and 13.26 give a 2-to-1 surjection

$$N^{\mathcal{A}}_{E,c(m_2)} \to \mathrm{Ext}^{C_4/F,\mathcal{A}}_{2/E,\le m_2}.$$

If $m_2 \ge 4e_F - m_1 + 2$, then Lemma 8.3 tells us that

$$\mathrm{Ext}^{C_4/F}_{2/E,\le m_2} = \mathrm{Ext}^{C_4/F}_{2/E,\le 4e_F - m_1 + 2},$$

and we have

$$\#\mathrm{Ext}^{C_4/F}_{2/E,\le 4e_F - m_1+2} = \frac{1}{2}\cdot\#N^{\mathcal{A}}_E$$

by Lemmas 8.19 and 13.16. The result for $m_1 \le e_F$ follows. The argument for $m_1 > e_F$ is similar but easier, so we omit it. □

Proof of Theorem 10.12. We prove the statements one at a time:

(1) This is immediate from Lemma 13.21.

(2) This follows easily from Lemma 8.3, Theorem 12.24, Lemma 13.22, and Lemma 13.23.
(3) This is precisely Lemma 13.25.
(4) This is immediate from Lemma 13.27.

□

Algorithm 13.28. Let F be a 2-adic field, let m_1 be an even integer with $m_1 \leq e_F$, and let $E \in \acute{\mathrm{E}}\mathrm{t}_{(1^2)/F,m_1}$ be C_4-extendable.

(1) Take $d \in F^\times$ such that $E = F(\sqrt{d})$ and $v_F(d) = m_1$.
(2) Take $a, b \in F^\times$ with $d = a^2 + 4b$, such that $v_F(a) = m_1/2$ and $v_F(b) = 1$.
(3) Define $\rho = \frac{a+\sqrt{d}}{2}$, which is a uniformiser of E.
(4) Choose $\omega \in E^\times$ such that $N_{E/F}\omega \in dF^{\times 2}$ and $v_E(\omega) = 0$.
(5) Take $\lambda \in F^\times$ such that

$$N_{E/F}\omega \equiv \lambda^2 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}.$$

(6) Define

$$\omega_1 = \begin{cases} \omega & \text{if } v_E(\omega - \lambda) \geq m_1, \\ \frac{\omega b}{\rho^2} & \text{if } v_E(\omega - \lambda) = m_1 - 1. \end{cases}$$

(7) Define

$$\omega_2 = \begin{cases} \omega_1 & \text{if } v_E(\omega_1 - \bar{\omega}_1) = 2m_1, \\ \omega_1(1+\rho)^2 & \text{if } v_E(\omega_1 - \bar{\omega}_1) > 2m_1, \end{cases}$$

and

$$\lambda_2 = \begin{cases} \lambda & \text{if } v_E(\omega_1 - \bar{\omega}_1) = 2m_1, \\ \lambda(1+a-b) & \text{if } v_E(\omega_1 - \bar{\omega}_1) > 2m_1. \end{cases}$$

(8) Write $\omega_2 = r_2 + s_2\rho$ for $r_2, s_2 \in F$, and define

$$q = \frac{r_2 - \lambda_2}{s_2}, \quad n = \frac{q^2 + b}{r_2}.$$

(9) Output $\frac{\omega_2 n}{(q+\rho)^2}$.

Theorem 13.29. *Let E, m_1 be as in Algorithm 13.28.*

(1) All the steps of the algorithm are well-defined.
(2) Let ω be the output of the algorithm. Then $E(\sqrt{\omega}) \in \acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^2)/E,3m_1-2}$.

Proof. This is essentially [CDO05, Proposition 3.15]. We rewrite their proof using our notation in Appendix A. □

Definition 13.30. Let K be a field and let M be a matrix with entries in K. A *reduced row decomposition of* M is a triple $(\widetilde{M}, T, T^{-1})$, where $\widetilde{M}$ is a matrix in reduced row echelon form and T is a composition of elementary matrices with $M = T\widetilde{M}$. For computational efficiency, we consider the inverse matrix T^{-1} to be part of the data of the reduced row decomposition.

Lemma 13.31. *Let M be an $m \times n$ matrix defined over a field K. We can compute a reduced row decomposition of M using $O(mn \min\{m, n\})$ field operations in K.*

Proof. For $i = 1, \ldots, \min\{m, n\}$, the i^{th} step of Gaussian elimination (i.e. reducing the i^{th} column) requires $O(n)$ elementary row operations. Each elementary row operation requires $O(m)$ field operations in K, so we are done. □

Definition 13.32. Let F be a p-adic field for some rational prime p. Let E/F be a field extension with $[E : F] \leq 4$, let $m(X) \in \mathbb{Q}_p[X]$ be a monic degree f_E polynomial that is irreducible over $\mathbb{F}_p[X]$, and let $\alpha \in E$ be a root of $m(X)$. Define the set

$$\mathcal{B}_0^E = \{1, \alpha, \ldots, \alpha^{f_E - 1}\}.$$

We will assume that (as is the case with Magma's 'FldPad' object class) the maximal unramified subextension of $E/\mathbb{Q}_p$ is defined as $\frac{\mathbb{Q}_p[X]}{(m(X))}$, so that $\mathcal{B}_0^E$ is part of the data of E.

Lemma 13.33. *Let F and E be as in Definition 13.32. The following three statements are true:*

(1) The set $\mathcal{B}_0^E$ descends to an $\mathbb{F}_p$-basis for the vector space $\mathbb{F}_E$.
(2) For any $x \in \mathcal{O}_E$, we can compute the $\mathcal{B}_0^E$-coefficients of $[x] \in \mathbb{F}_E$ with time complexity $O_F(1)$.
(3) Suppose that we have an $\mathbb{F}_p$-linear transformation $\varphi : \mathbb{F}_E \to \mathbb{F}_E$ that we can evaluate with time complexity $O_F(t)$, for some function t. We can compute the matrix $[\varphi]_{\mathcal{B}_0^E}$ with time complexity $O_F(f_F \cdot t)$.

Proof. Recall the polynomial $m(X) \in \mathbb{Q}_p[X]$ from Definition 13.32. The first statement follows from the fact that $\mathbb{F}_E$ is defined by $m(X)$ as an extension of $\mathbb{F}_p$. The second statement follows from the fact that (at least in Magma) x is implemented as a power series in π_E with coefficients in the maximal unramified subextension E^{ur} of E, and elements of E^{ur} are stored as $\mathbb{Z}_p$-linear combinations of $\mathcal{B}_0^E$. We can reduce all of these $\mathbb{Z}_p$-coefficients modulo p with time complexity $O(f_F) \ll O_F(1)$. The third statement follows immediately from the second. □

Lemma 13.34. *Let F be a p-adic field for some rational prime p, and let E/F be a field extension with $[E : F] \leq 4$. Recall the map*

$$\varphi : \mathbb{F}_E \to \mathbb{F}_E, \quad [y] \mapsto \left[y + \frac{\pi_E^{e_E}}{p} y^p\right]$$

from Algorithm 12.19. We can compute a reduced row decomposition of the matrix $[\varphi]_{\mathcal{B}_0^E}$ with time complexity $O_F(f_F^3 + f_F \log e_F + f_F \log p)$.

Proof. A single evaluation of φ has time complexity $O_F(\log e_F + \log p)$, so Lemma 13.33 tells us that we can compute $[\varphi]_{\mathcal{B}_0^E}$ with time complexity $O_F(f_F \log e_F + f_F \log p)$. The result follows from Lemma 13.31. □

Lemma 13.35. *Let F be a p-adic field for some rational prime p and let $\varphi : \mathbb{F}_F \to \mathbb{F}_F$ be the map from Algorithm 12.19. If we have already computed a reduced row decomposition for $[\varphi]_{\mathcal{B}_0^F}$, then Algorithm 12.19 can be run with time complexity $O_F([F : \mathbb{Q}_p])$.*

Proof. Steps (1) and (3) have time complexity $O_F(1)$. Consider the iteration in Step (2). The steps with $p \nmid i$ have time complexity $O_F(1)$, and there are $O(e_F)$ such steps, so we can perform them all with time complexity $O_F(e_F)$. The steps with $p \mid i$ and $i < \frac{pe_F}{p-1}$ have time complexity $O_F(f_F \log p)$, since taking p^{th} roots in $\mathbb{F}_F$ is equivalent to raising to the power of $p^{f_F - 1}$. There are $O(e_F/p)$ such steps, so we can perform all of them with time complexity $O_F([F : \mathbb{Q}_p] \cdot \frac{\log p}{p})$. Thus, we can perform all the steps where $i < \frac{pe_F}{p-1}$ with time complexity $O_F([F : \mathbb{Q}_p])$.

Assume that we have a primitive root modulo p and a logarithm table for $\mathbb{F}_p$ with respect to this primitive root, so that we can perform any field operation in $\mathbb{F}_p$ with time complexity $O(1)$. This is a modest requirement, and we consider it to be part of any sensible implementation. Let

$(\widetilde{M}, T, T^{-1})$ be our reduced row descomposition of $[\varphi]_{\mathcal{B}_0^F}$. Then the final step amounts to finding a vector $v \in \mathbb{F}_p^{f_F}$ with $\widetilde{M}v = T^{-1}[\frac{m_i - 1}{\pi_F^{e_F/(p-1)} p}]_{\mathcal{B}_0^E}$. This has time complexity $O(f_F^2) \ll O_F(1)$. □

Lemma 13.36. *Let F be a p-adic field for some rational prime p, and let E be an extension of F with $[E : F] \leq 4$. Let $\mathcal{B}_{-1} = \{\pi_E\}$ and let $\mathcal{B}_0 = \mathcal{B}_0^E$. If $\mu_p \not\subseteq E$, then set $\mathcal{B}_{\frac{pe_E}{p-1}} = \varnothing$. Suppose instead that $\mu_p \subseteq E$. Let $u_{\frac{pe_E}{p-1}} \in \mathcal{O}_E^\times$ be an element such that $[u_{\frac{pe_E}{p-1}}] \in \mathbb{F}_E$ is not in the image of the map*

$$\varphi : \mathbb{F}_E \to \mathbb{F}_E, \quad [y] \mapsto \Big[y + \frac{\pi_E^{e_E}}{p} y^p\Big],$$

and define $\mathcal{B}_{\frac{pe_E}{p-1}} = \{1 + p\pi_E^{e_E/(p-1)} u_{\frac{pe_E}{p-1}}\}$. Define

$$\mathcal{B} = \mathcal{B}_{-1} \sqcup \mathcal{B}_{\frac{pe_E}{p-1}} \sqcup \bigsqcup_{\substack{1 \leq i \leq \lceil \frac{pe_E}{p-1} \rceil - 1 \\ p \nmid i}} \{1 + \pi_E^i u : u \in \mathcal{B}_0\}.$$

The following two statements are true:

(1) $\mathcal{B}$ is a system of representatives for a basis of the $\mathbb{F}_p$-vector space $E^\times / E^{\times p}$.

(2) Assume that we have already computed a reduced row decomposition of $[\varphi]_{\mathcal{B}_0^E}$. For any element $\alpha \in E^\times$, we can compute the coefficients of $[\alpha] \in E^\times / E^{\times p}$ with respect to the basis induced by $\mathcal{B}$ with time complexity $O_F([F : \mathbb{Q}_p])$.

Proof. Corollary 12.22 tells us that the size of $\mathcal{B}$ equals the dimension of $E^\times / E^{\times p}$. Therefore, it suffices to prove that $\mathcal{B}$ spans $E^\times / E^{\times p}$. We will thus give an $O_F([F : \mathbb{Q}_p])$ algorithm for expressing $[\alpha] \in E^\times / E^{\times p}$ as a linear combination of $\mathcal{B}$, for any $\alpha \in E^\times$, thus proving both statements simultaneously.

Let $\alpha \in E^\times$. Without loss of generality, we may assume that $v_E(\alpha) \in \{0, 1, \ldots, p-1\}$. Let $\alpha_0 = \frac{\alpha}{\pi_E^{v_E(\alpha)}}$. We will recursively define an element α_{i+1} for each $i = 0, 1, 2, \ldots, \lceil \frac{pe_E}{p-1} \rceil - 1$. We claim that for each of these i, we have $\alpha_{i+1} \in U_E^{(i+1)}$. Clearly $\alpha_0 \in U_E^{(0)}$, so we have the base case for our induction.

- Suppose that $p \mid i$. With time complexity $O_F(f_F \log p)$, we can find $[y_i] \in \mathbb{F}_E$ such that
$$y_i^p \equiv \frac{\alpha_i - 1}{\pi_E^i} \pmod{\mathfrak{p}_E}.$$
Then set $\alpha_{i+1} = \alpha_i / (1 + \pi_E^{i/p} y_i)^p$, so that $\alpha_{i+1} \in U_E^{(i+1)}$ by Lemma 12.18.
- Suppose that $p \nmid i$. Since $\big[\frac{\alpha_i - 1}{\pi_E^i}\big] \in \mathbb{F}_E$, there are unique coefficients $\lambda_u^{(i)} \in \{0, 1, \ldots, p-1\}$ such that
$$\Big[\frac{\alpha_i - 1}{\pi_E^i}\Big] = \sum_{u \in \mathcal{B}_0} \lambda_u^{(i)} [u],$$
and by Lemma 13.33 we can determine the coefficients $\lambda_u^{(i)}$ with time complexity $O_F(1)$. By the natural isomorphism $\mathbb{F}_E \to U_E^{(i)} / U_E^{(i+1)}$, we have
$$\alpha_i \equiv \prod_{u \in \mathcal{B}_0} (1 + \pi_E^i u)^{\lambda_u^{(i)}} \pmod{\mathfrak{p}_E^{i+1}},$$
so we define
$$\alpha_{i+1} = \frac{\alpha_i}{\prod_{u \in \mathcal{B}_0} (1 + \pi_E^i u)^{\lambda_u^{(i)}}} \in U_E^{(i+1)}.$$

Suppose that $\mu_p \not\subseteq E$. Then Corollary 12.21 tells us that $\alpha_{\lceil \frac{pe_E}{p-1} \rceil} \in E^{\times p}$, and therefore

$$\alpha E^{\times p} = \pi_E^{v_E(\alpha)} \cdot \prod_{\substack{1 \leq i \leq \lceil \frac{pe_E}{p-1} \rceil - 1 \\ p \nmid i}} (1 + \pi_E^i u)^{\lambda_u^{(i)}} E^{\times p},$$

as required.

The coefficients $\lambda_u^{(i)}$ we have found so far were computed in $O(e_F)$ steps of time complexity $O_F(1)$, and $O(e_F/p)$ steps of time complexity $O_F(f_F \log p)$, so the algorithm so far has time complexity $O_F([F : \mathbb{Q}_p])$.

Suppose instead that $\mu_p \subseteq E$, so $(p-1) \mid e_E$. Let $\lambda^{(\frac{pe_E}{p-1})}$ be the unique element of $\mathbb{F}_p$ with

$$\alpha_{\frac{pe_E}{p-1}} - \lambda^{(\frac{pe_E}{p-1})} u_{\frac{pe_E}{p-1}} \in \operatorname{im} \varphi.$$

Let $(\widetilde{M}, T, T^{-1})$ be our reduced row decomposition of $[\varphi]_{\mathcal{B}_0^E}$. Then $\lambda^{(\frac{pe_E}{p-1})}$ can be read off from the final entries of the vectors $T^{-1}[\alpha_{\frac{pe_E}{p-1}}]_{\mathcal{B}_0^E}$ and $T^{-1}[u_{\frac{pe_E}{p-1}}]_{\mathcal{B}_0^E}$, which can be computed with time complexity $O(f_F) \ll O_F(1)$.

By Corollary 12.15, Lemma 12.18, and Lemma 12.20, we have

$$\alpha_{\frac{pe_E}{p-1}} / (1 + p\pi_E^{e_E/(p-1)} u_{\frac{pe_E}{p-1}})^{\lambda^{(\frac{pe_E}{p-1})}} \in E^{\times p}.$$

Thus, we have

$$\alpha E^{\times p} = \pi_E^{v_E(\alpha)} \cdot (1 + p\pi_E^{e_E/(p-1)} u_{\frac{pe_E}{p-1}})^{\lambda^{(\frac{pe_E}{p-1})}} \cdot \prod_{\substack{1 \leq i \leq \frac{pe_E}{p-1} - 1 \\ p \nmid i}} \prod_{u \in \mathcal{B}_0} (1 + \pi_E^i u)^{\lambda_u^{(i)}} E^{\times p},$$

as required. □

Lemma 13.37. *Let F be a 2-adic field and let $L/E/F$ be a tower of field extensions, where L/E is quadratic and $[E : F] \leq 2$. Let $d \in E^\times$. We can do the following with time complexity $O_F([F : \mathbb{Q}_2]^3)$:*

1. *(1) Determine whether $d \in N_{L/E} L^\times$.*
2. *(2) If so, find an element $\omega \in L^\times$ such that $N_{L/E}\omega \in dE^{\times 2}$.*

Proof. By Lemma 13.34, we can quickly compute a reduced row decomposition of $[\varphi]_{\mathcal{B}_0^E}$. Using Lemma 13.36, we can quickly write down a set $\mathcal{B} \subseteq L^\times$, of size $2 + [L : \mathbb{Q}_2]$, that descends to a basis of $L^\times / L^{\times 2}$. Taking norms[1], we obtain a spanning set $\operatorname{Nm} \mathcal{B}$ for $N_{L/E} L^\times / E^{\times 2}$.

Again using Lemma 13.36, fix a basis for $E^\times / E^{\times 2}$. Let $A \in \mathbb{F}_2^{(2+[E:\mathbb{Q}_2]) \times (2+[L:\mathbb{Q}_2])}$ be the matrix whose columns are the coordinates of the elements of $\operatorname{Nm} \mathcal{B}$, and let $v \in \mathbb{F}_2^{2+[E:\mathbb{Q}_2]}$ be the coordinate vector of $[d] \in E^\times / E^{\times 2}$. Note that, by Lemma 13.36, A and v can be computed with time complexity $O_F([F : \mathbb{Q}_2]^2)$. It then suffices to perform Gaussian elimination on the augmented matrix $(A \mid v)$. By Lemma 13.31, this Gaussian elimination be performed with time complexity $O_F([F : \mathbb{Q}_2]^3)$, so we are done. □

[1] Note that norms can be computed quickly since they are determinants of linear transformations in 2 dimensions.

Theorem 13.38. *Let F be a 2-adic field and let $\varphi : \mathbb{F}_F \to \mathbb{F}_F$ be the map from Algorithm 12.19. Assume that we have already computed a reduced row decomposition for $[\varphi]_{\mathcal{B}_0^F}$. Then Algorithm 13.28 can be performed with time complexity $O_F([F : \mathbb{Q}_2]^3)$.*

Proof. We compute the time complexity of each step of the algorithm, one by one. In Appendix A, we give expanded descriptions of these steps. In our analysis here, we use these expanded descriptions without reference.

(1) Clearly this has time complexity $O_F(1)$.
(2) We need to solve the congruence $\frac{X^2}{d} - 1 \equiv 0 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}$. By Lemma 13.35, we can do this with time complexity $O_F([F : \mathbb{Q}_2])$.
(3) This is clearly $O_F(1)$.
(4) By Lemma 13.37, this has time complexity $O_F([F : \mathbb{Q}_2]^3)$.
(5) Using Algorithm 12.19, we can find λ with time complexity $O_F([F : \mathbb{Q}_2])$, by Lemma 13.35.
(6)-(9) The remaining steps are all just computations in F, so they have time complexity $O_F(1)$.

□

Lemma 13.39. *Let K be a field, and let m, n_1, and n_2 be positive integers. For each $i \in \{1, 2\}$, let M_i be an $m \times n_i$ matrix with entries in K. We can compute a basis for*

$$\operatorname{colspan}(M_1) \cap \operatorname{colspan}(M_2)$$

using $O(m \cdot (n_1 + n_2) \cdot \min\{m, n_1 + n_2\})$ field operations in K.

Proof. We acknowledge the StackExchange answer [glS] as the inspiration for our argument. For each i, let $r_i = \operatorname{rank}(M_i)$. For each i, Lemma 13.31 tells us that, with $O(mn_i \min\{m, n_i\})$ field operations in K, we can use elementary column operations to replace M_i with an $m \times r_i$ matrix with the same column span. Do this for both i, so that both linear transformations $M_i : K^{r_i} \to K^m$ are injective. Let A be the matrix $(M_1| - M_2)$, so that we have a linear transformation $A : K^{r_1+r_2} \to K^m$. Lemma 13.31 tells us that we may compute a reduced row decomposition of A using $O(m \cdot (n_1 + n_2) \cdot \min\{m, n_1 + n_2\})$ field operations in K. Using this decomposition, we may then quickly find a basis $\{v_i\}_i$ for $\ker A$. For each i, write

$$v_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$$

for $x_i \in K^{r_1}$ and $y_i \in K^{r_2}$. Since M_1 and M_2 are injective, it is easy to see that $\{M_1 x_i\}_i$ is a basis for $\operatorname{colspan}(M_1) \cap \operatorname{colspan}(M_2)$, so we are done. □

Lemma 13.40. *Let F be a 2-adic field, let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup, and let c be a nonnegative integer. Given choices for ω and $\mathcal{G}_4(\mathcal{A})$, the size $\#N_{E,c}^{\mathcal{A}}$ may be computed with either of the following two time complexities:*

(1) $O_F(\#\mathcal{G}_4(\mathcal{A}) \cdot 2^{[F:\mathbb{Q}_2]} \cdot [F : \mathbb{Q}_2]^3)$.
(2) $O_F(2^{\#\mathcal{G}_4(\mathcal{A})} \cdot [F : \mathbb{Q}_2]^3)$.

Proof. The first algorithm is by brute-force. For each $x \in F^\times/F^{\times 2}$ and each $\alpha \in \mathcal{G}_4(\mathcal{A})$, Lemmas 13.15 and 13.37 tell us that we can check whether $\alpha \in N_\omega$ and whether $x \in \overline{N}_\alpha^2$ with time complexity $O_F([F : \mathbb{Q}_2]^3)$. Since $F^\times/F^{\times 2}$ has $2^{2+[F:\mathbb{Q}_2]}$ elements, this first algorithm has the claimed time complexity.

We now describe the second algorithm. Using Lemma 13.36, fix a basis for $F^\times/F^{\times 2}$. Also using Lemma 13.36, for each $\alpha \in \mathcal{G}_4(\mathcal{A})$, we can write down a basis for $F(\sqrt{\alpha})^\times/F(\sqrt{\alpha})^{\times 2}$ and use it to obtain a generating set for $\overline{N}^2_\alpha$. We can do this for all $\alpha \in \mathcal{G}_4(\mathcal{A})$ with time complexity $O_F(\#\mathcal{G}_2(\mathcal{A}) \cdot [F : \mathbb{Q}_2])$. Moreover, using Lemma 13.36, we can quickly express these generating sets in terms of our fixed basis for $F^\times/F^{\times 2}$, and by Lemma 13.31 we can reduce all of these generating sets to bases with time complexity

$$O_F(\#\mathcal{G}_2(\mathcal{A}) \cdot [F : \mathbb{Q}_2]^3).$$

Define the $\mathbb{F}_2$-vector subspace $V \subseteq F^\times/F^{\times 2}$ by

$$V = U_F^{(c)} F^{\times 2}/F^{\times 2} \cap \bigcap_{\alpha \in \mathcal{G}_4(\mathcal{A}) \cap N_\omega} \overline{N}^2_\alpha.$$

By Lemmas 13.15, 13.36, and 13.37, we can compute the intersection $\mathcal{G}_4(\mathcal{A}) \cap N_\omega$ with time complexity $O_F(\#\mathcal{G}_4(\mathcal{A}) \cdot [F : \mathbb{Q}_2]^3)$. Taking successive intersections, Lemma 13.39 tells us that we can compute a basis of V with time complexity

$$O_F(\#\mathcal{G}_4(\mathcal{A}) \cdot [F : \mathbb{Q}_2]^3).$$

Write $\{\alpha_1, \ldots, \alpha_m\} = \mathcal{G}_4(\mathcal{A}) \setminus N_\omega$, and for each i let

$$U_i = \overline{N}^2_{\alpha_i}.$$

Let k be a positive integer and suppose that we have integers i_j with $1 \leq i_1 < \ldots < i_k \leq m$. If we already have a basis for $V \cap \bigcap_{1 \leq j \leq k-1} U_{i_j}$, then using Lemma 13.39, we can compute a basis for $V \cap \bigcap_{1 \leq j \leq k} U_{i_j}$ with time complexity $O_F([F : \mathbb{Q}_2]^3)$. Doing this for each of the $2^{\#\mathcal{G}_4(\mathcal{A})}$ possible tuples (i_j), we can use the inclusion-exclusion principle to evaluate

$$\#N^{\mathcal{A}}_{E,c} = \#\Big(V \setminus \bigcup_i U_i\Big)$$

with time complexity $O_F(2^{\#\mathcal{G}_4(\mathcal{A})} \cdot [F : \mathbb{Q}_2]^3)$, as required. □

Lemma 13.41. *Let F be a 2-adic field, let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup, and fix a choice of $\mathcal{G}_4(\mathcal{A})$. Let $E \in \acute{\mathrm{E}}\mathrm{t}_{(1^2)/F}$. For each positive integer m_2, we can compute $\#\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(1^2)/E,m_2}$ with either of the following two time complexities:*

(1) $O_F(e_F \cdot \#\mathcal{G}_4(\mathcal{A}) \cdot 2^{[F:\mathbb{Q}_2]} \cdot [F : \mathbb{Q}_2]^3)$.
(2) $O_F(e_F \cdot 2^{\#\mathcal{G}_4(\mathcal{A})} \cdot [F : \mathbb{Q}_2]^3)$.

Proof. By class field theory, we have

$$\operatorname{Nm} F\big(\sqrt{\langle \mathcal{A}, -1\rangle}\big) = \operatorname{Nm} F(\sqrt{-1}) \cap \bigcap_{\alpha \in \mathcal{G}_4(\mathcal{A})} \operatorname{Nm} F(\sqrt{\alpha}).$$

Let $d \in F^\times$ be such that $E = F(\sqrt{d})$. By Lemma 13.37, we can determine whether $d \in \operatorname{Nm} F\big(\sqrt{\langle \mathcal{A}, -1\rangle}\big)$ with time complexity $O_F(\#\mathcal{G}_4(\mathcal{A}) \cdot [F : \mathbb{Q}_2]^3)$. Suppose that $d \notin \operatorname{Nm} F\big(\sqrt{\mathcal{A}, -1}\big)$. By symmetry of the quadratic Hilbert symbol, we have $\mathcal{A} \not\subseteq N_{E/F}E^\times$ or $-1 \notin N_{E/F}E^\times$. By the tower law for norms and Corollary 8.8, this implies that $\acute{\mathrm{E}}\mathrm{t}^{C_4/F,\mathcal{A}}_{(1^2)/E,m_2} = \varnothing$.

Suppose instead that $d \in \operatorname{Nm} F\big(\sqrt{\mathcal{A}, -1}\big)$, so that $E \in \acute{\mathrm{E}}\mathrm{t}^{\mathcal{A}}_{(1^2)/F}$ and $-1 \in N_{E/F}E^\times$. Let $m_1 = v_F(d_{E/F})$. If $m_1 \leq e_F$, then Theorem 13.29, Lemma 13.34, and Theorem 13.38 tell us that we can compute $\omega \in E^\times$ such that $E(\sqrt{\omega}) \in \acute{\mathrm{E}}\mathrm{t}^{C_4/F}_{(1^2)/E,3m_1-2}$ with time complexity $O_F([F : \mathbb{Q}_2]^3)$. If $m_1 > e_F$, then let $d \in F^\times$ be such that $E = F(\sqrt{d})$, and, again with time complexity $O_F([F : \mathbb{Q}_2]^3)$, let $\omega \in E^\times$ be such that $N_{E/F}\omega \in dF^{\times 2}$. In that case, Lemma 8.7 tells us that $E(\sqrt{\omega}) \in \text{Ét}^{C_4/F}_{(1^2)/E}$. Moreover, Lemma 8.3 tells us that $E(\sqrt{\omega})$ has minimal discriminant among elements of $\text{Ét}^{C_4/F}_{(1^2)/E}$. By Lemma 13.27, we now just need to compute each size $\#N^{\mathcal{A}}_{E,c}$ for $O(e_F)$ values of c, so the result follows by Lemma 13.40. □

Lemma 13.42. *Let F be a 2-adic field, and let $\mathcal{A} \subseteq F^\times$ be a finitely generated subgroup. Given a choice of $\mathcal{G}_4(\mathcal{A})$, the mass*

$$\widetilde{m}\left(\text{Ét}^{C_4/F,\mathcal{A}}_{(1^4)/F}\right)$$

can be computed with either of the following time complexities:

(1)
$$O_F\left(e_F \cdot \#\mathcal{G}_4(\mathcal{A}) \cdot 2^{2[F:\mathbb{Q}_2]} \cdot [F:\mathbb{Q}_2]^3\right).$$

(2)
$$O_F\left(e_F \cdot 2^{\#\mathcal{G}_4(\mathcal{A})} \cdot 2^{[F:\mathbb{Q}_2]} \cdot [F:\mathbb{Q}_2]^3\right).$$

Proof. There is a natural bijection

$$\bigsqcup_{\substack{2m_1+m_2=m\\ m_1,m_2>0}} \bigsqcup_{E\in\text{Ét}^{\mathcal{A}}_{(1^2)/F,m_1}} \text{Ét}^{C_4/F,\mathcal{A}}_{(1^2)/E,m_2} \longleftrightarrow \text{Ét}^{C_4/F,\mathcal{A}}_{(1^4)/F,m}.$$

Since $\#\text{Ét}^{C_2/F}_{(1^2)/F} = 4q^{e_F} - 2$, the result follows from Lemma 13.41. □

Proof of Theorem 10.13. It is clear that of all the quantities in Theorems 10.9, 10.10, 10.11, and 10.12, those in Theorem 10.12(4) are by far the most difficult to evaluate. Thus, the result follows immediately from Lemma 13.42. □

Appendix A. Proof of Theorem 13.29

Let E, m_1 be as in the setup of Algorithm 13.28. In this appendix, we will step through the algorithm, showing that each stage is well-defined, and eventually proving that the output has the desired property.

(1) Start by taking any d with $E = F(\sqrt{d})$. Since $v_F(d_{E/F}) \le e_F$, Lemma 8.5 tells us that $v_F(d)$ is even, which means we can multiply by some even power of π_F to get $v_F(d) = m_1$.

(2) Lemma 8.5 tells us that there is some $a \in F^\times$ such that $\frac{d}{a^2} \equiv 1 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}$, and moreover that there is no such a for any higher power of $\mathfrak{p}_F$. This implies that

$$v_F\left(\frac{d}{a^2} - 1\right) = 2e_F + 1 - m_1,$$

so

$$v_F(d - a^2) = 2e_F + 1.$$

Setting $b = \frac{d-a^2}{4}$, we obtain a, b as required.

(3) It is easy to see that $\rho^2 - a\rho - b = 0$, so the minimal polynomial of ρ over F is Eisenstein, and therefore ρ is a uniformiser of E with $\mathcal{O}_E = \mathcal{O}_F \oplus \mathcal{O}_F \cdot \rho$.

(4) Since $-1 \equiv 1 \pmod{\mathfrak{p}_F^{e_F}}$, we have $v_F(d_{F(\sqrt{-1})/F}) \le e_F + 1$ by Corollary 8.6, so $U_F^{(e_F+1)} \subseteq \operatorname{Nm} F(\sqrt{-1})$, and therefore

$$\frac{d}{a^2} \in U_F^{(2e_F+1-m_1)} \subseteq U_F^{(e_F+1)} \subseteq \operatorname{Nm} F(\sqrt{-1}),$$

which implies that $(-1,d)_F = 1$, and therefore Lemma 8.7 and Corollary 8.8 tell us that we may choose $\omega \in E^\times$ with $N_{E/F}\omega \in dF^{\times 2}$. Moreover, we may ensure that $v_E(\omega) = 0$, since $v_F(d)$ is even.

(5) We know that $N_{E/F}\omega = dx^2$ for some $x \in F^\times$ with $v_F(x) = -m_1/2$. Setting $\lambda = ax$, it is easy to see that $N_{E/F}\omega \equiv \lambda^2 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}$.

(6) We address Step 6 with a sequence of lemmas.

Lemma A.1. *For all $x \in \mathcal{O}_E$, we have $v_F(\operatorname{Tr}_{E/F} x) \geq \frac{m_1}{2}$.*

Proof. This follows easily from the fact that $x = s + t\rho$ for elements $s, t \in \mathcal{O}_F$. □

Lemma A.2. *We have*

$$v_E(\omega - \lambda) \geq m_1 - 1.$$

Proof. Let $\gamma = \omega - \lambda$. Define the sequence $(a_n)_{n\geq 0}$ as follows. Set $a_0 = 0$, and for each $n \geq 0$, define

$$a_{n+1} = \min\Big\{ \Big\lfloor \frac{a_n}{2} \Big\rfloor + \frac{m_1}{2}, 2e_F + 1 - m_1 \Big\}.$$

We claim that $v_E(\gamma) \geq a_n$ for all n. The base case $n = 0$ is clear. Suppose that $v_E(\gamma) \geq a_n$ for some n. Then $\gamma/\pi_F^{\lfloor \frac{a_n}{2} \rfloor} \in \mathcal{O}_E$, so it follows from Lemma A.1 that

$$v_F(\operatorname{Tr}_{E/F} \gamma) \geq \frac{m_1}{2} + \Big\lfloor \frac{a_n}{2} \Big\rfloor.$$

Since $N_{E/F}\omega \equiv \lambda^2 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}$, we have

$$\lambda \operatorname{Tr}_{E/F} \gamma + N_{E/F}\gamma \equiv 0 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}},$$

and it follows that $v_F(N_{E/F}\gamma) \geq a_{n+1}$. Since E/F is totally ramified, we have

$$v_F(N_{E/F}\gamma) = v_E(\gamma),$$

so indeed $v_E(\gamma) \geq a_{n+1}$, and by induction this is true for all n.

It is easy to see that if $a_n < m_1 - 1$, then $a_n < a_{n+1}$, so there is some n with $a_n \geq m_1 - 1$, and therefore $v_E(\gamma) \geq m_1 - 1$, as required. □

Lemma A.2 tells us that ω_1 is well-defined.

Lemma A.3. *The following two statements are true:*

(a) $N_{E/F}\omega_1 = N_{E/F}\omega$.

(b) $\omega_1 \equiv \lambda \pmod{\mathfrak{p}_E^{m_1}}$.

Proof. If $v_E(\omega - \lambda) \geq m_1$, then there is nothing to prove, so let us assume that $v_E(\omega - \lambda) = m_1 - 1$. The first claim follows from that fact that $N_{E/F}\rho = -b$. Write $\gamma = \omega - \lambda$. Since $v_E(\gamma) = m_1 - 1$, we have $\gamma/\pi_F^{m_1/2-1} = u + v\rho$ for elements $u, v \in \mathcal{O}_F$ with $v_F(u) \geq 1$ and $v_F(v) = 0$. We have

$$\begin{aligned} N_{E/F}\omega - \lambda^2 &= \lambda \operatorname{Tr}_{E/F} \gamma + N_{E/F}\gamma \\ &= \lambda \pi_F^{\frac{m_1}{2}-1}(2u + av) + \pi_F^{m_1-2}(u^2 + auv - bv^2) \\ &\equiv \lambda av\pi_F^{\frac{m_1}{2}-1} - bv^2\pi_F^{m_1-2} \pmod{\mathfrak{p}_F^{m_1}}. \end{aligned}$$

We know that $N_{E/F}\omega \equiv \lambda^2 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}$, and $m_1 \leq e_F$, so in fact

$$N_{E/F}\omega \equiv \lambda^2 \pmod{\mathfrak{p}_F^{m_1}},$$

and it follows that

$$\lambda av\pi_F^{-\frac{m_1}{2}} - bv^2\pi_F^{-1} \equiv 0 \pmod{\mathfrak{p}_F}.$$

Since $v_F(v) = 0$, it follows that

$$v \equiv \frac{\lambda a}{b\pi_F^{\frac{m_1}{2}-1}} \pmod{\mathfrak{p}_F},$$

and therefore

$$\gamma \equiv \frac{\lambda a\rho}{b} \pmod{\mathfrak{p}_E^{m_1}},$$

so

$$\omega \equiv \lambda\Big(1 + \frac{a\rho}{b}\Big) \pmod{\mathfrak{p}_E^{m_1}},$$

and it follows that

$$\begin{aligned}\omega_1 &= \frac{\omega b}{\rho^2}\\ &\equiv \lambda\Big(\frac{b}{\rho^2} + \frac{a}{\rho}\Big) \pmod{\mathfrak{p}_E^{m_1}}\\ &= \lambda \cdot \frac{b + a\rho}{\rho^2}\\ &= \lambda.\end{aligned}$$

□

(7) Write $\omega_1 = r_1 + s_1\rho$, for $r_1, s_1 \in \mathcal{O}_F$.

Lemma A.4. *The following two statements are true:*
(a) $v_F(s_1) \geq \frac{m_1}{2}$.
(b) $v_E(\omega_1 - \bar{\omega}_1) = 2v_F(s_1) + m_1$.

Proof. Since $\omega_1 \equiv \lambda \pmod{\mathfrak{p}_E^{m_1}}$, we have

$$(r_1 - \lambda) + s_1\rho \equiv 0 \pmod{\mathfrak{p}_E^{m_1}},$$

so $v_F(s_1) \geq \frac{m_1}{2}$. The second statement is obvious. □

It follows that ω_2 and λ_2 are well-defined and their definitions are equivalent to

$$\omega_2 = \begin{cases}\omega_1 & \text{if } v_F(s_1) = \frac{m_1}{2},\\ \omega_1(1+\rho)^2 & \text{if } v_F(s_1) > \frac{m_1}{2},\end{cases}$$

and

$$\lambda_2 = \begin{cases}\lambda & \text{if } v_F(s_1) = \frac{m_1}{2},\\ \lambda(1+a-b) & \text{if } v_F(s_1) > \frac{m_1}{2}.\end{cases}$$

Write $\omega_2 = r_2 + s_2\rho$.

Lemma A.5. *We have*
(a) $N_{E/F}\omega_2 \equiv \lambda_2^2 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}$.
(b) $\omega_2 \equiv \lambda_2 \pmod{\mathfrak{p}_E^{m_1}}$.
(c) $v_F(s_2) = \frac{m_1}{2}$.

Proof. If $v_F(s_1) = \frac{m_1}{2}$, then this is Lemma A.3, so we will assume that $v_F(s_1) > \frac{m_1}{2}$. The first statement follows from Lemma A.3, along with the fact that $N_{E/F}(1+\rho) = 1+a-b$. It is easy to see that

$$(1+\rho)^2 - N_{E/F}(1+\rho) = (1+\rho)\sqrt{d},$$

so

$$(1+\rho)^2 \equiv 1 + a - b \pmod{\mathfrak{p}_E^{m_1}},$$

and the second statement follows. Since $(1+\rho)^2 = (1+b) + (2+a)\rho$, we have

$$\omega_2 = (1+b)\omega_1 + (2+a)\rho\omega_1,$$

and therefore

$$\bar{\omega}_2 = (1+b)\bar{\omega}_1 + (2+a)\bar{\rho}\bar{\omega}_1,$$

so

$$\omega_2 - \bar{\omega}_2 = (1+b)(\omega_1 - \bar{\omega}_1) + (2+a)(\rho\omega_1 - \bar{\rho}\bar{\omega}_1).$$

We know that $v_E(\omega_1 - \bar{\omega}_1) > 2m_1$, so

$$\omega_2 - \overline{\omega}_2 \equiv (2+a)(\rho\omega_1 - \bar{\rho}\bar{\omega}_1) \pmod{\mathfrak{p}_E^{2m_1+1}}.$$

Since $\omega_1 = r_1 + s_1\rho$, we have

$$\rho\omega_1 - \bar{\rho}\bar{\omega}_1 = (\rho - \bar{\rho})(r_1 + s_1(\rho + \bar{\rho})).$$

It is easy to see that $v_E(\rho - \bar{\rho}) = m_1$. Since $v_E(\omega_1) = 0$, we have $v_E(r_1) = 0$, so

$$v_E(r_1 + s_1(\rho + \bar{\rho})) = 0,$$

and therefore

$$v_E(\rho\omega_1 - \bar{\rho}\bar{\omega}_1) = m_1.$$

It is easy to see that $v_E(2+a) = m_1$, so $v_E(\omega_2 - \overline{\omega}_2) = 2m_1$, and therefore

$$v_F(s_2) = \frac{m_1}{2}.$$

□

(8) We know that $s_2 \neq 0$ since $N_{E/F}\omega_2 \in dF^{\times 2}$, so $\omega_2 \notin F^\times$. Similarly, $v_E(\omega_2) = 0$ so $r_2 \neq 0$. It follows that q and n are well-defined.
(9) Since $q \in F$ and $\rho \notin F$, we have $q + \rho \neq 0$, and therefore the output is well-defined. Since $n \in F^\times$, we have

$$N_{E/F}\Big(\frac{\omega_2 n}{(q+\rho)^2}\Big) \in dF^{\times 2}.$$

Lemma A.6. *We have* $v_F(r_2 - \lambda_2) = \frac{m_1}{2}$.

Proof. We have

$$N_{E/F}\omega_2 = r_2^2 + ar_2s_2 - bs_2^2,$$

so

$$(*) \qquad (r_2^2 - \lambda_2^2) + ar_2s_2 - bs_2^2 \equiv 0 \pmod{\mathfrak{p}_F^{2e_F+1-m_1}}.$$

We know that $v_F(bs_2^2) = m_1 + 1$ and $v_F(ar_2s_2) = m_1$, so Equation $(*)$ implies that

$$v_F(r_2^2 - \lambda_2^2) = m_1.$$

Suppose for a contradiction that $v_F(r_2 - \lambda_2) \geq e_F$. Then $v_F(r_2 + \lambda_2) \geq e_F$, so

$$m_1 = v_F(r_2^2 - \lambda_2^2) \geq 2e_F > e_F,$$

contradicting the fact that $m_1 \leq e_F$. Therefore, we have $v_F(r_2 - \lambda_2) < e_F$, and consequently $v_F(r_2 + \lambda_2) = v_F(r_2 - \lambda_2)$, so the result follows. □

We also have

$$
\begin{aligned}
\omega_2 n - (q+\rho)^2 &= (b-\rho^2) + \frac{\rho b s_2}{r_2} - q\rho\frac{\lambda_2 + r_2}{r_2} \\
&= (b-\rho^2) + \frac{\rho b s_2}{r_2} + \rho\frac{\lambda_2^2 - r_2^2}{r_2 s_2} \\
&= \frac{\rho}{r_2 s_2}\big(\lambda_2^2 - r_2^2 + \frac{r_2 s_2}{\rho}(b-\rho^2) + b s_2^2\big) \\
&= \frac{\rho}{r_2 s_2}(\lambda_2^2 - r_2^2 + b s_2^2 - a r_2 s_2) \\
&= \frac{\rho}{r_2 s_2}(\lambda_2^2 - N_{E/F}\omega_2).
\end{aligned}
$$

Since $v_E(r_2) = 0$ and $v_E(s_2) = m_1$, we have $v_E(\frac{\rho}{r_2 s_2}) = 1 - m_1$. Since

$$v_E(\lambda_2^2 - N_{E/F}\omega_2) \geq 4e_F + 2 - 2m_1,$$

it follows that

$$\omega_2 n \equiv (q+\rho)^2 \pmod{\mathfrak{p}_E^{4e_F+3-3m_1}}.$$

Lemmas A.5 and A.6 tell us that $v_F(q) = 0$, and therefore $v_E(q+\rho) = 0$, so it follows that

$$\frac{\omega_2 n}{(q+\rho)^2} \equiv 1 \pmod{\mathfrak{p}_E^{4e_F+3-3m_1}}.$$

Theorem 13.29 then follows by Lemma 8.3 and Lemma 8.5.

Appendix B. Explicit helper functions

- Let p be an integer with $p \geq 2$, and let q be a positive rational number. For integers t with $t \geq 2$, define the functions $A(t)$ and $B(t)$ by

$$A(t) = \begin{cases} q^{1-\lfloor\frac{t}{2}\rfloor} \cdot \frac{q^{\lfloor\frac{t}{2}\rfloor}-1}{q-1} & \text{if } p = 2, \\ q^{-p(p-2)} \cdot \frac{q^{(p-1)(p-2)}-1}{q^{p-2}-1} \cdot \frac{q^{-(p-1)^2\cdot\lfloor\frac{t}{p}\rfloor}-1}{q^{-(p-1)^2}-1} & \text{if } p \neq 2, \end{cases}$$

and

$$B(t) = \begin{cases} 0 & \text{if } p = 2, \\ q^{-\lfloor\frac{t}{p}\rfloor} \cdot \frac{q^{-(p-2)(t+1)}-q^{-(p-2)(\lfloor\frac{t}{p}\rfloor p+2)}}{q^{-(p-2)}-1} & \text{if } p \neq 2. \end{cases}$$

- Define the explicit function $N^{\neq}_{(1^21^2)}$ by

$$N^{\neq}_{(1^21^2)}(m) = \begin{cases} 2(q-1)^2 q^{\frac{m}{2}-2}(\frac{m}{2}-1) - \mathbb{1}_{4\mid m}(q-1)q^{\frac{m}{4}-1} & \text{if } 4 \leq m \leq 2e_F \text{ and } m \text{ is even,} \\ 2(q-1)^2 q^{\frac{m}{2}-2}(2e_F - \frac{m}{2}+1) - \mathbb{1}_{4\mid m}(q-1)q^{\frac{m}{4}-1} & \text{if } 2e_F + 2 \leq m \leq 4e_F \text{ and } m \text{ is even,} \\ 4(q-1)q^{\frac{m-1}{2}-1} & \text{if } 2e_F + 3 \leq m \leq 4e_F + 1 \text{ and } m \text{ is odd,} \\ q^{e_F}(2q^{e_F}-1) & \text{if } m = 4e_F + 2, \\ 0 & \text{otherwise.} \end{cases}$$

- For even integers m_1 with $2 \leq m_1 \leq 2e_F$, define

$$N_{\text{ext}}(m_1) := (1 + \mathbb{1}_{m_1 \leq 2e_F - d_{(-1)}})q^{\frac{m_1}{2}-1}(q - 1 - \mathbb{1}_{m_1 = 2e_F - d_{(-1)}+2}).$$

For $m_1 = 2e_F + 1$, define

$$N_{\text{ext}}(2e_F+1) = \begin{cases} 2q^{e_F} & \text{if } -1 \in F^{\times 2}, \\ q^{e_F} & \text{if } F(\sqrt{-1})/F \text{ is quadratic and totally ramified,} \\ 0 & \text{if } F(\sqrt{-1})/F \text{ is quadratic and unramified.} \end{cases}$$

Set $N_{\text{ext}}(m_1) = 0$ for all other real numbers m_1.

- For each integer m_2, define

$$N^{C_2}(m_2) = \begin{cases} 2(q-1)q^{\frac{m_2}{2}-1} & \text{if } 0 \le m_2 \le 4e_F \text{ and } m_2 \text{ is even,} \\ 2q^{2e_F} & \text{if } m_2 = 4e_F + 1, \\ 0 & \text{otherwise.} \end{cases}$$

- Let m_1 be an even integer with $2 \le m_1 \le e_F$. For each integer m_2, define

$$N^{C_4}(m_1, m_2) = \begin{cases} q^{m_1-1} & \text{if } m_2 = 3m_1 - 2, \\ q^{\lfloor \frac{m_1+m_2}{4} \rfloor} - q^{\lfloor \frac{m_1+m_2-2}{4} \rfloor} & \text{if } 3m_1 \le m_2 \le 4e_F - m_1 \text{ and } m_2 \text{ is even,} \\ q^{e_F} & \text{if } m_2 = 4e_F - m_1 + 2, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $m_1 = 2e_F + 1$ or m_1 is even with $e_F < m_1 \le 2e_F$. Then define

$$N^{C_4}(m_1, m_2) = \begin{cases} 2q^{e_F} & \text{if } m_2 = m_1 + 2e_F, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, define $N^{C_4}(m_1, m_2) = 0$ for all other pairs of integers (m_1, m_2).

- Let m_1 be either $2e_F + 1$ or an even integer with $2 \le m_1 \le 2e_F$. Define

$$N^{V_4}(m_1, m_2) = \begin{cases} 2(q-1)q^{\frac{m_2}{2}-1} & \text{if } 2 \le m_2 < m_1 \text{ and } m_2 \text{ is even,} \\ (q-2)q^{\frac{m_1}{2}-1} & \text{if } m_2 = m_1 \text{ and } m_1 \text{ is even,} \\ (q-1)q^{\frac{m_1+m_2}{4}-1} & \text{if } m_1 < m_2 \le 4e_F - m_1 \text{ and } m_1 \equiv m_2 \pmod 4, \\ q^{e_F} & \text{if } m_2 > m_1 \text{ and } m_1 + m_2 = 4e_F + 2, \\ 0 & \text{otherwise.} \end{cases}$$

Define $N^{V_4}(m_1, m_2) = 0$ for all other pairs of integers (m_1, m_2).

References

[AMS15] C. Awtrey, N. Mistry, and N. Soltz. “Centralizers of transitive permutation groups and applications to Galois theory”. In: *Missouri Journal of Mathematical Sciences* 27.1 (2015), pp. 16–32.

[AT68] E. Artin and J.T. Tate. *Class Field Theory*. AMS Chelsea publishing. American Mathematical Soc., 1968. ISBN: 9780821869512. URL: https://books.google.co.uk/books?id=8odbx9-9HBMC.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125.

[Bha04] M. Bhargava. “Higher composition laws. III. The parametrization of quartic rings”. In: *Annnals of Mathematics* 159.3 (2004), pp. 1329–1360. ISSN: 0003-486X. DOI: 10.4007/annals.2004.159.1329. URL: https://doi.org/10.4007/annals.2004.159.1329.

[Bha05] M. Bhargava. “The Density of Discriminants of Quartic Rings and Fields”. In: *Annals of Mathematics* 162.2 (2005), pp. 1031–1063. ISSN: 0003486X. URL: http://www.jstor.org/stable/20159935 (visited on 11/03/2024).

[Bha07] M. Bhargava. “Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants”. In: *Int. Math. Res. Not. IMRN* 17 (2007), Art. ID rnm052, 20. ISSN: 1073-7928. DOI: 10.1093/imrn/rnm052. URL: https://doi.org/10.1093/imrn/rnm052.

[Bha08] M. Bhargava. “Higher composition laws IV: The parameterization of quintic rings”. English (US). In: *Annals of Mathematics* 167.1 (Jan. 2008), pp. 53–94. ISSN: 0003-486X. DOI: 10.4007/annals.2008.167.53.

[Bha10] M. Bhargava. “The density of discriminants of quintic rings and fields”. In: *Annals of Mathematics* 172.3 (2010), pp. 1559–1591. ISSN: 0003486X. URL: http://www.jstor.org/stable/29764652 (visited on 11/03/2024).

[BJ20] A. Bartel and H.W. Lenstra Jr. “On class groups of random number fields”. In: *Proceedings of the London Mathematical Society* 121.4 (2020), pp. 927–953. DOI: https://doi.org/10.1112/plms.12343. eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms.12343. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms.12343.

[Bro05] T. Browning. “An overview of Manin’s conjecture for del Pezzo surfaces”. In: *Analytic Number Theory* 7 (Dec. 2005).

[BS10] M. Bhargava and A. Shankar. “Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves”. In: *Annals of Mathematics* 181 (June 2010). DOI: 10.4007/annals.2015.181.1.3.

[BS13a] M. Bhargava and A. Shankar. “The average number of elements in the 4-Selmer groups of elliptic curves is 7”. In: *arXiv* (2013). eprint: 1312.7333 (math.NT). URL: https://arxiv.org/abs/1312.7333.

[BS13b] M. Bhargava and A. Shankar. “The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1”. In: *arXiv* (2013). eprint: 1312.7859 (math.NT). URL: https://arxiv.org/abs/1312.7859.

[BS15] M. Bhargava and A. Shankar. “Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0”. In: *Annals of Mathematics* 181.2 (2015), pp. 587–621. ISSN: 0003486X. URL: http://www.jstor.org/stable/24522944 (visited on 04/26/2025).

[BST13] M. Bhargava, A. Shankar, and J. Tsimerman. “On the Davenport-Heilbronn theorems and second order terms”. English (US). In: *Inventiones Mathematicae* 193.2 (Aug. 2013), pp. 439–499. ISSN: 0020-9910. DOI: 10.1007/s00222-012-0433-0.

[BSW15] M. Bhargava, A. Shankar, and X. Wang. “Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces”. In: *arXiv* (2015). eprint: 1512.03035 (math.NT). URL: https://arxiv.org/abs/1512.03035.

[BT22] A. Burungale and Y. Tian. “The even parity Goldfeld conjecture: Congruent number elliptic curves”. In: *Journal of Number Theory* 230 (2022). Proceedings of the First JNT Biennial Conference 2019, pp. 161–195. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2021.05.001. URL: https://www.sciencedirect.com/science/article/pii/S0022314X21001773.

[BW07] M. Bhargava and M. Wood. “The density of discriminants of S_3-sextic number fields”. In: *Proceedings of The American Mathematical Society - PROC AMER MATH SOC* 136 (May 2007), pp. 1581–1588. DOI: 10.1090/S0002-9939-07-09171-X.

[CDO05] H. Cohen, F. Diaz y Diaz, and M. Olivier. “Counting cyclic quartic extensions of a number field”. In: *Journal de Théorie des Nombres de Bordeaux* 17.2 (2005), pp. 475–510. ISSN: 12467405, 21188572. URL: http://www.jstor.org/stable/43974348 (visited on 02/21/2023).

[CL84] H. Cohen and H. W. Lenstra. “Heuristics on class groups of number fields”. In: *Number Theory Noordwijkerhout 1983*. Ed. by Hendrik Jager. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984, pp. 33–62. ISBN: 978-3-540-38906-4.

[Dab01] M. Daberkow. “On Computations in Kummer Extensions”. In: *Journal of Symbolic Computation* 31.1 (2001), pp. 113–131. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.2000.1013. URL: https://www.sciencedirect.com/science/article/pii/S0747717100910137.

[Dal10] C.S. Dalawat. *Final remarks on local discriminants.* 2010. eprint: 0912.2829 (math.NT). URL: https://arxiv.org/abs/0912.2829.

[DF64] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree.* Vol. 10. American Mathematical Society, 1964.

[DH71] H. Davenport and H. Heilbronn. “On the Density of Discriminants of Cubic Fields. II”. In: *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* 322.1551 (1971), pp. 405–420. ISSN: 00804630. URL: http://www.jstor.org/stable/77760 (visited on 11/01/2024).

[FLN22] C. Frei, D. Loughran, and R. Newton. “Number fields with prescribed norms”. In: *Comment. Math. Helv.* 97.1 (2022). With an appendix by Y. Harpaz and O. Wittenberg, pp. 133–181. ISSN: 0010-2571. DOI: 10.4171/cmh/528. URL: https://doi.org/10.4171/cmh/528.

[glS] Mathematics StackExchange user glS. “How to find a basis for the intersection of two vector spaces in $\mathbb{R}^n$?” In: (). URL:https://math.stackexchange.com/q/3322086 (version: 2023-05-21). eprint: https://math.stackexchange.com/q/3322086. URL: https://math.stackexchange.com/q/3322086.

[Gol79] D. Goldfeld. “Conjectures on elliptic curves over quadratic fields”. In: (1979). Ed. by Melvyn B. Nathanson, pp. 108–118. DOI: 10.1007/BFb0062705. URL: https://doi.org/10.1007/BFb0062705.

[J F89] J. Franke, Y.I. Manin., Y. Tschinkel. “Rational points of bounded height on Fano varieties.” In: *Inventiones mathematicae* 95.2 (1989), pp. 421–436. URL: http://eudml.org/doc/143659.

[Ked07] K.S. Kedlaya. “Mass Formulas for Local Galois Representations (with an Appendix by Daniel Gulotta)”. In: *International Mathematics Research Notices* 2007 (Jan. 2007), rnm021. ISSN: 1073-7928. DOI: 10.1093/imrn/rnm021. eprint: https://academic.oup.com/imrn/article-pdf/doi/10.1093/imrn/rnm021/1943241/rnm021.pdf. URL: https://doi.org/10.1093/imrn/rnm021.

[Keu23] F. Keune. *Number Fields.* Radboud University Press, 2023. URL: http://www.jstor.org/stable/jj.1666828.

[Kra66] M. Krasner. “Nombre des extensions d’un degré donné d’un corps p-adique”. In: *Les Tendances Géom. en Algèbre et Théorie des Nombres, Editions du Centre National de la Recherche Scientifique* 143 (Jan. 1966).

[Lbe09] A. Lbekkouri. “On the construction of normal wildly ramified extensions over $\mathbb{Q}_2$”. In: *Archiv der Mathematik* 93 (Oct. 2009), pp. 235–243. DOI: 10.1007/s00013-009-0024-5.

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database.* https://www.lmfdb.org. [Online; accessed 29 May 2023]. 2023.

[Mil22] J. S. Milne. *Fields and Galois Theory.* Ann Arbor, MI: Kea Books, 2022. ISBN: 979-8218073992.

[Neu13] J. Neukirch. *Class field theory.* The Bonn lectures, edited and with a foreword by A. Schmidt, Translated from the 1967 German original by F. Lemmermeyer and W. Snyder, Language editor: A. Rosenschon. Springer, Heidelberg, 2013, pp. xii+184.

ISBN: 978-3-642-35436-6; 978-3-642-35437-3. DOI: 10.1007/978-3-642-35437-3. URL: https://doi.org/10.1007/978-3-642-35437-3.

[NS13] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013. ISBN: 9783662039830. URL: https://books.google.co.uk/books?id=hS3qCAAAQBAJ.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*. Vol. 323. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2000, pp. xvi+699. ISBN: 3-540-66671-0.

[Pey95] E. Peyre. "Hauteurs et mesures de Tamagawa sur les variétés de Fano". In: *Duke Mathematical Journal* 79.1 (1995), pp. 101–218. DOI: 10.1215/S0012-7094-95-07904-6. URL: https://doi.org/10.1215/S0012-7094-95-07904-6.

[PR01] S. Pauli and X.F. Roblot. "On the computation of all extensions of a p-adic field of a given degree". In: *Math. Comp.* 70.236 (2001), pp. 1641–1659. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-01-01306-0. URL: https://doi.org/10.1090/S0025-5718-01-01306-0.

[PS15] S. Pauli and B. Sinclair. "Enumerating Extensions of (π)-Adic Fields with Given Invariants". In: *arXiv* (2015). DOI: 10.48550/ARXIV.1504.06671. URL: https://arxiv.org/abs/1504.06671.

[Ser78] J.P. Serre. "Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local". In: *C. R. Acad. Sci. Paris Sér. A-B* 286.22 (1978), A1031–A1036. ISSN: 0151-0509.

[Ser95] J.P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995. ISBN: 9780387904245. URL: https://books.google.co.uk/books?id=DAxlMdw%5C_QloC.

[Sin15] B. Sinclair. "Counting Extensions of $\mathfrak{p}$-Adic Fields with Given Invariants". In: *arXiv* (2015). DOI: 10.48550/ARXIV.1512.06946. URL: https://arxiv.org/abs/1512.06946.

[Tun78] J.B. Tunnell. "On the local Langlands conjecture for $GL(2)$". In: *Invent. Math.* 46.2 (1978), pp. 179–200. ISSN: 0020-9910. DOI: 10.1007/BF01393255. URL: https://doi.org/10.1007/BF01393255.

[Vos88] V. E. Voskresenskii. "Maximal tori without affect in semisimple algebraic groups". In: *Mat. Zametki* 44.3 (1988), pp. 309–318, 410. ISSN: 0025-567X. DOI: 10.1007/BF01159125. URL: https://doi.org/10.1007/BF01159125.

[Was97] L.C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 1997. ISBN: 9780387947624. URL: https://books.google.co.uk/books?id=qea_0XafBFoC.

[WJ07] D.S. Wei and C.G. Ji. "On the Number of Certain Galois Extensions of Local Fields". In: *Proceedings of the American Mathematical Society* 135.10 (2007), pp. 3041–3047. ISSN: 00029939, 10886826. URL: http://www.jstor.org/stable/20534923 (visited on 05/19/2023).

[Woo16] M. M. Wood. "Asymptotics for Number Fields and Class Groups". In: *Directions in Number Theory*. Ed. by E. E. Eischen et al. Cham: Springer International Publishing, 2016, pp. 291–339. ISBN: 978-3-319-30976-7.

[WY15] M.M. Wood and T. Yasuda. "Mass Formulas for Local Galois Representations and Quotient Singularities. I: A Comparison of Counting Functions". In: *International Mathematics Research Notices* 2015.23 (Mar. 2015), pp. 12590–12619. ISSN: 1073-7928. DOI: 10.1093/imrn/rnv074. eprint: https://academic.oup.com/imrn/article-pdf/2015/23/12590/1962988/rnv074.pdf. URL: https://doi.org/10.1093/imrn/rnv074.