Volumes of Integer Polynomials over Local Fields

A Thesis
Presented to
The Division of Mathematics and Natural Sciences
Reed College

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Arts

Asher N. Auel

May 2003

Approved for the Division
(Mathematics)

Joe P. Buhler

Acknowledgments

Most of all, I would like to thank my two greatest inspirations and role models of this past year: my best friend Jesse Johnson and my thesis adviser Joe Buhler.

Second, I would like to thank Ray Mayer, one of my favorite professors and dearest friends, who helped inspire me to become a mathematician, and who was willing to really challenge me mathematically throughout my time here at Reed. He also unselfishly helped me an enormous amount on this current work. I also commend him for inspiring in us the love of "pretty" and "ugly" pictures, and for making the distinction clear between them.

I would like to acknowledge the absolutely important role my family has and will continue to have in my life. Though at times they are bewildered by my mathematical endeavors, without their constant and undying support, I would have never made it this far. I love you all immensely.

I thank Billy Holloway, Scott Blais, and friends, for their generous spirits, and for having open enough minds to accept and make room for a mathematician among their ranks as artists. I thank Lara Sands, not only for being the greatest dance partner ever, but for applying her expert legal copy editing skills to my much appreciative thesis. Lastly, I would like to thank Amanda Lucier for helping me through my final thesis week and night.

Contents

Introduction **1**

1 Introduction to Local Fields **5**
1.1 Discrete Valuation Fields 5
1.2 Haar Measure 9
1.3 Extensions of Local Fields 11
1.4 Quadratic Extensions of $\mathbb{Q}_p$ 16
1.5 Étale Algebras 18

2 Quadratic Volume Computations **21**
2.1 Completely Split Quadratic Polynomials 21
2.2 Irreducible Polynomials 22
2.3 Visualizing Quadratic Polynomials over $\mathbb{Q}_p$ 24

3 Cubic Volume Computations **33**
3.1 Cubic Polynomials in General 33
3.2 Explicit Computations for Cubics over $\mathbb{Q}_p$ 35

4 General Volume Computations **43**
4.1 The Index Form of an Algebraic Extension 44
4.2 Serre's "mass formula" 48
4.3 Completely Split Polynomials 49
4.4 Unramified Extensions 56

A Glossary of Terms **61**

Bibliography **63**

List of Tables

2.1 Volumes for Quadratic Étale Algebras over $\mathbb{Q}_p$ 24

3.1 Index Forms of Quadratic and Cubic Étale Algebras 35
3.2 Generating Polynomials of Cubic Extensions of $\mathbb{Q}_3$ 37
3.3 Volumes for Cubic Étale Algebras over $\mathbb{Q}_p$ 41

4.1 Volumes for Completely Split Polynomials 52
4.2 Volumes for Unramified Extensions 60

List of Figures

1.1 Ramification Index and Residue Degree 12
1.2 Quadratic Extensions of $\mathbb{Q}_p$ 17

2.1 Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_2$ . . . 25
2.2 Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_3$ . . . 27
2.3 Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_5$ . . . 28
2.4 Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_7$ . . . 29
2.5 Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_{11}$ . . . 30
2.6 Detail of Picture 2.3 for $\mathbb{Q}_5$ 31
2.7 Detail of Picture 2.4 for $\mathbb{Q}_7$ 32

Abstract

Let F be a non-Archimedean local field of characteristic 0, complete with respect to a discrete valuation, with finite residue field, and ring of integers $\mathcal{O}_F$. The coefficient-wise identification of monic degree n polynomials $f \in \mathcal{O}_F[x]$ with points in $\mathcal{O}_F^n$ defines a natural volume (the normalized Haar measure) on this set of polynomials. For a given extension K of F, and more generally, for a given étale algebra over F, we wish to compute the volume of polynomials which generate K over F. Generalizing methods of Serre in [18], we find this volume in the case of quadratic extensions, unramified extensions, and in the case of polynomials which split completely over F, i.e. factor into linear terms. We also find these volumes for all quadratic and cubic étale algebras over the field of p-adic numbers $\mathbb{Q}_p$.

Introduction

Imagine looking at a chocolate mousse pie, but not one which has been cut up into the canonical thick slices radiating out from the center, but into lots of small triangles and squares like an abstract painting. Seeing such a pie, one might want to study the division more closely and wonder at its origin. In this work we are handed a naturally cut pie and ask for the area of each piece. The motivation for such a project could be the elegant pie piece formula discovered by French mathematician Jean-Pierre Serre, and after which much of this work is inspired, or we might just be intrinsically interested in such a question. Here is our pie: the space of polynomials with integer coefficients; x^2+3x+6 and x^2-2 are two examples. Polynomials are just strings of powers of an indeterminate x with integers (called coefficients) hung on each one. We may think of them as formal clotheslines for integers, or as functions (if we substitute numbers for x). A *root* of a polynomial is a number α, which when substituted for x in the polynomial gives 0. Here we have a division: each slice of the pie corresponds to the collection of polynomials whose roots generate a given extension of our chosen field of numbers.

What do I mean by that? Roots don't generally sit in the same field of numbers as the coefficients of their polynomials. To give an example, if we choose our coefficients from the field of rational numbers $\mathbb{Q}$, then it was already known by the 5^{th} century Greek mathematician Theodorus of Cyrene that the root of the polynomial x^2-2, namely the square root of 2, is not a rational number – it's *irrational*![1] We don't just leave it there. If $\sqrt{2}$ does not live with the rational numbers then it lives somewhere, no doubt. We call this place the *extension* of $\mathbb{Q}$ generated by $\sqrt{2}$ or simply $\mathbb{Q}(\sqrt{2})$. It is the smallest reasonable set of numbers which contains both the rational numbers $\mathbb{Q}$ and $\sqrt{2}$. We think of $\mathbb{Q}(\sqrt{2})$ as *over* or *covering* the field $\mathbb{Q}$ and we express this pictorially as:

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}) \\ 2\Big| \\ \mathbb{Q} \end{array}$$

where the 2 in the diagram indicates that the polynomial, of which $\sqrt{2}$ is a root, has degree 2 or is *quadratic*.

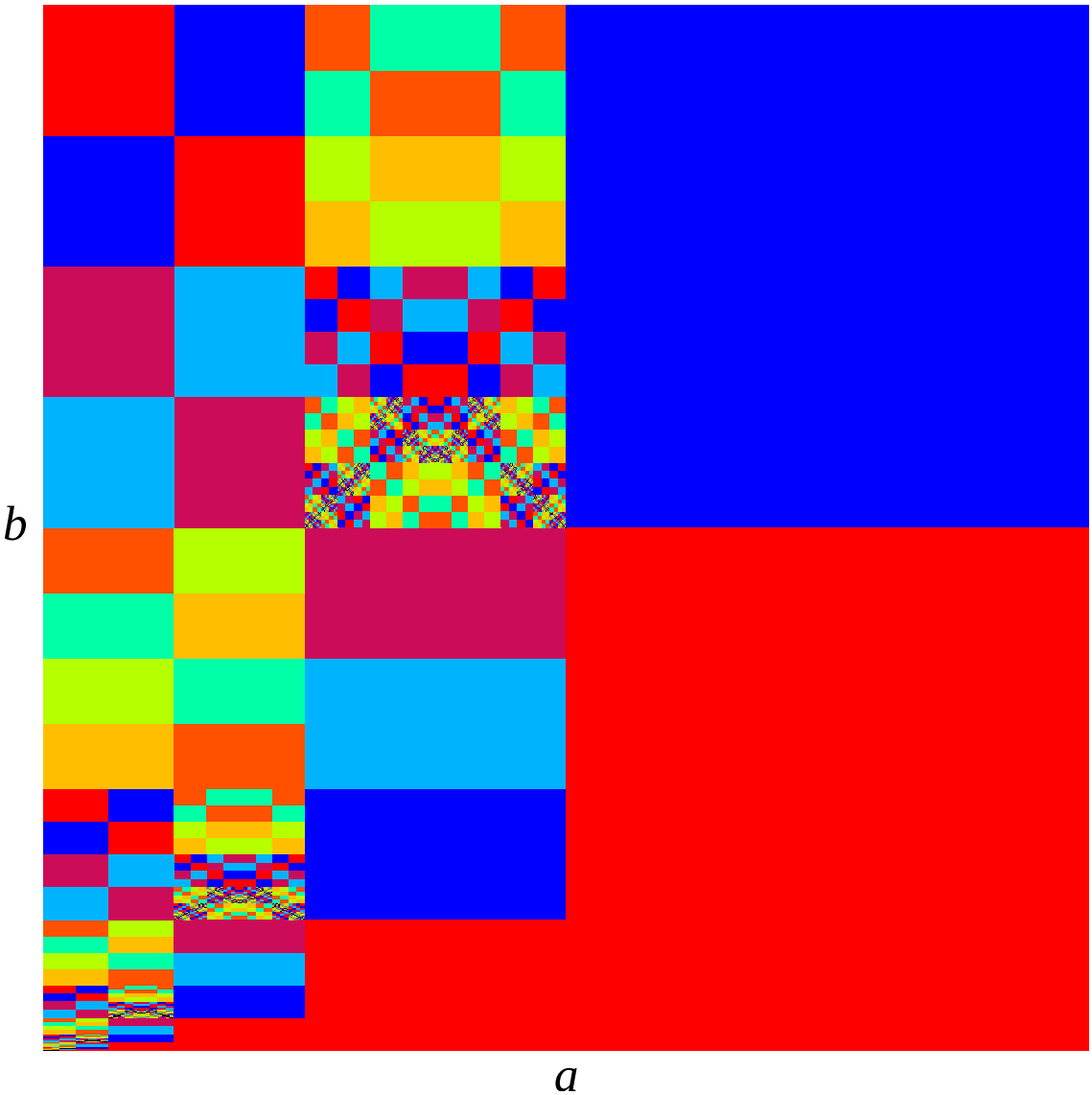
So now we want to cut up the set of quadratic polynomials with integer coefficients into slices according to which extension its roots generate. One problem here is that there are an infinite number of different extensions over the rational numbers

[1] see Plato, *Theaetetus*, 147d.

$\mathbb{Q}$, i.e. an infinite number of slices. Furthermore, there is no nice way to *measure* the various slices of the pie.

Our question is still well posed, we are just choosing the wrong field of numbers. In the following, we work over a "local" field of numbers F, where our question is a natural one. In fact there are now only a finite number of pieces to the polynomial pie, and there is an intrinsic notion of measurement on our pie called the *Haar measure*.

To give an example, the field of 2-adic numbers $\mathbb{Q}_2$ (defined in Section 1.1) is a local field, and there turn out to be 8 pieces to its quadratic pie, i.e. there are precisely 8 different flavors of extensions.[2] The following picture actually shows the pie with the 8 slices color coded.



Which flavor of root does $x^2 + ax + b$ have?

[2]This is a bit of a lie, there are actually 7 flavors of extensions, and one "split" polynomial case.

From now on, we will work strictly with *monic* polynomials, i.e. ones whose coefficient on the highest power of x is 1. Here is how the picture works: the general monic quadratic polynomial looks like

$$x^2 + ax + b,$$

where the numbers a and b are now 2-adic integers. To specify such a polynomial we only need to give a pair of integers (a, b), and conversely, any pair of integers (a, b) specifies such a polynomial:

$$x^2 + ax + b \quad \leftrightarrow \quad (a, b).$$

Thus we can think of the monic quadratic polynomials as living on a Cartesian plane, where a is the coordinate in the horizontal direction, and b is the coordinate in the vertical direction. The above picture is a representation of that plane. For further details, see Section 2.3.

This thesis is an attempt to answer the question, "If the total pie has area 1, how much area does each piece have?" We will discover, among other things, that in the above picture, the red and blues pieces each have area $\frac{1}{3}$, the magenta and light blue pieces each have area $\frac{1}{12}$, and the orange and green pieces only get area $\frac{1}{24}$ each.

Specifically, let F be a non-Archimedean local field complete with respect to a discrete valuation and with finite residue field. We will also assume throughout that our field has characteristic 0. We follow some of J.-P. Serre's techniques in his 1968 paper [18], where he derives his elegant "mass formula" for totally ramified extensions of local fields. Though Serre briefly notes that his methods hold for both the mixed and equi-characteristic cases, we have not sufficiently experimented with the positive characteristic case to be sure. Since our inspiration and examples are derived from the field of p-adic numbers $\mathbb{Q}_p$, we will err on the side of caution and only state our results for characteristic 0 local fields, though we expect that they hold in both cases.

Let F be such a local field with ring of integers $\mathcal{O}_F$. Under the coefficient mapping

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \mapsto (a_1, \ldots, a_n) \in \mathcal{O}_F^n,$$

the set of monic polynomials of degree n and with coefficients in $\mathcal{O}_F$ inherits the normalized product Haar measure from the compact group $\mathcal{O}_F$. Given an étale algebra A, i.e. a finite direct sum of field extensions, we find the volume of polynomials which generate this algebra over F, call this $m_F(A)$, in a number of cases.

Chapter 1 is an introduction to local fields, with special emphasis on algebraic extensions and their generating polynomials, Haar measure, Hensel's lemma, and étale algebras. The bulk of this chapter is meant as a reminder. In it, we will state most of the definitions and theorems assumed throughout this work. In principle, one could follow this chapter with just a little field theory and the ability to take a fair amount on faith.

Chapter 2 deals with general quadratic étale algebras A of a local field F (i.e. A is a quadratic extension or the algebra F^2). We find that the volume $m_F(A)$ is a

simple function of D_A, the discriminant of A, (see Definition 43 for D_A when A is a general étale algebra).

Theorem 45. Let F be a local field with residue field of order q, and let A be a quadratic étale algebra over F. Then we have,

$$m_F(A) = \frac{1}{2}\frac{1}{q^{d(A)}}\frac{q}{q+1},$$

where $d(A) = v_F(D_A)$ is the valuation of the discriminant of A over F. Thus we have the following identity,

$$\sum_A \frac{1}{2}\frac{1}{q+1}\frac{1}{q^{d(A)-1}} = 1,$$

where the sum is over all quadratic étale algebras A over F inside a fixed separable closure of F.

We also classify the quadratic extensions K of $\mathbb{Q}_p$, give the explicit numbers $m_{\mathbb{Q}_p}(K)$ in Table 2.1, and show more pretty pictures like the one above.

Chapter 3 deals with general cubic étale algebras of a local field F. We introduce the *index form* of an étale algebra A, and show how it can be used to calculate $m_F(A)$, though this direct method gets increasingly difficult as the degree of the algebra goes up. We classify the cubic algebras and compute the volumes explicitly for $\mathbb{Q}_p$, see Table 3.3.

In Chapter 4 we find a recursion for the volume of polynomials of degree n that split completely over F, i.e. that generate the étale algebra F^n.

Theorem 53. Let F be a local field with residue field of order q, then we have the recursion,

$$m_F(F^n) = \sum_{\lambda} \prod_{k=1}^{q} q^{-\binom{\lambda_k+1}{2}} m_F(F^{\lambda_k}),$$

where the sum is over all $\lambda = (\lambda_1, \ldots, \lambda_q) \in \mathbb{N}^q$ such that $\lambda_1 + \cdots + \lambda_q = n$, and where $m_F(F^0) = 1$ by definition and $m_F(F^1) = 1$ holds trivially.

In Theorem 54, we find a recursion for the volume $m_F(K)$ when K is an unramified extension of F. We also give tables (Tables 4.1, 4.2) of these numbers as rational functions in q, and note that they have special factorizations in terms of cyclotomic polynomials Φ_n and the polynomials $\phi_n = q^n - 1$. We also describe asymptotic results for both cases.

Chapter 1

Introduction to Local Fields

1.1 Discrete Valuation Fields

Definition 1. Let F be a field. Then a *discrete valuation* on F is a map $v : F^* \to \mathbb{Z}$ (or to any discrete subgroup of $\mathbb{Q}$ isomorphic to $\mathbb{Z}$) with the following properties,

$$\begin{aligned} &v(ab) = v(a) + v(b), \quad \text{for all } a, b \in F^*, \\ &v(a+b) \geq \min(v(a), v(b)), \quad \text{for all } a, b \in F^*. \end{aligned}$$

We make the convention that v is defined on F by setting $v(0) = \infty$, where the symbol ∞ obeys the reasonable formal properties $n \leq \infty$, $\infty \leq \infty$, $n + \infty = \infty$, and $\infty + \infty = \infty$ for all $n \in \mathbb{Z}$. Note that the function $a \mapsto 1$ for all $a \in F^*$ is always a discrete valuation, called the trivial valuation. Call a field F a *discrete valuation field* if it admits a nontrivial discrete valuation.

In fact, a discrete valuation v on a field F satisfies the stronger property,

$$v(a) \neq v(b) \quad \Rightarrow \quad v(a+b) = \min(v(a), v(b)).$$

To see this, first note that

$$v(1) = v(1 \cdot 1) = v(1) + v(1) \quad \Rightarrow \quad v(1) = 0,$$

and similarly $v(-1) = 0$. Thus for any $a \in F^*$,

$$v(-a) = v(-1) + v(a) = v(a).$$

Now let $a, b \in F$ with $v(a) < v(b)$, then

$$v(a+b) \geq \min(v(a), v(b)) = v(a) = v(a+b-b) \geq \min(v(a+b), v(b)),$$

and thus in fact, $v(a+b) = v(a)$.

Definition 2. Let F be a discrete valuation field with valuation v. Define

$$\begin{aligned} \mathcal{O}_F &= \{a \in F : v(a) \geq 0\} \\ \mathfrak{p}_F &= \{a \in F : v(a) > 0\} \end{aligned}$$

suppressing the dependence on v when it is clear.

Example 3. For any prime number p, the rational numbers $\mathbb{Q}$ form a discrete valuation field with valuation $v_p : \mathbb{Q}^* \to \mathbb{Z}$ defined by the relation

$$r = \pm \prod_p p^{v_p(r)} \in \mathbb{Q},$$

where the product is the unique prime factorization of r taken over all primes, i.e. $v_p(r)$ is the number of times p divides r. Then

$$\mathcal{O}_{\mathbb{Q}} = \left\{ \frac{a}{b} p^n \in \mathbb{Q} : \gcd(a,p) = \gcd(b,p) = 1,\ n \in \mathbb{N} \right\}.$$

Example 4. Let p be a prime number. The field $\mathbb{Q}_p$ of *p-adic numbers* consists of all formal power series in p,

$$a = \sum_{n=-\infty}^{\infty} a_n p^n, \quad a_n \in \{0, \ldots, p-1\},$$

which are Laurent series, i.e. $a_n = 0$ for all but finitely many negative values of $n \in \mathbb{Z}$. Then $\mathbb{Q}_p$ is a discrete valuation field with valuation $v_p = \mathrm{ord}_p : \mathbb{Q}_p^* \to \mathbb{Z}$, defined by $v_p(a) = \min\{n \in \mathbb{Z} : a_n \neq 0\}$. Then $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$, the set of *p-adic integers* and $\mathfrak{p}_{\mathbb{Q}_p} = p\mathbb{Z}_p$.

Example 5. Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients in k. Then $k(x)$ is a discrete valuation field with valuation the degree function $\deg : k[x]^* \to \mathbb{Z}$, extended to $k(x)$ by

$$\deg(f(x)/g(x)) = \deg(f(x)) - \deg(g(x)), \quad \text{for all } f(x), g(x) \in k[x], g(x) \neq 0.$$

Then $\mathcal{O}_{k(x)} = k[x]$ and $\mathfrak{p}_{k(x)}$ is the set of polynomials with zero constant coefficient.

For every irreducible polynomial $p(x) \in k[x]$, the field $k(x)$ also has a valuation $v_{p(x)}$, defined by the relation

$$f(x) = a \prod_{p(x)} p(x)^{v_{p(x)}(f(x))} \in k(x),$$

for some $a \in F$, and where the product is the unique irreducible factorization of $f(x)$ taken over all monic (leading coefficient is 1) irreducible polynomials $p(x) \in k[x]$. In this case,

$$\mathcal{O}_{k(x)} = \left\{ \frac{f(x)}{g(x)} p(x)^n \in k(x) : f(x), g(x) \in k[x] \text{ have no factors of } p(x),\ n \in \mathbb{N} \right\}.$$

Example 6. Let $\mathcal{M}$ be the field of complex analytic functions on a deleted neighborhood A of $a \in \mathbb{C}$. We identify $\mathcal{M}$ with $\mathbb{C}((x-a))$ by writing $f \in \mathcal{M}$ as its Laurent series,

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-a)^n, \quad \text{for all } z \in A.$$

Then $\mathcal{M}$ is a discrete valuation field with valuation the order function at a, $\mathrm{ord}_a : \mathcal{M}^* \to \mathbb{Z}$, defined by $\mathrm{ord}_a(f) = \min\{n \in \mathbb{Z} : a_n \neq 0\}$. Then $\mathcal{O}_{\mathcal{M}}$ is the set of functions analytic at a, and $\mathfrak{p}_{\mathcal{M}}$ the set of functions that vanish at a.

Note that $v(a^{-1}) = -v(a)$ for all $a \in F^*$, so $a \in \mathcal{O}_F^*$ if and only if $v(a) = 0$. Thus $\mathfrak{p}_F$ is precisely the set of noninvertible elements in $\mathcal{O}_F$. This makes $\mathcal{O}_F$ into a local ring, called the *ring of integers* of F or a *discrete valuation ring*, with unique prime ideal $\mathfrak{p}_F$. The field $\overline{F} = \mathcal{O}_F/\mathfrak{p}_F$ is called the *residue field* of F. Denote by $\overline{a}$ the image of an element $a \in \mathcal{O}$ under the canonical map $\mathcal{O}_F \to \mathcal{O}_F/\mathfrak{p}_F$. An element $\pi \in \mathcal{O}_F$ is called a *uniformizing parameter* or *prime element* of F if $v(\pi) = 1$ (or $v(\pi)$ generates the group isomorphic to $\mathbb{Z}$).

Example 7. From our previous examples we have: with valuation v_p, $\mathbb{Q}_p$ has residue field $\mathbb{F}_p$ and a uniformizing parameter p; with valuation deg, $k(x)$ has residue field k and a uniformizing parameter x; and with valuation ord_a, $\mathcal{M}$ has residue field $\mathbb{C}$ and a uniformizing parameter $z - a$.

Proposition 8. Let F be a discrete valuation field with uniformizing parameter π. Then the following hold:

- $\mathfrak{p} = (\pi) = \pi\mathcal{O}_F$, and any ideal of $\mathcal{O}_F$ is principal and corresponds with $\mathfrak{p}_F^n$ for some $n \in \mathbb{N}$.
- The intersection of all ideals of $\mathcal{O}_F$ is the zero ideal.
- Any element $a \in F^*$ can be uniquely written as $a = \pi_F^n u$ for some $n \in \mathbb{Z}$ and for some unit $u \in \mathcal{O}_F^*$.

Proof. Let $I \subset \mathcal{O}_F$ be a proper ideal. There exists some $n = \min\{v(a) : a \in \mathcal{O}_F\}$, and choose $a \in I$ such that $v(a) = n$. Then $v(a) = v(\pi^n)$ and so $a = \pi^n u$ for some unit $u \in \mathcal{O}_F^*$, thus $\pi^n\mathcal{O}_F \subset I$. Since n is the minimal such integer, we also have $I \subset \pi_F^n\mathcal{O}_F$. Thus $\mathfrak{p}_F = \pi\mathcal{O}_F$ and $I = \mathfrak{p}_F^n$ for some $n \in \mathbb{N}$. Now let $a \in \cap_n \mathfrak{p}_F^n$, then a has valuation greater than any given integer so $a = 0$ by Def. 1.

Now for $a \in F^*$, let $v(a) = n$ for some $n \in \mathbb{Z}$, then

$$v(a\pi^{-n}) = 0 \quad \Rightarrow \quad a\pi^{-n} \in \mathcal{O}_F^* \quad \Rightarrow \quad a = \pi^n u,$$

for some $u \in \mathcal{O}_F^*$, the uniqueness of u follows immediately. □

One may consult [17], Chp. I, §§2–3 for a characterization of discrete valuation rings and fields via commutative algebra.

Topology and Local Fields

Let F be a field with discrete valuation v, let $d \in \mathbb{R}$ with $0 < d < 1$, and define an absolute value $|\cdot|_v : F^* \to \mathbb{R}$ by

$$|a|_v = d^{v(a)}, \quad \text{for all } a \in F^*,$$

extending to F by letting $|0|_v = 0$. One may easily check that in fact, $|\cdot|_v$ satisfies the conditions of an absolute value on F, i.e. that for $a, b \in F$, $|a| \geq 0$, $|0|_v = 0$,

$|ab|_v = |a|_v|b|_v$, and $|a+b|_v \leq |a|_v + |b|_v$. In fact, this absolute value satisfies the stronger *non-Archimedean* condition,

$$|a+b|_v \leq \max(|a|_v, |b|_v).$$

We usually call this absolute value $|\cdot|_F$, when the choice of v is clear. As usual, define the metric $d_v : F \times F \to \mathbb{R}$ by $d_v(a,b) = |a-b|_v$. One may easily check that this metric induces a topology in which the sets $a + \mathfrak{p}^n$ for $n \in \mathbb{Z}$ form a basis of open neighborhoods at $a \in F$. This topology will be called the *discrete valuation topology* on F. If F has a finite residue field of order q, we usually take $d = 1/q$ in the above definition. This topology is also independent of the choice of valuation v.

Lemma 9. Let F be a discrete valuation field with valuations $v : F^* \to \mathbb{Z}$ and $w : F^* \to \Gamma$, where $\Gamma \cong \mathbb{Z}$. Then the topologies induced by two discrete valuations v, w coincide if and only if $v = g \circ w$ for a group isomorphism $g : \Gamma \to \mathbb{Z}$.

We say a field F is a *complete discrete valuation field* if F is complete with respect to a discrete valuation topology, i.e. if for every Cauchy sequence $\{a_n\}$ in F, there exists an $a \in F$ such that $\{|a_n - a|_v\} \to 0$ in $\mathbb{R}$. There is a nice way to represent elements in a complete discrete valuation field.

Definition 10. Let F be a discrete valuation field. A set of *representatives* R for the residue field $\overline{F}$ satisfies $R \subset \mathcal{O}_F$, $0 \in R$, and the reduction map $r \mapsto \overline{r} : R \to \overline{F}$ is a bijection.

Proposition 11. Let F be a complete discrete valuation field with uniformizing parameter π. Then any element $a \in F$ can be uniquely written as a Laurent series in π with coefficients in R, i.e.

$$a = \sum_{n=-\infty}^{\infty} a_n \pi^n, \quad a_n \in R,$$

where $a_n = 0$ for all but finitely many negative values of $n \in \mathbb{Z}$.

Let F be a complete discrete valuation field with finite residue field $\overline{F}$, then call F a *local field*. The conditions that F be complete with respect to a discrete valuation and has finite residue field impart it with nice topological properties, and from now on, we will only consider local fields.

Lemma 12. Let F be a local field. Then F is a locally compact field with respect to the discrete valuation topology. The ring of integers $\mathcal{O}_F$ and prime ideal $\mathfrak{p}_F$ are compact subrings. The multiplicative group F^* is locally compact, and the unit group $\mathcal{O}_F^*$ is a compact subgroup.

As a converse, any locally compact field F is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or a local field. In the latter case we have:

Theorem 13. Let F be a local field and let $\mathrm{char}(\overline{F}) = p$. Then $\mathrm{char}(F)$ is either 0 or p. If $\mathrm{char}(F) = 0$, then F is isomorphic to a finite extension of $\mathbb{Q}_p$. If $\mathrm{char}(F) = p$, then F is isomorphic to a finite extension of the field of formal Laurent series $\mathbb{F}_p((x))$.

See [15], App. to Chp. 2 or [5], Chp. 4.1.1 for a proof, and for further discussion. From now on, we restrict ourselves to the case of local fields with characteristic 0.

1.2 Haar Measure

Since a local field F is locally compact with respect to its additive group structure, there exists a Haar measure on F.

Theorem 14. Let G be a locally compact abelian topological group written additively. Let $\mathcal{B}(G)$ be the set of Borel sets of G, i.e. the σ-algebra generated by the open sets of G. Then there exists a nonzero measure $\mu : \mathcal{B}(G) \to \mathbb{R}$, which is translation-invariant, i.e.

$$\mu(g + E) = \mu(E), \quad \text{for all } E \in \mathcal{B}(G), g \in G.$$

For a discussion of the general theory of topological groups and Haar measure, see [9], Chp. 2–4, or [3].

In the case of a local field F, the Haar measure is usually normalized so that $\mu(\mathcal{O}_F) = 1$. Let F have finite residue field of order q, and let $R = \{a_0, \ldots, a_{q-1}\}$ with $a_0 = 0$, be a set of representatives for $\overline{F}$, then by the decomposition of local fields in Proposition 11, we have the disjoint union,

$$\mathcal{O}_F = \bigcup_{i=0}^{q-1} (a_i + \mathfrak{p}_F). \tag{1.1}$$

Since $\mu(a_i + \mathfrak{p}_F) = \mu(\mathfrak{p}_F)$, normalizing $\mu(\mathcal{O}_F) = 1$ forces $\mu(\mathfrak{p}_F) = 1/q$. By similar arguments we have

$$\mu(\mathfrak{p}_F^n) = q^{-n}, \quad \text{for all } n \in \mathbb{Z}. \tag{1.2}$$

Similarly, we have,

$$\mathcal{O}_F^* = \bigcup_{i=1}^{q-1} (a_i + \mathfrak{p}_F), \tag{1.3}$$

thus we have,

$$\mu(\mathcal{O}_F^*) = \frac{q-1}{q}.$$

Another useful disjoint decomposition is

$$\mathcal{O} = \bigcup_{n=0}^{\infty} \mathfrak{p}_F^n \backslash \mathfrak{p}_F^{n+1}, \tag{1.4}$$

where $\mathfrak{p}_F^0 = \mathcal{O}_F$. In this case, we have,

$$\mu(\mathfrak{p}_F^n \backslash \mathfrak{p}_F^{n+1}) = q^{-n} - q^{n+1} = q^{-n}\frac{q-1}{q}. \tag{1.5}$$

For a general locally compact group G, the Haar measure μ defines an integral on G, i.e. a positive continuous translation-invariant linear functional,

$$f \mapsto \int_G f \, d\mu : C_c(G) \to \mathbb{R},$$

where positive means $f \geq 0 \Rightarrow \int_G f\, d\mu \geq 0$, translation-invariant means $\int_G t_a f\, d\mu = \int_G f\, d\mu$, where $t_a f(x) = f(a+x)$ for all $x, a \in G$, and where $C_c(G)$ is the set of continuous real functions on G with compact support. From now on we will be concerned only with the unique normalized Haar measure, so we will write $\int_G f(x)\, d\mu(x)$ or just $\int_G f(x)\, dx$ in place of $\int_G f\, d\mu$.

Example 15. Let F be a local field with finite residue field of order q, discrete valuation v, and normalized absolute value $|x|_F = q^{-v(x)}$. We will integrate the continuous function $x \mapsto |x|_F : \mathcal{O}_F \to \mathbb{R}$ over $\mathcal{O}_F$. We employ the decomposition of $\mathcal{O}_F$ in Equation 1.4, and note that $|\cdot|_F$ has constant value q^{-k} on the sets $\mathfrak{p}_F^k \backslash \mathfrak{p}_F^{k+1}$. We have,

$$\begin{aligned}\int_{\mathcal{O}_F} |x|_F\, dx &= \sum_{k=0}^{\infty} \int_{\mathfrak{p}_F^k \backslash \mathfrak{p}_F^{k+1}} |x|_F\, dx = \sum_{k=0}^{\infty} q^{-k} \int_{\mathfrak{p}_F^k \backslash \mathfrak{p}_F^{k+1}} \mathbf{1}\, dx \\ &= \sum_{k=0}^{\infty} q^{-2k} \frac{q-1}{q} = \frac{q^2}{q^2-1}\frac{q-1}{q} = \frac{q}{q+1},\end{aligned}$$

where $\mathbf{1} : \mathcal{O}_F \to \mathbb{R}$ is the constant function with value 1.

In the case of integration on a local field F, almost everything from multivariable calculus on real manifolds may be carried over to the study of so-called F-analytic manifolds. Most notably, as in complex analysis, all continuously differentiable mappings on F are analytic, i.e. representable by power series. Of particular importance to us here is Fubini's theorem and the change of variables theorem from multivariable integration.

Lemma 16. Let G, H be locally compact groups with respective Haar measures μ, λ. Then the measure $\mu \otimes \lambda$ on $G \times H$ defined by

$$(\mu \otimes \lambda)(E \times F) = \mu(E)\lambda(F), \quad \text{for all } E \times F \in \mathcal{B}(G \times H),$$

is a Haar measure on $G \times H$ with the product topology.

Theorem 17 (Fubini). Let G, H, μ, and λ be as above, and let $f \in C_c(G \times H)$, then

$$x \mapsto \int_H f(x,y)\, dy : G \to \mathbb{R} \quad \text{and} \quad y \mapsto \int_G f(x,y)\, dx : H \to \mathbb{R}$$

are functions in $C_c(G)$ and $C_c(H)$, respectively, and furthermore,

$$\begin{aligned}\int_{G\times H} f\, d(\mu \otimes \lambda) &= \int_G \left(\int_H f(x,y)\, dy \right) dx \\ &= \int_H \left(\int_G f(x,y)\, dx \right) dy.\end{aligned}$$

For a discussion of Fubini's theorem on arbitrary locally compact groups, see [9], Chp. III, §13 or [3], Chp. VII, §1, n° 5.

Theorem 18 (Change of Variables). Let F be a local field, let $E \in \mathcal{B}(F^n)$, let $\varphi : E \to F^n$ be an F-analytic even k-fold covering map onto its image, and let $f \in C_c(F^n)$. Then $\varphi(E) \in \mathcal{B}(F^n)$, and

$$\int_{\varphi(E)} f(x)\, dx = \frac{1}{k} \int_E (f \circ \varphi)(x)\, |\det(J\varphi(x))|_F\, dx,$$

where $|\cdot|_F$ is the normalized absolute value on F, and where $x \mapsto J\varphi(x)$ is the Jacobian matrix of φ at x.

For a statement of this theorem and a general treatment of local F-analytic manifolds, see [4], §10, and for a proof of this theorem in the case where φ is a polynomial function and another general and interesting discussion, see [10], Chp. 2.

Example 19. We compute the same integral here as in Example 15, except here we employ the change of variables theorem. Let F be a local field with finite residue field of order q and uniformizing parameter π. In this case, we employ the decomposition $\mathcal{O}_F = \mathcal{O}_F^* \cup \mathfrak{p}_F$, and so

$$\int_{\mathcal{O}_F} |x|_F\, dx = \int_{\mathcal{O}_F^*} |x|_F\, dx + \int_{\mathfrak{p}_F} |x|_F\, dx.$$

Now, the map $\varphi : \mathcal{O}_F \to \mathfrak{p}_F$, where $\varphi(x) = \pi x$ for all $x \in \mathcal{O}_F$ is a bijection and has $\det(J\varphi(x)) = \pi$. Thus by the change of variables theorem,

$$\int_{\mathfrak{p}_F} |x|_F\, dx = \int_{\varphi(\mathcal{O}_F)} |x|_F\, dx = \int_{\mathcal{O}_F} |\pi x|_F |\pi|_F\, dx = \frac{1}{q^2} \int_{\mathcal{O}_F} |x|_F\, dx,$$

and, using Equation 1.3,

$$\int_{\mathcal{O}_F} |x|_f\, dx = \frac{q-1}{q} + \frac{1}{q^2} \int_{\mathcal{O}_F} |x|_F\, dx \quad \Rightarrow \quad (1 - q^{-2}) \int_{\mathcal{O}_F} |x|_F\, dx = \frac{q-1}{q}.$$

Again, we arrive at

$$\int_{\mathcal{O}_F} |x|_F\, dx = \frac{q}{q+1}.$$

We will be using this technique of changing variables and then solving a recursion many times throughout this work.

1.3 Extensions of Local Fields

In this section we study extensions of local fields, ramification, and review the basic properties of polynomials which generate extensions of a particular type. For a wonderful and very general discussion of these topics, consult [5], Chp. II.2, or for a very terse review, see [17], Chp. I, §§1–7, and Chp. II, §§2–3.

Lemma 20 (Gauss). Let F be a local field, and let $f \in \mathcal{O}_F[x]$ be monic with a root $a \in F$, then in fact, $a \in \mathcal{O}$.

Let K be a field such that $F \subset K$, then we say that K is an *extension* of F. We define the *degree* of the extension K over F, or $\dim_F(K)$ to be the dimension of K as a vector space over F. We say K is a finite extension of F if $\dim_F(K)$ is finite. Unless otherwise stated, all extensions will be over the field F.

If α is the root of a monic polynomial with coefficients in F, we say α is an *algebraic number*; if this polynomial is monic and has coefficients in $\mathcal{O}_F$, we say α is an *algebraic integer*. The unique monic irreducible polynomial of minimal degree of which an algebraic number α is a root, is called the *minimal polynomial* of α.

Proposition 21. Let K be a finite extension of a local field F, then $\mathcal{O}_K$ is the integral closure of $\mathcal{O}_F$ in K, i.e. if f is the minimal polynomial for $a \in \mathcal{O}_K$, then $f \in \mathcal{O}_F[x]$, and conversely, if $f \in \mathcal{O}_F[x]$ is monic and $a \in K$ is a root of f, then $a \in \mathcal{O}_K$.

Define $F(\alpha)$, or the extension *generated* over F by α, to be the smallest field containing both F and α. If α has a minimal polynomial of degree n then $F(\alpha)$ is a finite extension of F of degree n. Call an extension K of F a *separable extension* if every element $\alpha \in K$ has a minimal polynomial over F with no multiple roots. In the case that F has characteristic 0, every extension of F is separable. Let a *separable closure* of F, or F^{sep}, be a separable extension of F containing every algebraic number.

Theorem 22. Let K be a finite separable extension of a local field F of degree n, then $K = F(\alpha)$ for some algebraic integer $\alpha \in \mathcal{O}_K$, with minimal polynomial of degree n over F. Also, the ring of integers $\mathcal{O}_K$ is simply generated over $\mathcal{O}_F$ by an algebraic integer $\beta \in \mathcal{O}_K$, and we write $\mathcal{O}_K = \mathcal{O}_F[\beta]$, i.e. the powers $1, \beta, \ldots, \beta^{n-1}$ form a module basis for $\mathcal{O}_K$ over $\mathcal{O}_F$.

Let K be a finite extension of a local field F with discrete valuation $w : K^* \to \mathbb{Z}$. Then the restriction $w|_F : F^* \to \mathbb{Z}$ is a discrete valuation on F, and the group index $[w(K^*) : w(F^*)]$ is called the *ramification index*, or $e(K/F)$. Thus $w|_F : F \to e(K/F)\mathbb{Z} \cong \mathbb{Z}$, i.e. $w(a) = e(K/F)v(a)$ for $a \in F$, where v is a discrete valuation on F. Under this induced valuation, the ring of integers $\mathcal{O}_F$ is a subring of the ring of integers $\mathcal{O}_K$, and the prime ideal $\mathfrak{p}_F = \mathfrak{p}_K \cap \mathcal{O}_F$ is contained in $\mathfrak{p}_K^e$. In other words, for respective uniformizing parameters π_F and π_K, we have $\pi_F = \pi_K^e u$ for some unit $u \in \mathcal{O}_K^*$. Also in this picture, the residue field $\overline{F} = \mathcal{O}_F/\mathfrak{p}_F$ is a subfield of $\overline{K} = \mathcal{O}_K/\mathfrak{p}_K$. The degree of the field extension $\overline{K}$ over $\overline{F}$ is called the *residue degree*, or $f(K/F)$.

$$\begin{array}{ccc} K & \mathfrak{p}_K^e & \overline{K} = \mathbb{F}_{q^f} \\ n\,\big| & \big\uparrow & f\,\big| \\ F & \mathfrak{p}_F & \overline{F} = \mathbb{F}_q \end{array}$$

Figure 1.1: Diagram of ramification index and residue degree.

Theorem 23. Let K be an extension of a local field F of degree n, then

$$e(K/F)f(K/F) = n.$$

Remark 24. Let K be an extension of F of degree n, with $e(K/F) = e$, $f(K/F) = f$, uniformizing parameters π_F and π_K, discrete valuations v_K and v_F, and normalized absolute values $|\cdot|_K$ and $|\cdot|_F$. Then if F has residue field of order q, K has residue field of order q^f, and we make the following simple but important observation,

$$v_K(\pi_F) = e \quad \Rightarrow \quad |\pi_F|_K = q^{-fv_K(\pi_F)} = q^{-ef} = q^{-n} = |\pi_F|_F^n.$$

Since knowing the absolute value of a uniformizing parameter determines it everywhere, we have,

$$|\cdot|_K = |\cdot|_F^n, \tag{1.6}$$

where $|\cdot|_F$ and $|\cdot|_K$ are the normalized absolute values on F and K, respectively.

Definition 25. Let K be a finite extension of F of degree n. If $e(K/F) = 1$, so $f(K/F) = n$, then say K is an *unramified extension* of F. If $e(K/F) = n$, so $f(K/F) = 1$, then say K is a *totally ramified extension* of F. Let $\mathrm{char}(\overline{F}) = p$. If $p \nmid e(K/F)$, then say K is *tamely ramified*. If $p \mid e(K/F)$, then say K is *wildly ramified*.

Definition 26. For a polynomial $f(x) = a_n x^n + \cdots + a_0 \in \mathcal{O}_F[x]$, define the *reduction* of f in the residue field,

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_0 \in \overline{F}[x].$$

If $\alpha, \beta \in \mathcal{O}_F$, or $f, g \in \mathcal{O}_F[x]$, then say

$$\alpha \equiv \beta \bmod \mathfrak{p}_F^n \quad \text{or} \quad f \equiv g \bmod \mathfrak{p}_F^n$$

if $\alpha - \beta \in \mathfrak{p}_F^n$, or $f(x) - g(x) \in \mathfrak{p}_F^n[x]$, respectively. Also, for $\alpha_0 \in \overline{F}$, or $f_0 \in \overline{F}[x]$, define a *lift* to be any element $\alpha \in \mathcal{O}_F$, or $f \in \mathcal{O}_F[x]$ such that $\overline{\alpha} = \alpha_0$, or $\overline{f} = f_0$, respectively.

Definition 27. A monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_F$ is called an *Eisenstein polynomial* over F if $a_0, \ldots, a_{n-1} \in \mathfrak{p}_F$, but $a_0 \notin \mathfrak{p}_F^2$.

Proposition 28. Let K be a finite separable extension of F of degree n, and let π_K and π_F be uniformizing parameters for K and F, respectively.

- If K is an unramified extension of F, then $K = F(\zeta)$ and $\mathcal{O}_K = \mathcal{O}_f[\zeta]$ for some $\zeta \in \mathcal{O}_K$ for which $\overline{K} = \overline{F}(\overline{\zeta})$, i.e. such that $\overline{\zeta}$ satisfies an irreducible polynomial of degree n over $\overline{F}$. Conversely, for any monic irreducible polynomial $f \in \mathcal{O}_F$ of degree n such that $\overline{f}$ is irreducible over $\overline{F}$, a root of f generates an unramified extension of degree n in which π_F is still a uniformizing parameter.

- If K is totally ramified, then $K = F(\pi_K)$, $\mathcal{O}_K = \mathcal{O}_F[\pi_K]$, and π_K is the root of an Eisenstein polynomial of degree n. Conversely, any Eisenstein polynomial of degree n over F is irreducible, and for any root π, $F(\pi)$ is totally ramified over F of degree n, π is a uniformizing parameter in $F(\pi)$, and $\mathcal{O}_{F(\pi)} = \mathcal{O}[\pi]$.

See specifically [5], Chp. II.3.3 for a proof.

Definition 29. Let K be a separable extension of a field F of degree n. Then let $\mathrm{Aut}_F(K)$ be the set of automorphisms of K which fix F, i.e. automorphisms $s : K \to K$ such that $sa = a$ for every $a \in F$. Define $w(K/F) = w(K) = \#\mathrm{Aut}_F(K)$.

If K is an extension of F of degree n, then $w(K) \leq n$. If $w(K) = n$ we say K is a *Galois extension* of F, and call $\mathrm{Aut}_F(K)$ the *Galois group* of K over F.

Definition 30. Let K be a separable extension of a field F of degree n. Then let $\mathrm{Hom}_F(K, F^{\mathrm{sep}})$ be the set of continuous injective homomorphisms $\sigma : K \to F^{\mathrm{sep}}$ which fix F, called *embeddings* of K over F.

Theorem 31. Let $K = F(\alpha)$ be a separable extension of F of degree n. Then $\#\mathrm{Hom}_F(K, F^{\mathrm{sep}}) = n$, and for each $\sigma \in \mathrm{Hom}_F(K, F^{\mathrm{sep}})$, $\sigma\alpha$ is a root of the minimal polynomial of α.

Let $\alpha \in F^{\mathrm{sep}}$ be an algebraic number with minimal polynomial f over F. Then any root β of f is said to be a *conjugate* of α over F. If $K = F(\alpha)$, then $\mathrm{Hom}_F(K, F^{\mathrm{sep}})$ acts on K by shuffling the conjugates of α.

Definition 32. Let K be a separable extension of F, and let $H = \mathrm{Hom}_F(K, F^{\mathrm{sep}})$. Then for $\alpha \in K$ define,

$$N_{K/F}(\alpha) = \prod_{\sigma \in H} \sigma\alpha, \qquad T_{K/F}(\alpha) = \sum_{\sigma \in H} \sigma\alpha,$$

and call these the *norm* and *trace*, respectively, of α from K down to F.

Proposition 33. For $\alpha, \beta \in K$, we have $N_{K/F}(\alpha), T_{K/F}(\alpha) \in F$, and

$$N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta), \qquad T_{K/F}(\alpha + \beta) = T_{K/F}(\alpha) + T_{K/F}(\beta).$$

If $K = F(\alpha)$ and f is the minimal polynomial of α over F, then

$$\begin{aligned} f(x) &= N_{K/F}(x - \alpha) = \prod_{\sigma \in H} (x - \sigma\alpha) \\ &= x^n - T_{K/F}(\alpha)x^{n-1} + \cdots + (-1)^n N_{K/F}(\alpha). \end{aligned}$$

The norm and trace are examples of the *elementary symmetric functions*, $e_1, \ldots, e_n$, of n indeterminates $a_1, \ldots, a_n$, and defined by the relation,

$$\prod_{i=1}^{n}(x - a_i) = x^n - e_1(a_1, \ldots, a_n)x^{n-1} + e_2(a_1, \ldots, a_n)x^{n-2} - \ldots + (-1)^n e_n(a_1, \ldots, a_n),$$

or explicitly given by

$$e_1(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i, \quad e_2(a_1, \ldots, a_n) = \sum_{i<j} a_i a_j, \quad \ldots, \quad e_n(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_i.$$

Definition 34. Let $f \in \mathcal{O}_F[x]$ be monic, and let α be a root of f. Then define the *discriminant* of f by,

$$\mathrm{discr}(f) = \prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha)^2,$$

where $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_F(F(\alpha), F^{\mathrm{sep}})$. Now let K be an extension of F, and let f be a polynomial whose root generates $\mathcal{O}_K$ over $\mathcal{O}_F$. Then define D_K, the *discriminant* of the field K, by $D_K = \mathrm{discr}(f)$, and define $d(K) = v_F(D_K)$.

Example 35. Let K be an extension of F of degree n. If K is unramified over F, then $d(K) = 0$. If K is tamely ramified over F, then $v_F(K) = n - 1$. If K is wildly ramified over F, then $d(K) > n - 1$.

A celebrated lemma we will need later on is:

Lemma 36 (Krasner). Let F be a local field, and let $\alpha, \beta \in F^{\mathrm{sep}}$, then

$$|\alpha - \beta|_F < |\alpha - \alpha'|_F, \text{ for every conjugate } \alpha' \text{ of } \alpha \quad \Rightarrow \quad \alpha \in F(\beta).$$

This says that for a given extension K of a local field F, the set of elements which generate K over F is an open subset inside K.

Hensel's Lemma

Hensel's Lemma is a tool for determining when a polynomial with coefficients in a local field factors, and will be invaluable to us soon enough. Let F be a local field with ring of integers $\mathcal{O}$, prime ideal $\mathfrak{p}$, and residue field $\overline{F} = \mathcal{O}/\mathfrak{p} = \mathbb{F}_q$.

A handy tool for checking the irreducibility of a polynomial with rational integer coefficients $f \in \mathbb{Z}[x]$ is to reduce f in the field $\mathbb{F}_p$ for various rational primes p. If the reduction of f is irreducible for a given prime p, then f is irreducible over $\mathbb{Z}$. This trick also holds for monic polynomials $f \in \mathcal{O}[x]$ with reduction to the residue field $\overline{F}$. In general, the converse of this is not true, i.e. if $f \in \mathbb{Z}[x]$ is reducible modulo every prime p, it does not follow that f is reducible over $\mathbb{Z}$ (the polynomial $x^4 - 10x^2 + 1$ is an example). Hensel's Lemma gives the extent to which this converse is true in a local field.

Lemma 37 (Hensel's Lemma). Let $f \in \mathcal{O}[x]$ be monic. Then if $\overline{f}$ splits in $\overline{F}$ into relatively prime factors, then f splits in F, i.e. if there exist relatively prime and monic $\overline{g}, \overline{h} \in \overline{F}$ with $\overline{f} = \overline{g}\overline{h}$, then there exist monic lifts $g, h \in \mathcal{O}[x]$ with $f = gh$.

This gives the main idea of Hensel's Lemma. In practice though, a slightly stronger version is usually needed.

Lemma 38 (Hensel's Lemma). Let $f \in \mathcal{O}[x]$, $\alpha_0 \in \mathcal{O}$, and $n \in \mathbb{N}$ be such that

$$f(\alpha_0) \in \mathfrak{p}^{2n+1} \text{ and } f'(\alpha_0) \notin \mathfrak{p}^{n+1} \quad \text{i.e.} \quad |f(\alpha_0)|_F < |f'(\alpha_0)|_F^2,$$

then there exists a lift $\alpha \in \mathcal{O}$, such that $f(\alpha) = 0$, with $\alpha \equiv \alpha_0 \bmod \mathfrak{p}^{n+1}$.

See [5], Chp. 2.1 for a very general proof or [8], Chp. 3.4 and 5.4 for a very friendly introduction and a concrete proof.

1.4 Quadratic Extensions of $\mathbb{Q}_p$

Using Hensel's Lemma, we will classify all quadratic extensions of $\mathbb{Q}_p$. By the quadratic formula, we need to consider only the equivalence classes of nonsquare elements, i.e. the multiplicative group

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2.$$

Indeed, given a coset $a(\mathbb{Q}_p^*)^2$, any $x \in a(\mathbb{Q}_p^*)^2$ is represented as $x = ay^2$ for some $y \in \mathbb{Q}_p$, so the quadratic extensions $\mathbb{Q}_p(\sqrt{x})$ and $\mathbb{Q}_p(\sqrt{a})$ will be equal. It is our task to find suitable coset representatives for this group. To this end, we study the polynomial $f_a(x) = x^2 - a$ for a given $a \in \mathbb{Q}_p^*$, and ask whether or not it splits, i.e. has a root in $\mathbb{Q}_p$. The polynomial f_a splits if and only if $\sqrt{a} \in \mathbb{Q}_p$.

First note that for $a \in \mathbb{Q}_p^*$ to be a square, $v_p(a)$ must be even, i.e.

$$a = p^{2n}a' \quad \text{for some } n \in \mathbb{Z}, a' \in \mathbb{Z}_p^*.$$

Thus we are reduced to finding which p-adic integer units $a \in \mathbb{Z}_p^*$ are squares. By Hensel's Lemma, we just need to know whether $\overline{f}_a$ splits in $\overline{\mathbb{Q}}_p = \mathbb{F}_p$ into relatively prime factors. For $p = 2$, $\overline{f}_a$ is always a square in $\mathbb{F}_2$, since for any $a \in \mathbb{Z}_2^*$,

$$\overline{a} \equiv 1 \quad \text{in } \mathbb{F}_2 \quad \Rightarrow \quad \overline{f}_a(x) = x^2 - \overline{a} \equiv x^2 - 1 \equiv (x-1)^2 \quad \text{in } \mathbb{F}_2.$$

The first version of Hensel's Lemma doesn't apply here since the factors of $\overline{f}_a$ aren't relatively prime in $\mathbb{F}_2$. Before proceeding, also note that given $a \in \mathbb{Z}_2^*$, we can write $a = 1 + 2b$ for some $b \in \mathbb{Z}_2$, then

$$a^2 = 1 + 4(b + b^2) + 4b^2 = 1 + 8c, \quad \text{for some } c \in \mathbb{Z}_2,$$

since $b + b^2 \equiv 0$ in $\mathbb{F}_2$. Now given any $a = 1 + 8\mathbb{Z}_2$, we can use the stronger version of Hensel's Lemma, with $\alpha_0 = 1$. We have,

$$f_a(1) = 1 - a \in 8\mathbb{Z}_2 \quad \text{and} \quad f_a'(1) = 2 \notin 4\mathbb{Z}_2,$$

thus f_a has a root if and only if $a \in 1 + 8\mathbb{Z}_2$.

For odd p, the first version of Hensel's Lemma applies whenever a is a quadratic residue modulo p, i.e. $\overline{a}$ is a square in $\mathbb{F}_p$. Indeed, given $a \in \mathbb{Z}_p^*$ with $\overline{a} = b^2$, we have

$$\overline{f}_a(x) = x^2 - \overline{a} = (x - b)(x + b) \quad \text{in } \mathbb{F}_p,$$

thus f_a has a root in $\mathbb{Z}_p$. Of course, this condition is necessary. We have proved the following:

Proposition 39. The squares in $\mathbb{Z}_2^*$ are precisely the units of the form $1 + 8\mathbb{Z}_2$. The squares in $\mathbb{Z}_p^*$ for odd p are precisely those of the form $r + p\mathbb{Z}_p$, where $\overline{r}$ is a quadratic residue modulo p.

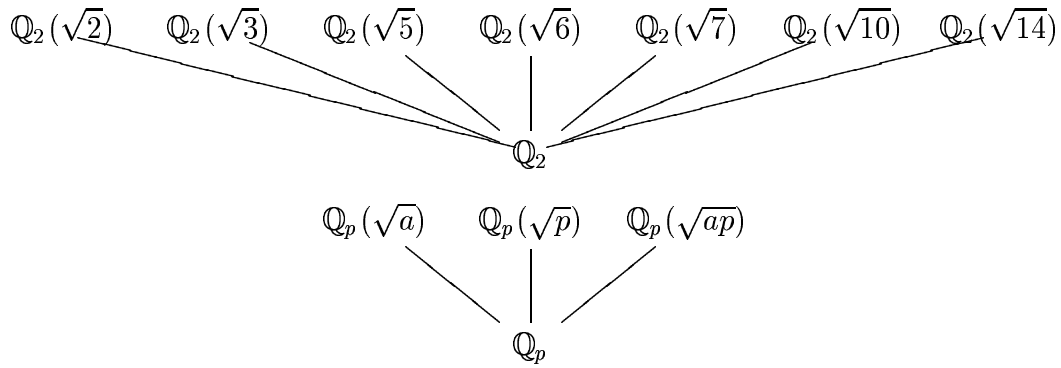


Figure 1.2: Quadratic Extensions of $\mathbb{Q}_p$

Corollary 40. For $p = 2$, the group $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is of order 8 with coset representatives $\{1, 2, 3, 5, 6, 7, 10, 14\}$. For odd primes p, the group $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ is of order 4 with coset representatives $\{1, a, p, ap\}$ for some fixed nonquadratic residue a modulo p. The square roots of these elements generate the isomorphism classes of quadratic extensions over $\mathbb{Q}_2$ and $\mathbb{Q}_p$, respectively.

We picture these extensions in Figure 1.2, and can now proceed to identify the ramification type and calculate the discriminant of each.
First let $p = 2$.

- We first notice that the minimal polynomials of $\sqrt{2}$, $\sqrt{6}$, $\sqrt{10}$, and $\sqrt{14}$ are x^2-2, x^2-6, x^2-10, and x^2-14, respectively. Each is an Eisenstein polynomial f, whose roots generate a totally ramified extension K by Proposition 28, with $d(K) = v(\text{discr}(f)) = 3$ (remember that $\text{discr}(x^2 + ax + b) = a^2 - 4b$).

- Next notice that the minimal polynomials for $\sqrt{3}$ and $\sqrt{7}$ are x^2-3 and x^2-7, respectively, and can be translated to the polynomials $(x+1)^2-3 = x^2+2x-2$ and $(x+1)^2-7 = x^2+2x-6$. Thus each is an Eisenstein polynomial f, whose roots generate a totally ramified extension K with $d(K) = v(\text{discr}(f)) = 2$.

- Finally, for the extension $K = \mathbb{Q}_2(\sqrt{5})$, note that $\alpha = \frac{1+\sqrt{5}}{2} \in K$, but furthermore, that the minimal polynomial of α, $x^2 - x - 1$ is monic and irreducible in $\mathbb{F}_2$. So in fact $\alpha \in \mathcal{O}_K$, and by Proposition 28, K is unramified over $\mathbb{Q}_2$, $\mathcal{O}_K = \mathbb{Z}_2(\alpha)$, and $d(K) = 0$.

Now for an odd prime p and a fixed nonquadratic residue a modulo p.

- The minimal polynomial of $\sqrt{p}$ and $\sqrt{ap}$ is $x^2 - p$ and $x^2 - ap$, respectively. Each is an Eisenstein polynomial that generates a totally ramified extension K with $d(K) = 1$.

- The minimal polynomial of $\sqrt{a}$ is $x^2 - a$, which is irreducible in the residue field $\mathbb{F}_p$, thus $\sqrt{a}$ generates an unramified extension K with $d(K) = 0$, and generates $\mathcal{O}_K$ over $\mathbb{Z}_p$.

1.5 Étale Algebras

Our study of polynomials generating a given extension of a local field F will soon lead to considering reducible polynomials. The roots of reducible polynomials don't naturally lie in any single finite extension of F, but in a number of them. The natural generalization of the root field of an irreducible polynomial is a direct sum of root fields of the irreducible factors of a reducible polynomial. This direct sum forms an algebra, i.e. a vector space over F with a defined multiplication ([2], Chp. III).

Definition 41. Let F be a field, and let A be a finite dimensional commutative F-algebra, then call A an *étale algebra* over F if

$$A \cong \bigoplus_{i=1}^{\ell} K_i,$$

for finite separable extensions K_i of F. Define $\dim_F(A)$ to be the vector space dimension of A over F. Denote by $\mathcal{A}_n(F)$ the set of isomorphism classes of étale algebras A over F with $\dim_F(A) = n$ inside a fixed F^{sep}.

One should note that in the characteristic 0 case, which we are restricting ourselves to, there is a finite number of extensions of F of a given degree. Thus the set of isomorphism classes $\mathcal{A}_n(F)$ is finite.

Example 42. The only quadratic étale algebras over a local field F are quadratic extensions of F and the algebra F^2. From Corollary 40, we know the quadratic extensions of $\mathbb{Q}_p$, and thus we have,

$$\begin{aligned} \mathcal{A}_2(\mathbb{Q}_2) &= \{\mathbb{Q}_2^2\} \cup \{\mathbb{Q}_2(\sqrt{a}) : a = 2, 3, 5, 6, 7, 10, 14\} \\ \mathcal{A}_2(\mathbb{Q}_p) &= \{\mathbb{Q}_p^2, \mathbb{Q}_p(\sqrt{a}), \mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{ap})\}, \end{aligned}$$

where in the second case, for odd p, a is a fixed nonquadratic residue modulo p.

From now on let F be a local field. If $f \in F[x]$ is irreducible over F, then

$$F[x]/(f) \cong F(\alpha),$$

where α is a root of f, and is thus an étale algebra. Moreover, if f is reducible but square-free, and $f = \prod_{i=1}^{\ell} f_i$, where each f_i is irreducible over F, then by the Chinese Remainder Theorem,

$$F[x]/(f) = F[x]/(\textstyle\prod_{i=1}^{\ell} f_i) \cong \displaystyle\bigoplus_{i=1}^{\ell} F[x]/(f_i) \cong \bigoplus_{i=1}^{\ell} K_i,$$

where each $K_i = F(\alpha_i)$ is a root field of f_i. Since every direct sum of separable extensions of F can arise in this way, we have, for any étale algebra A over F,

$$A \cong F[x]/(f),$$

for some square-free $f \in F[x]$. Note that f is square-free if and only if $\text{discr}(f) \neq 0$.

Definition 43. Let $A \in \mathcal{A}_n(F)$ with $A \cong \bigoplus_{i=1}^{\ell} K_i$, and let $\mathcal{O}$ be the ring of integers of F. Define the *ring of integers* of A to be

$$\mathcal{O}_A \cong \bigoplus_{i=1}^{\ell} \mathcal{O}_{K_i},$$

Also define the *discriminant* of A by

$$D_A = \prod_{i=1}^{\ell} D_{K_i},$$

and let $d(A) = v_F(D_A)$ for a valuation v_F on F.

For a definition of the discriminant of an arbitrary algebra, see [2], Chp. III, §9. For a very general discussion of étale algebras, see [12], Chp. 5, §18. By Theorem 22, if A is an étale algebra of dimension n over F then, $\mathcal{O}_A \cong \mathcal{O}^n$, and is thus a compact topological group in the product topology with normalized Haar measure $\mu = \mu_F^{\otimes n}$. In most respects, we treat an étale algebra as a field extension in the following chapters.

Chapter 2

Quadratic Volume Computations

Fix a local field F with ring of integers $\mathcal{O}$, prime ideal $\mathfrak{p}$, uniformizing parameter π, and residue field of order q. For $n \in \mathbb{N}$, let $\mathcal{P}_n(F) = \mathcal{P}_n \subset \mathcal{O}[x]$ be the set of all monic polynomials of degree n with coefficients in $\mathcal{O}$. Under the isomorphism,

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \mapsto (a_1, \ldots, a_n) \in \mathcal{O}^n : \mathcal{P}_n \to \mathcal{O}^n,$$

the set of polynomials $\mathcal{P}_n \cong \mathcal{O}^n$ becomes a compact topological group in the product topology with normalized Haar measure $\mu = \mu_F^{\otimes n}$ inherited from F. Let $\tilde{\mathcal{P}}_n$ be the set of those polynomials with nonzero discriminants. Since the set of polynomials with discriminant zero has measure zero in $\mathcal{P}_n$, $\mu(\tilde{\mathcal{P}}_n) = \mu(\mathcal{P}_n) = 1$.

For an étale algebra $A \in \mathcal{A}_n(F)$, let $\mathcal{P}^A \subset \tilde{\mathcal{P}}_n$ be the set of polynomials $f \in \tilde{\mathcal{P}}_n$ for which f generates the algebra A, i.e. such that $F[x]/(f) \cong A$. Also let $m_F(A) = \mu(\mathcal{P}^A)$.

2.1 Completely Split Quadratic Polynomials

Quadratic polynomials that split completely and have non-zero discriminant, (i.e. have distinct roots) generate the étale algebra F^2 over F. In this section we will calculate $m_F(F^2)$.

To that end, first note that by Gauss' Lemma (Lemma 20), if $f \in \mathcal{P}^{F^2}$ and $a \in F$ is a root of f, then in fact $a \in \mathcal{O}$. Now define the mapping, taking a pair of distinct roots to the polynomial with those roots, $\varphi : \tilde{\mathcal{O}}^2 \to \mathcal{P}^{F^2}$ given by

$$\varphi(a, b) = (x - a)(x - b) = x^2 - (a + b)x + ab, \quad \text{for all } (a, b) \in \tilde{\mathcal{O}}^2,$$

where $\tilde{\mathcal{O}}^2 = \{(a, b) \in \mathcal{O}^2 : a \neq b\}$. Note that φ is a surjective 2-to-1 mapping (since $\varphi(a, b) = \varphi(b, a)$). Thus $m_F(F^2) = \mu(\varphi(\tilde{\mathcal{O}}^2))$, and by the change of variables theorem (Theorem 18),

$$\begin{aligned} m_F(F^2) &= \mu(\varphi(\tilde{\mathcal{O}}^2)) = \int_{\varphi(\tilde{\mathcal{O}}^2)} \mathbf{1}\, d\mu \\ &= \frac{1}{2}\int_{\tilde{\mathcal{O}}^2} |\det(J\varphi)|_F \, d\mu = \frac{1}{2}\int_{\mathcal{O}^2} |\det(J\varphi)|_F \, d\mu, \end{aligned}$$

where $|\cdot|_F$ is the normalized absolute value on F. Written in coordinates, $\varphi : \mathcal{O}^2 \to \mathcal{P}^{F^2} \hookrightarrow \mathcal{O}^2$ is given by

$$\varphi(a,b) = (-(a+b), ab), \quad \text{for all } (a,b) \in \tilde{\mathcal{O}}^2,$$

and we can calculate

$$J(\varphi(a,b)) = \begin{pmatrix} -1 & -1 \\ b & a \end{pmatrix} \quad \Rightarrow \quad \det(J\varphi(a,b)) = b - a.$$

Thus we have

$$\begin{aligned} m_F(F^2) &= \frac{1}{2}\int_{\mathcal{O}^2} |a-b|_F \, da\, db = \frac{1}{2}\int_{\mathcal{O}} \left(\int_{\mathcal{O}} |a-b|_F \, da \right) db \\ &= \frac{1}{2}\int_{\mathcal{O}} \left(\int_{\mathcal{O}} |a|_F \, da \right) db = \frac{1}{2}\int_{\mathcal{O}} |a|_F \, da \\ &= \frac{1}{2}\frac{q}{q+1}, \end{aligned} \tag{2.1}$$

by Fubini's Theorem (Theorem 17), and by the calculation in Example 15. It is interesting to note here, and we will return to this point, that

$$\lim_{q\to\infty} m_F(F^2) = \lim_{q\to\infty} \frac{1}{2}\frac{q}{q+1} = \frac{1}{2}.$$

2.2 Irreducible Polynomials

Now we want to extend this idea to compute the volumes of irreducible quadratic polynomials with roots in a given quadratic extension K of F. Let $\mathcal{O}_K$ be the ring of integers of K, and let $\tilde{\mathcal{O}}_K$ be the set of elements that generate K over F, i.e. $\mathcal{O}_K \backslash \mathcal{O}$. The lower dimensional embedded subset $\mathcal{O} \subset \mathcal{O}_K \cong \mathcal{O}^2$ has measure zero, so $\mu(\tilde{\mathcal{O}}_K) = \mu(\mathcal{O}_K) = 1$. If α is a root of f that generates K, then so is α', where α' is a conjugate of α. By Proposition 21, we know that if $\alpha \in K$ is a root of f, then in fact $\alpha \in \mathcal{O}_K$. Define the mapping, taking roots to minimal polynomials, $\varphi_K : \tilde{\mathcal{O}}_K \to \mathcal{P}^K$ given by

$$\varphi_K(\alpha) = (x-\alpha)(x-\alpha') = x^2 - T(\alpha)x + N(\alpha), \quad \text{for all } \alpha \in \tilde{\mathcal{O}}_K,$$

where $T(\alpha) = T_{K/F}(\alpha)$, and $N(\alpha) = N_{K/F}(\alpha)$. As in the previous calculation, φ_K is a surjective 2-to-1 mapping (since $\varphi_K(\alpha) = \varphi_K(\alpha')$). Thus $m_F(K) = \mu(\varphi_K(\tilde{\mathcal{O}}_K))$, and again, by change of variables,

$$m_F(K) = \int_{\varphi(\tilde{\mathcal{O}}_K)} \mathbf{1} \, d\mu = \frac{1}{2}\int_{\tilde{\mathcal{O}}_K} |\det(J\varphi)|_F \, d\mu = \frac{1}{2}\int_{\mathcal{O}_K} |\det(J\varphi)|_F \, d\mu,$$

where here $|\cdot|_F$ is appropriate since $\tilde{\mathcal{O}}_K \cong \mathcal{P}^K \cong \mathcal{O}^2$, and we are really thinking of φ_K as a mapping of $\mathcal{O}^2$. Thus to really compute $J\varphi$, we need to choose a (module)

basis of $\mathcal{O}_K$ over $\mathcal{O}$. Write $\mathcal{O}_K = \mathcal{O}[\beta] = \mathcal{O} \oplus \beta\mathcal{O}$ where we can choose $\beta \in \mathcal{O}_K$, then in coordinates $\varphi_K : \tilde{\mathcal{O}}^2 \cong \tilde{\mathcal{O}}_K \to \mathcal{P}^K \hookrightarrow \mathcal{O}^2$ is given by

$$\begin{aligned} \varphi_K(a,b) &= (-T(a+b\beta), N(a+b\beta)) \\ &= (-2a - bT(\beta), a^2 + abT(\beta) + b^2N(\beta)), \quad \text{for all } (a,b) \in \tilde{\mathcal{O}}^2 \end{aligned}$$

where here $\tilde{\mathcal{O}}^2 = \{(a,b) \in \mathcal{O}^2 : b \neq 0\} \cong \tilde{\mathcal{O}}_K$. Thus we calculate,

$$\begin{aligned} \det(J\varphi_K(a,b)) &= \det \begin{pmatrix} -2 & -T(\beta) \\ 2a + bT(\beta) & aT(\beta) + 2bN(\beta) \end{pmatrix} \\ &= b(T(\beta)^2 - 4N(\beta)) \\ &= D_K b, \end{aligned}$$

where D_K is the discriminant of the extension K. Note that since $\mathcal{O}_K = \mathcal{O}[\beta]$, and the minimal polynomial of β is $f(x) = x^2 - T(\beta)x + N(\beta)$, we have $D_K = \mathrm{discr}(f) = T(\beta)^2 - 4N(\beta)$. Proceeding as above, we have

$$\begin{aligned} m_F(K) &= \frac{1}{2}\int_{\mathcal{O}^2} |D_K b|_F \, da\, db = \frac{1}{2}\frac{1}{q^{d(K)}}\int_{\mathcal{O}} |b|_F \, db \\ &= \frac{1}{2}\frac{1}{q^{d(K)}}\frac{q}{q+1}. \end{aligned} \tag{2.2}$$

Each polynomial $f \in \mathcal{P}_2$ with nonzero discriminant must generate either the algebra F^2 (in the case that f splits over F), or one of the finite number of quadratic extensions K of F. Thus we have the disjoint union,

$$\bigcup_{A \in \mathcal{A}_2(F)} \mathcal{P}^A = \tilde{\mathcal{P}}_2,$$

and putting together Equations 2.1 and 2.2, we have the following:

Theorem 44. Let F be a local field with residue field of order q and let $\mathcal{A}_2(F)$ denote the set of all isomorphism classes of quadratic algebras over F. Then we have,

$$\sum_{A \in \mathcal{A}_2(F)} \frac{1}{2}\frac{1}{q+1}\frac{1}{q^{d(A)-1}} = 1,$$

where recall that by Definition 43, $d(A) = 0$ for $A = F^2 \in \mathcal{A}_2(F)$.

Quadratic Polynomials over $\mathbb{Q}_p$

By Corollary 40, we know models for the isomorphism classes of quadratic extensions K of $\mathbb{Q}_p$, and we calculated $d(K)$ for each. Using Equation 2.2 to compute explicit numbers for the volumes $m_{\mathbb{Q}_p}(K)$, we summarize all this in Table 2.1. In accordance with Theorem 44, the sum of these volumes is 1.

$A \in \mathcal{A}_2(\mathbb{Q}_p)$	$d(A)$	$m_{\mathbb{Q}_2}(A)$
$p = 2$		
$\mathbb{Q}_2^2$	0	$\frac{1}{3}$
$\mathbb{Q}_2(\sqrt{5})$	0	$\frac{1}{3}$
$\mathbb{Q}_2(\sqrt{3})$, $\mathbb{Q}_2(\sqrt{7})$	2	$\frac{1}{12}$
$\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{6})$, $\mathbb{Q}_2(\sqrt{10})$, $\mathbb{Q}_2(\sqrt{14})$	3	$\frac{1}{24}$
p odd		
$\mathbb{Q}_p^2$	0	$\frac{1}{2}\frac{p}{p+1}$
$\mathbb{Q}_p(\sqrt{a})$	0	$\frac{1}{2}\frac{p}{p+1}$
$\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{ap})$	1	$\frac{1}{2}\frac{1}{p+1}$

Table 2.1: Volumes for Quadratic Étale Algebras over $\mathbb{Q}_p$

2.3 Visualizing Quadratic Polynomials over $\mathbb{Q}_p$

Now that we know the volume of monic $\mathbb{Z}_p$ polynomials that generate a given quadratic extension of $\mathbb{Q}_p$, we give a way to "visualize" them. To this end we describe a way to embed $\mathcal{P}_2 = \mathcal{P}_2(\mathbb{Q}_p) \cong \mathbb{Z}_p^2$ into the plane $\mathbb{R}^2$.

By the definition in Example 4, $a \in \mathbb{Z}_p$ is uniquely representable as a formal power series in the integer p, i.e.

$$a = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where the coefficients $a_i \in \{0, 1, \ldots, p-1\}$. There is an obvious continuous map $r : \mathbb{Z}_p \to \mathbb{R}$,

$$r(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots) = a_0 + \frac{a_1}{p} + \frac{a_2}{p^2} + \frac{a_3}{p^3} + \cdots = a_0.a_1 a_2 a_3 \ldots,$$

sending p-adic expansions to base-p expansions of real numbers. We normalize this map to the surjection $r : \mathbb{Z}_p \to [0, 1]$, given by

$$r\left(\sum_{n=0}^{\infty} a_n p^n\right) = \frac{1}{p} \sum_{n=0}^{\infty} \frac{a_n}{p^n}.$$

This map is not injective because of differing decimal expansions of real numbers. For a rigorous treatment of this "visualization" and other possible ones, see [15], Chp. 2.

To visualize the p-adic integer plane $\mathbb{Z}_p^2$, we just need to extend component-wise in the obvious way, $r : \mathbb{Z}_p^2 \to [0, 1] \times [0, 1]$,

$$r(x, y) = (r(x), r(y)), \quad \text{for all } (x, y) \in \mathbb{Z}_p^2.$$

Now we can visualize the set $\mathcal{P}_2(\mathbb{Q}_p)$ as follows: for each point $(a, b) \in \mathbb{Z}_p^2$, color the point $r(a, b) \in [0, 1]^2$ according to which quadratic algebra the polynomial $f_{(a,b)}(x) = x^2 + ax + b$ generates. We implement this in a `C` program which computes the the discriminant of the polynomial $f_{(a,b)}$, and after dividing out by the necessary powers of p looks modulo p, if p is odd, or modulo 8, if $p = 2$. By the work proceeding Corollary 40 this decides which algebra $f_{(a,b)}$ generates, and our program colors the corresponding point. If $p = 2$, red is for split, blue is for unramified, magenta and light blue are for totally ramified with discriminant 2, and shades of green and orange are for totally ramified with discriminant 3. For odd p, red is for split, blue for unramified, and light blue and green for totally ramified extensions. We give the pictures here for $p = 2, 3, 5, 7, 11$.

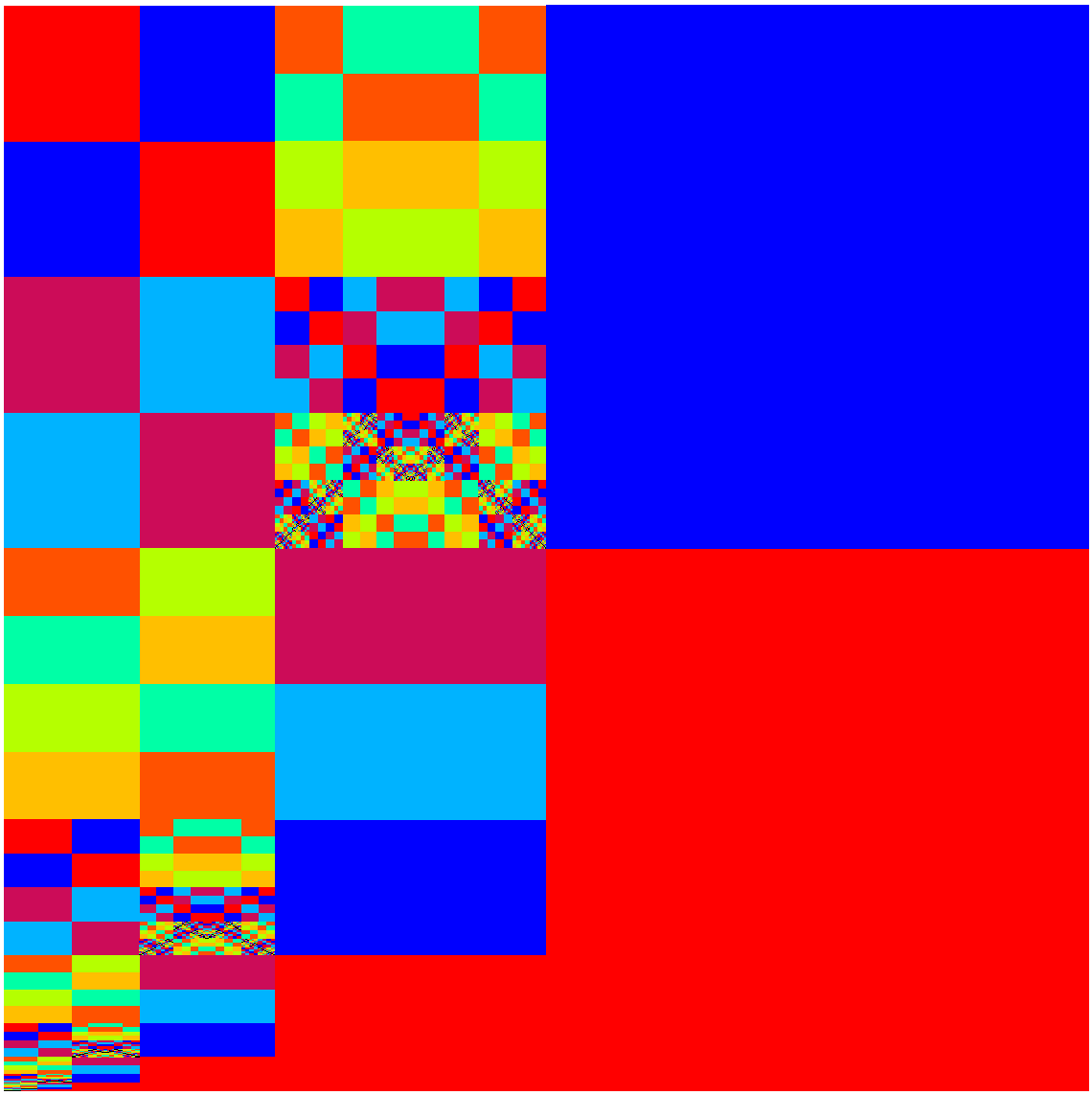


Figure 2.1: Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_2$

Looking at Figure 2.1, a few of the key details are explainable.

- In the lower right quarter, where $a \equiv 1 \bmod 2$ and $b \equiv 0 \bmod 2$, the reduced polynomial is $\overline{f}_{(a,b)}(x) \equiv x^2 + x \equiv x(x+1)$ in $\mathbb{F}_2$. So $f_{(a,b)}$ splits over $\mathbb{Q}_2$ by Hensel's Lemma. Accordingly, this entire quarter is colored red.

- In the upper right quarter, the reduced polynomial $\overline{f}_{(a,b)}(x) \equiv x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. By Proposition 28, $f_{(a,b)}$ generates the unramified extension of $\mathbb{Q}_2$. Accordingly, this entire quarter is colored blue.

- The upper half of the lower left quarter consists of all $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 4$, i.e. all Eisenstein polynomials. Accordingly, these areas are all colored magenta, light blue, or shades of green and orange for totally ramified extensions.

- The self-similar scaling and repetition going into the lower left corner is explained by looking at the discriminant of $f_{(a,b)}$. Under the scaling $(a, b) \mapsto (2a, 4b)$, the discriminant transforms by $a^2 - 4b \mapsto 4(a^2 - 4b)$, and thus the scaled polynomial generates the same algebra as the original. The entire picture is thus scaled by a factor of 2 in the a direction, and by a factor of 4 in the b direction.

In all the pictures, the areas where the "fractal" nature of the image seem to proceed indefinitely into the page correspond to the points of the discriminant variety, i.e. the points $(a, b) \in \mathbb{Z}_p^2$ such that $a^2 - 4b = 0$. Looking at Figures 2.2, 2.3, 2.4, and 2.5, similar comments can be made when p is odd.

- In the lower p^{th} section, to the right of the lower left corner square, where $a \not\equiv 0 \pmod p$ and $b \equiv 0 \pmod p$, $f_{(a,b)}$ splits over $\mathbb{Q}_p$ by Hensel's Lemma.

- Each polynomial $f_{(a,b)}$ in the left p^{th} section for which b is congruent to minus a quadratic residue modulo p splits again by Hensel's Lemma, for in this case $\overline{f}_{(a,b)}(x) \equiv x^2 - r^2$ in $\mathbb{F}_p$.

- The top $p - 1$ of the p^{th} sections of the lower left p^{th} square correspond to Eisenstein polynomials.

- It is a bit more difficult to see, but the entire picture is scaled by a factor of p in the a direction, and by a factor of p^2 in the b direction, since $(a, b) \mapsto (pa, p^2 b)$ leaves the algebra generated by $f_{(a,b)}$ unchanged.

- The isolated squares of "fractal" like self-similar behavior follow the discriminant variety, and correspond with the squares where $b \equiv a^2/4 \bmod p$.

- Except for the $a \equiv 0 \bmod p$ column, the picture has a right-left symmetry since the discriminant is invariant under the transformation $(a, b) \mapsto (-a, b)$. Really, the $a \equiv 0 \bmod p$ column itself (without the $a \equiv 0 \bmod p^2$ column) has this right-left symmetry, and so forth.

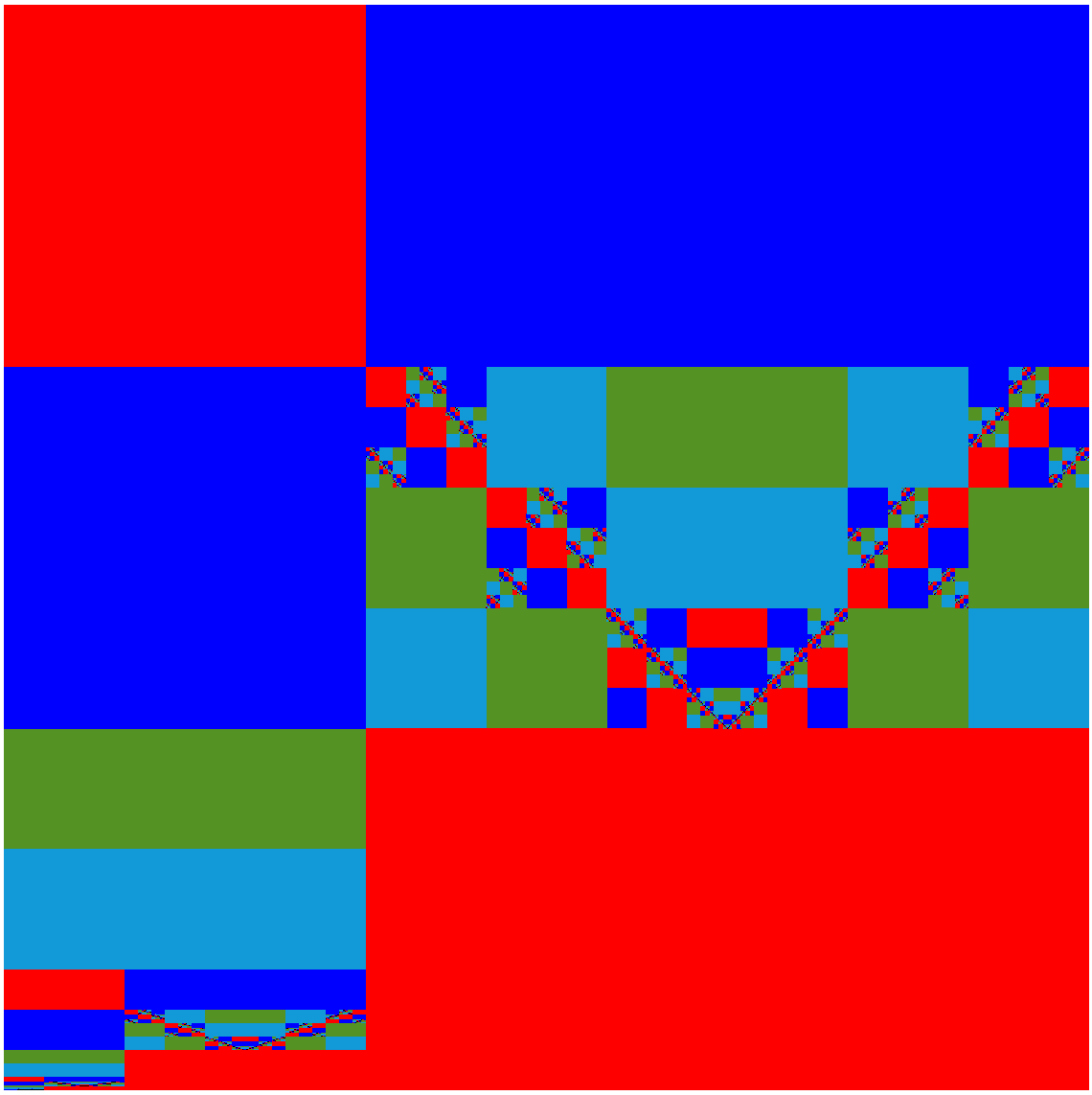


Figure 2.2: Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_3$

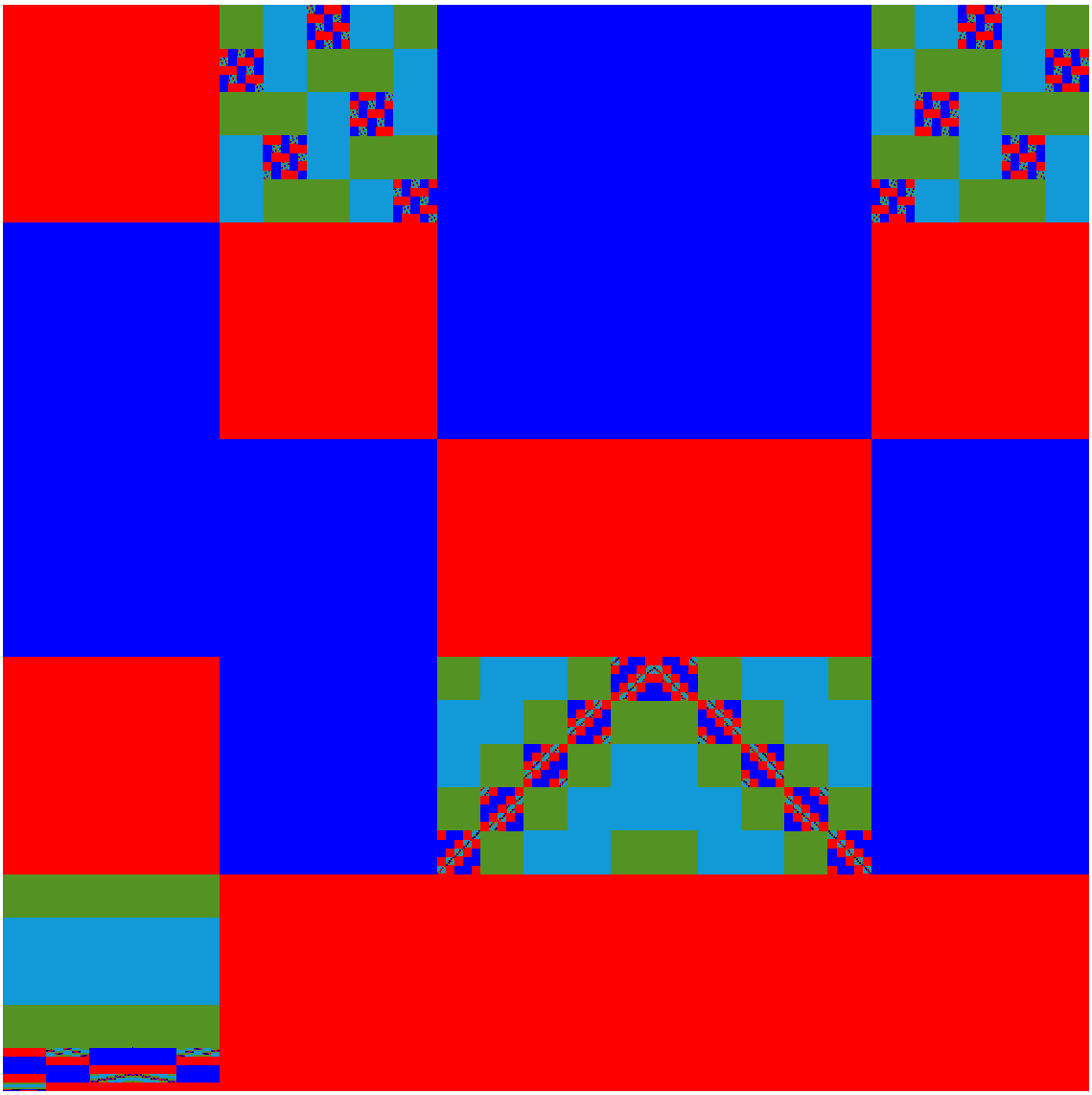


Figure 2.3: Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_5$

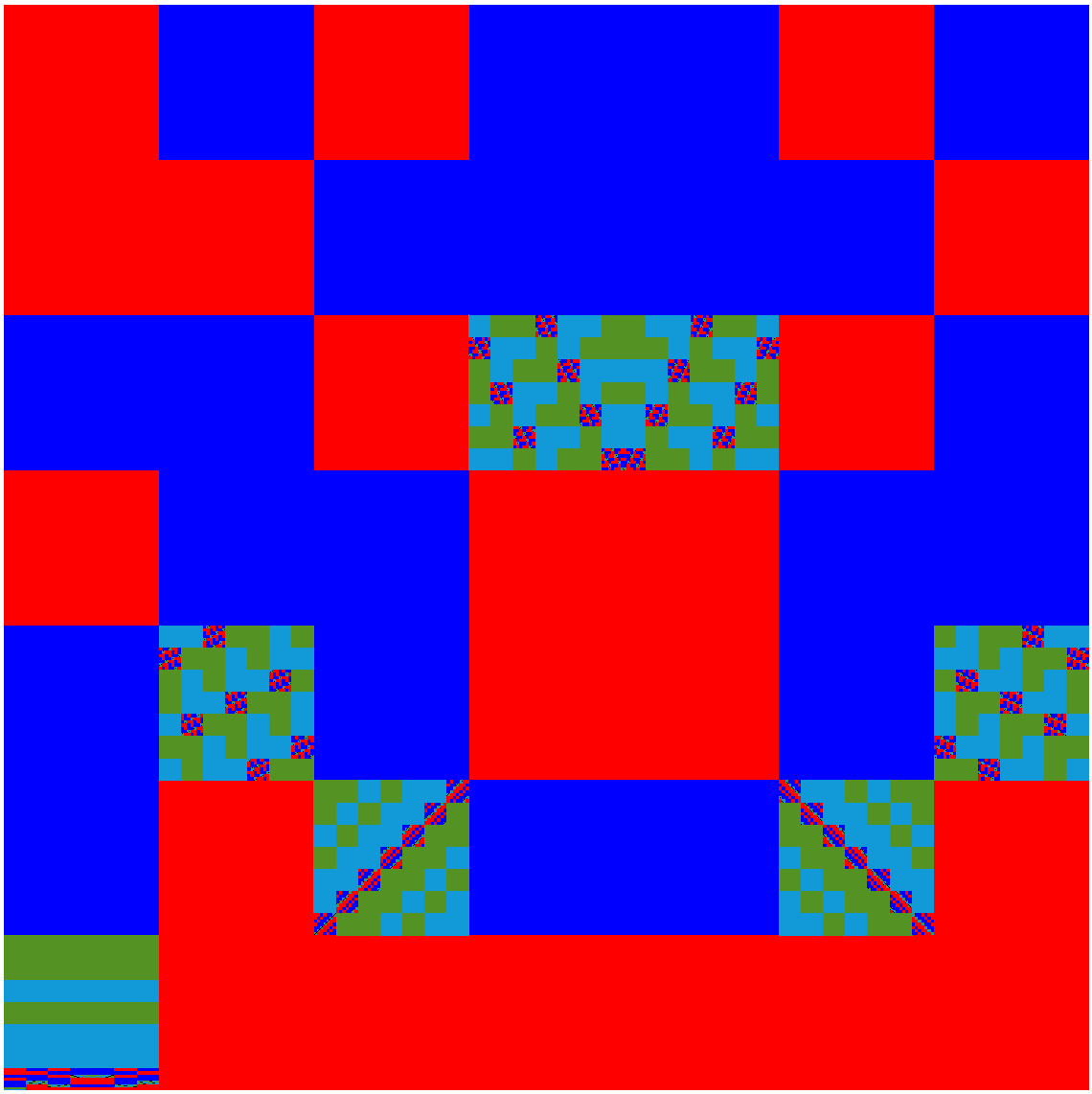


Figure 2.4: Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_7$

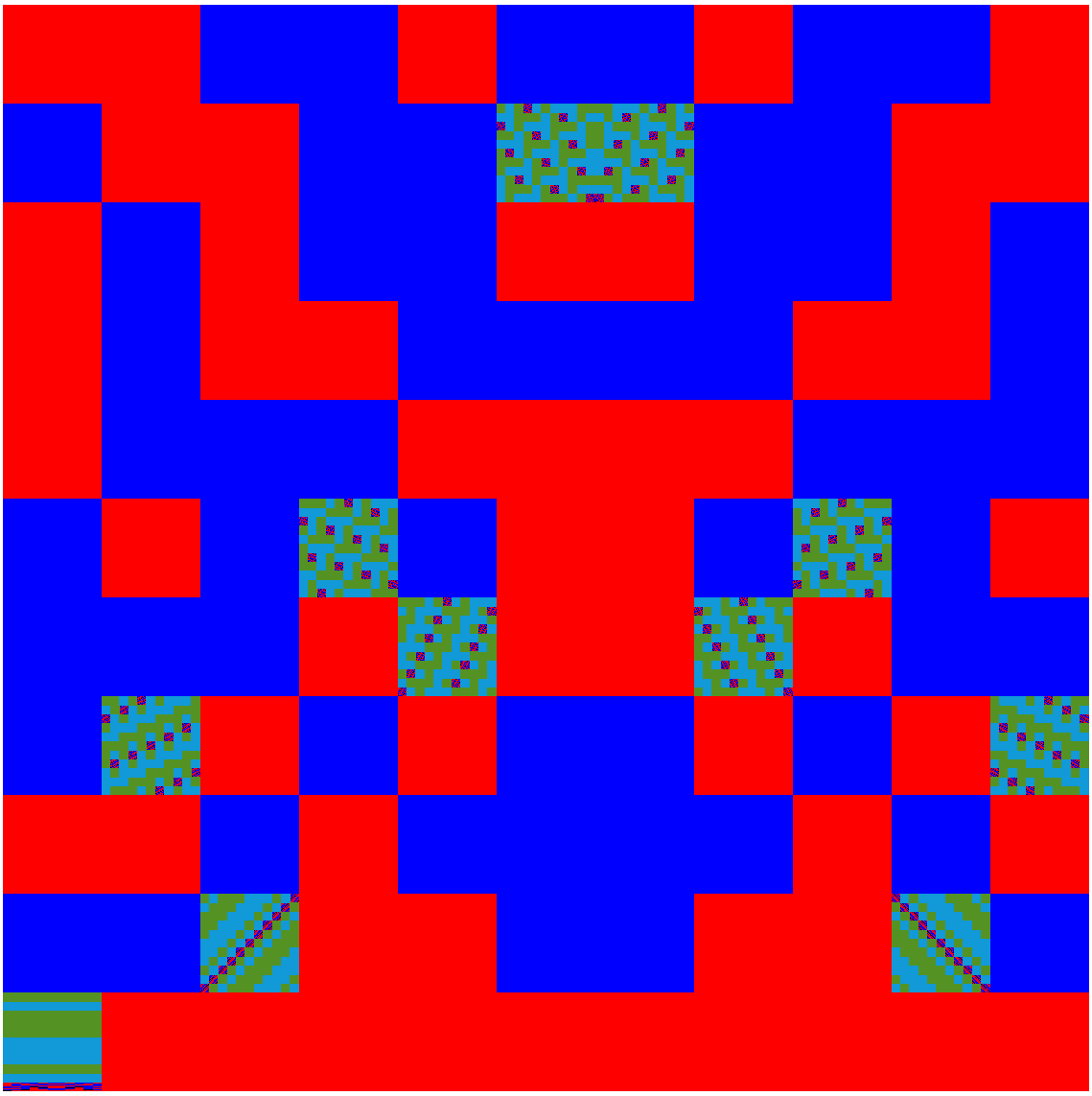


Figure 2.5: Picture of Splitting Behavior of Quadratic Polynomials over $\mathbb{Q}_{11}$

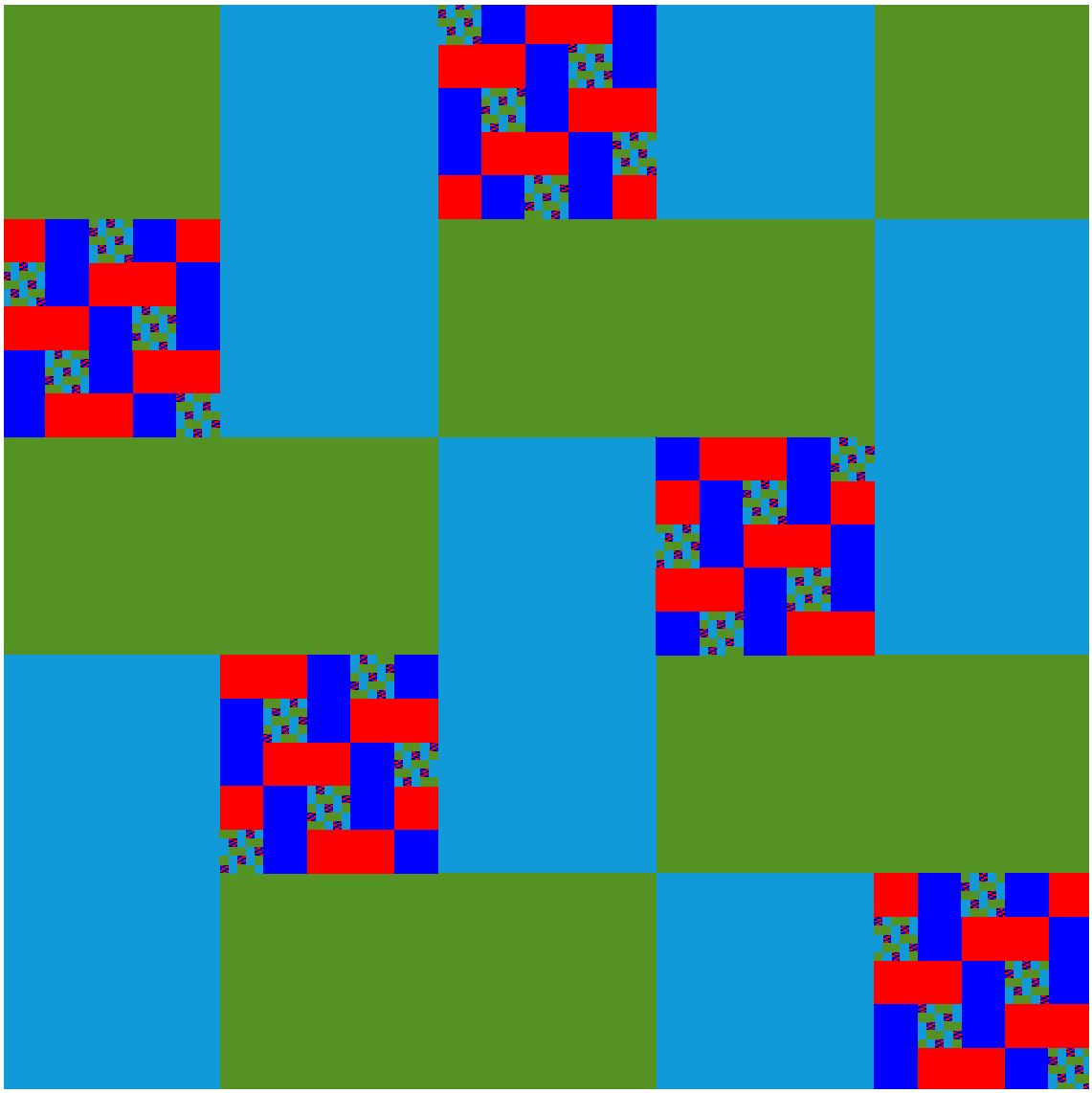


Figure 2.6: Detail of Picture 2.3 for $\mathbb{Q}_5$, where $a \equiv 1 \bmod 5$ and $b \equiv 4 \bmod 5$.

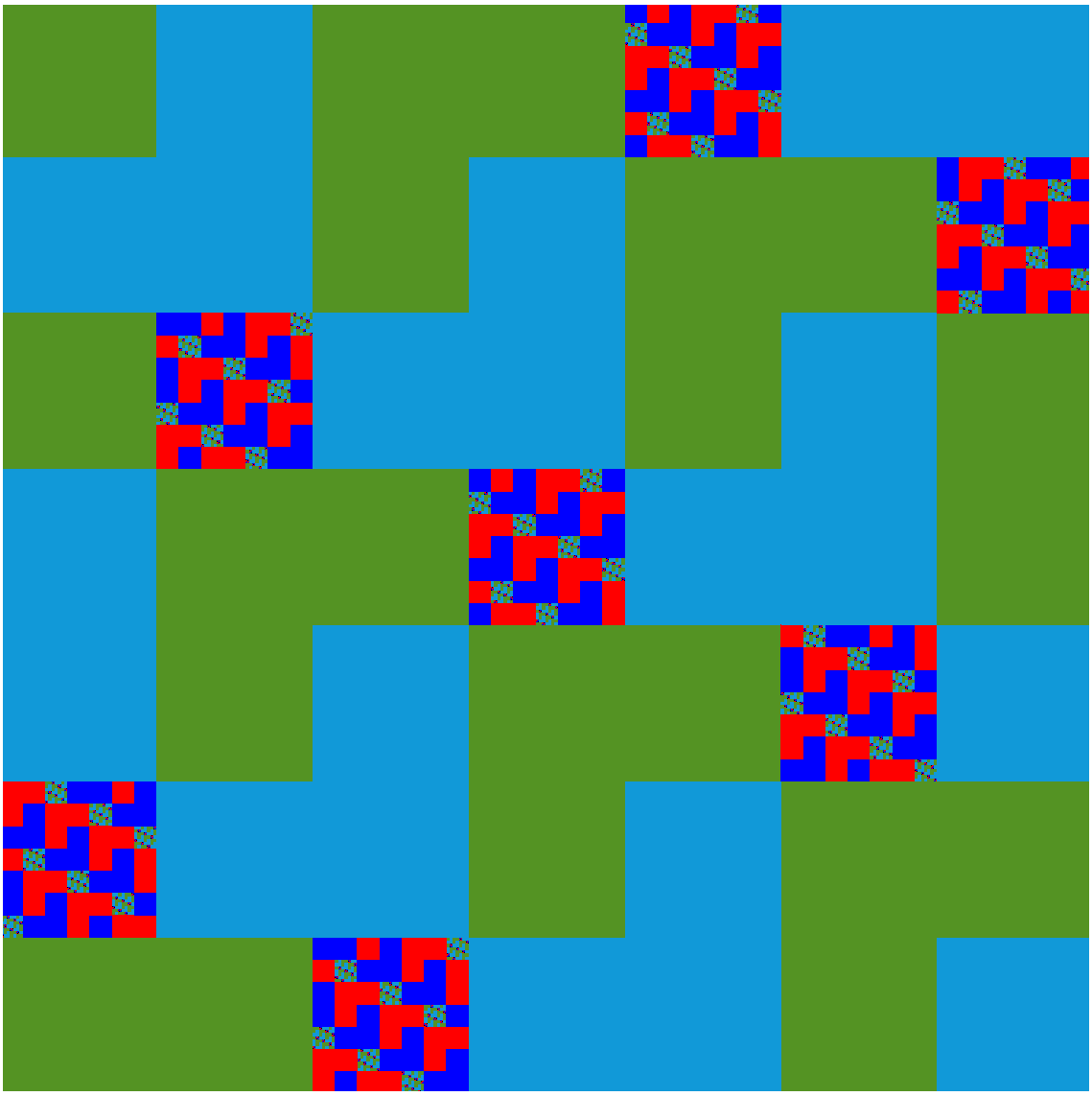


Figure 2.7: Detail of Picture 2.4 for $\mathbb{Q}_7$, where $a \equiv 6 \bmod 7$ and $b \equiv 2 \bmod 7$.

Chapter 3

Cubic Volume Computations

3.1 Cubic Polynomials in General

Irreducible Polynomials

Again, fix a local field F with ring of integers $\mathcal{O}$, prime ideal $\mathfrak{p}$, uniformizing parameter π, and residue field of order q. Let $\mathcal{P}_n(F) = \mathcal{P}_n \subset \mathcal{O}[x]$ be the set of all monic polynomials of degree n with coefficients in $\mathcal{O}$, and let $\tilde{\mathcal{P}}_n$ be those polynomials with nonzero discriminant. For an étale algebra $A \in \mathcal{A}_n(F)$, let $\mathcal{P}^A \subset \tilde{\mathcal{P}}_n$ be the set of polynomials $f \in \tilde{\mathcal{P}}_n$ for which f generates the algebra A, i.e. such that $F[x]/(f) \cong A$, and let $m_F(A) = \mu(\mathcal{P}^A)$. Following our earlier work in Section 2.2, we calculate the volume of cubic polynomials which generate a given cubic extension K of F. As always, let $\mathcal{O}_K$ be the ring of integers of K, and $\tilde{\mathcal{O}} = \mathcal{O}_K \backslash \mathcal{O}$ be the set of elements that generate K over F (again $\mu(\tilde{\mathcal{O}}_K) = \mu(\mathcal{O}_K) = 1$). For a root α of $f \in \mathcal{P}^K$, we denote by $\alpha = \alpha^{(1)}$, $\alpha^{(2)}$, and $\alpha^{(3)}$ the three conjugates of α; each generates a cubic extension $L \cong K$, and by Proposition 21, each lies in $\tilde{\mathcal{O}}_L$. Define the mapping, taking roots to minimal polynomials, $\varphi_K : \tilde{\mathcal{O}}_K \to \mathcal{P}^K$ given by

$$\varphi_K(\alpha) = (x - \alpha^{(1)})(x - \alpha^{(2)})(x - \alpha^{(3)}) = x^3 - T(\alpha)x^2 + S(\alpha)x - N(\alpha),$$

for all $\alpha \in \tilde{\mathcal{O}}_K$, and where $T(\alpha) = T_{K/F}(\alpha)$, $S(\alpha) = S_{K/F}(\alpha) = e_2(\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)})$, and $N(\alpha) = N_{K/F}(\alpha)$. As in the previous calculations, φ_K a is surjective $w(K)$-to-1 mapping (since $\varphi_K(\alpha) = \varphi_K(\alpha^{(i)})$ if $\alpha^{(i)} \in K$). Thus $m_F(K) = \mu(\varphi_K(\tilde{\mathcal{O}}_K))$, and by change of variables,

$$m_F(K) = \frac{1}{w(K)} \int_{\mathcal{O}_K} |\det(J\varphi_K)|_F \, d\mu,$$

where as always, the normalized absolute value $|\cdot|_F$ is appropriate. Now to compute $J\varphi_K$, we choose a module basis of $\mathcal{O}_K$ over $\mathcal{O}$. Writing $\mathcal{O}_K = \mathcal{O}[\beta]$ for suitable $\beta \in \mathcal{O}_K$, the induced mapping $\varphi_K : \tilde{\mathcal{O}}^3 \cong \tilde{\mathcal{O}}_K \to \mathcal{P}^K$ is given by

$$\varphi_K(a, b, c) = x^3 - T(a + b\beta + c\beta^2)x^2 + S(a + b\beta + c\beta^2)x - N(a + b\beta + c\beta^2),$$

for all $(a, b, c) \in \tilde{\mathcal{O}}^3 \cong \tilde{\mathcal{O}}_K$. We are really computing the minimal polynomial of a general element $a + b\beta + c\beta^2 \in \tilde{\mathcal{O}}_K$ in terms of indeterminates a, b, c. Letting the

minimal polynomial of β be $x^3 - Ax^2 + Bx - C \in \mathcal{O}[x]$, we are in effect computing the resultant (with the help of `Maple`),

$$\begin{aligned}
&\varphi_K(a,b,c)\\
&\quad = R_\beta(x-(a+b\beta+c\beta^2), \beta^3 - A\beta^2 + B\beta - C)\\
&\quad = x^3 - (3a + Ab + (A^2-2B)c)x^2\\
&\qquad +(3a^2 + Bb^2 + (B^2-2AC)c^2 + 2Aab + (2A^2-4B)ac + (AB-3C)bc)x\\
&\qquad -(a^3 + Cb^3 + C^2c^3 + Aa^2b + (A^2-2B)a^2c + Bab^2 + ACb^2c\\
&\qquad\quad +(B^2-2C)ac^2 + BCbc^2 + (AB-3C)abc).
\end{aligned}$$

Thus in coordinates, $\varphi_K : \tilde{\mathcal{O}}^3 \to \mathcal{P}^K \hookrightarrow \mathcal{O}^3$, we find that

$$\det(J\varphi_K(a,b,c)) = -D_K(b^3 + 2Ab^2c + (A^2+B)bc^2 + (C-AB)c^3).$$

And thus we have, integrating over the absent variable a,

$$m_F(K) = \frac{1}{w(K)q^{d(k)}} \int_{\mathcal{O}^2} |y^3 + 2Ay^2z + (A^2+B)yz^2 + (C-AB)z^3|_F \, dy\, dz. \quad (3.1)$$

Notice that the above integrand is a homogeneous polynomial of degree 3 in 2 variables. In each volume calculation so far, we define a mapping φ_A parameterizing the space of polynomials that generate a given étale algebra A over F, and we are lead to integrate the polynomial form $\det(J\varphi_K)$. The discriminant of the algebra has been a common factor in our forms so far, so without this factor, we will call this form the *index form*, or I_A, of the algebra A. For example, the index form of a general cubic extension of F is the integrand in Equation 3.1. The index form of a number field was independently defined and studied by Kronecker and Hensel, who called it the "*Fundamental-diskriminante*," and it is interesting that it arises in this context. See [7] for an overview of its uses in computing integral bases of number fields.

Reducible Polynomials

We compute one more index form explicitly here. To completely cover the splitting behavior of all monic cubic polynomials, we need to consider splittings into a linear factor and an irreducible quadratic. This type of polynomial generates the algebra $A = F \oplus K$ over F, where K is a quadratic extension of F. Let $\mathcal{O}_A = \mathcal{O} \oplus \mathcal{O}_K$, and define $\tilde{\mathcal{O}}_A = \mathcal{O} \oplus \tilde{\mathcal{O}}_K$. Once more, define the mapping, taking roots to polynomials with those roots, $\varphi_A : A = \tilde{\mathcal{O}}_A \to \mathcal{P}^A$ given by

$$\varphi_A(a,\alpha) = (x-a)(x-\alpha)(x-\alpha') = x^3 - (T(\alpha)+a)x^2 + (aT(\alpha)+N(\alpha))x - aN(\alpha),$$

for all $(a,\alpha) \in \mathcal{O} \oplus \tilde{\mathcal{O}}_K$. This is a surjective 2-to-1 mapping (since $\varphi(a,\alpha) = \varphi(a,\alpha')$). In this case we say that $w(A) = 2$. In general, one must be careful in defining the set of automorphisms of an étale algebra. To compute the index form for the algebra A, we choose a module basis of $\mathcal{O}_K$ over $\mathcal{O}$. Writing $\mathcal{O}_K = \mathcal{O}[\beta]$

for suitable $\beta \in \mathcal{O}_K$ with minimal polynomial $x^2 - Bx + C \in \mathcal{O}[x]$, in coordinates, $\varphi_K : \tilde{\mathcal{O}}^3 \cong \mathcal{O} \times \tilde{\mathcal{O}}_K \to \mathcal{P}^K \hookrightarrow \mathcal{O}^3$ is given by

$$\begin{aligned}\varphi_A(a,b,c) &= (-a - T(b+c\beta), aT(b+c\beta) + N(b+c\beta), -aN(b+c\beta)) \\ &= (-(a+2b+Bc), 2ab + Bac + b^2 + Bbc + Cc^2, -(ab^2 + Babc + Cac^2)),\end{aligned}$$

for $(a,b,c) \in \tilde{\mathcal{O}}^3$. This time, we find that

$$\det(J\varphi_A(a,b,c)) = -D_K c(a^2 + b^2 + Cc^2 - 2ab - Bac + Bbc).$$

In the above two cubic cases, evaluating the necessary integral seems difficult for a general local field F, thus we proceed for $\mathbb{Q}_p$, with explicit generating polynomials. The index form of a general algebra seems to become increasingly complicated as the degree of the algebra gets larger. We organize the index forms computed so far into Table 3.1, and include the "completely split" index form of the étale algebra F^3, to be computed in general in Chapter 4, for completeness.

Structure	Generating Polynomial	Index Form, $I_A(a,b,c)$
2	$x^2 - Ax + B$	b
$1 \cdot 1$	$(x-A)(x-B)$	$a - b$
3	$x^3 - Ax^2 + Bx - C$	$b^3 + 2Ab^2c + (A^2+B)bc^2 + (C - AB)c^3$
$1 \cdot 2$	$(x-A)(x^2 - Bx + C)$	$c(a^2 + b^2 + Cc^2 - 2ab - Bac + Bbc)$
$1 \cdot 1 \cdot 1$	$(x-A)(x-B)(x-C)$	$(a-b)(a-c)(b-c)$

Table 3.1: Index Forms of Quadratic and Cubic Étale Algebras

3.2 Explicit Computations for Cubics over $\mathbb{Q}_p$

To determine the structure of $\mathcal{A}_3(\mathbb{Q}_p)$, we first need to know the cubic extensions of $\mathbb{Q}_p$, which are given by the following:

Proposition 45.

- The field $\mathbb{Q}_3$ has a unique unramified C_3 extension, 3 nonisomorphic totally ramified C_3 extensions, and 6 nonisomorphic totally ramified S_3 extensions.
- For $p \equiv 1 \bmod 3$, the field $\mathbb{Q}_p$ has a unique unramified C_3 extension, and 3 non-isomorphic totally ramified C_3 extensions.
- For $p \equiv 2 \bmod 3$, the field $\mathbb{Q}_p$ has a unique unramified C_3 extension, and a unique totally ramified S_3 extension.

See [6], Chp. VI for a proof using local class field theory, noting the error in the proposition on p. 57 regarding the case $p \equiv 1 \bmod 3$ which is corrected here (in this case, $3 \mid p-1$, thus $\mathbb{Q}_p$ does in fact contain the third roots of unity; see [8], Chp. 3.4 or [15], Chp. 6.7).

Case $p \equiv 1 \bmod 3$

Using Hensel's Lemma and methods similar to those in Section 1.3, we can show that in this case, any cube in $\mathbb{Z}_p$ has the form $r + p\mathbb{Z}_p$ for some r that is a cube in $\mathbb{F}_p$. The cubes in $\mathbb{F}_p$ make up a subgroup of index 3, with lifted representatives 1, b, and b^2. Thus we have $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^3 = \{1, b, b^2, p, bp, b^2p, p^2, bp^2, b^2p^2\}$, where many of the cube roots of these elements generate isomorphic extensions. The element $\sqrt[3]{b}$ generates a model of the unique unramified cubic extension of $\mathbb{Q}_p$, and the 3 nonisomorphic totally ramified extensions with Galois group C_3 can be generated by $\sqrt[3]{p}$, $\sqrt[3]{bp}$, and $\sqrt[3]{b^2p}$. The unramified case will be taken care of in general in Chapter 4.

Let $K = \mathbb{Q}_p(\sqrt[3]{ap})$, where a equals 1, b, or b^2. Each extension K has Galois group C_3, thus $w(K) = 3$, and $d(K) = v_p(\mathrm{discr}(x^3 - ap)) = v_p(-27a^2p^2) = 2$. By Table 3.1, we have $I_K(x, y, z) = I_K(y, z) = y^3 + apz^3$, so by Equation 3.1,

$$m_{\mathbb{Q}_2}(K) = \frac{1}{3}\int_{\mathbb{Z}_p^3} |-D_K(y^3 + apz^3)|_p \, dx\, dy\, dz = \frac{1}{3}p^{-2}\int_{\mathbb{Z}_p^2} |y^3 + apz^3|_p \, dy\, dz = \frac{1}{3}I.$$

Using the standard decomposition, we have,

$$I = \sum_{(i,j)\in\{0,\ldots,p-1\}^2} I_{ij},$$

where we define

$$\begin{aligned} I_{ij} &= \int_{(i+p\mathbb{Z}_p)\times(j+p\mathbb{Z}_p)} |y^3 + apz^3|_p \, dy\, dz \\ &= p^{-2}\int_{\mathbb{Z}_p^2} |I_K^{ij}|_p \, dy\, dz, \end{aligned}$$

$$I_K^{ij} = I_K(i + py, j + pz) = i^3 + apj^3 + 3apyi^2 + p^2P(y, z),$$

for some polynomial $P(y, z)$. Now from the above we clearly see that

$$|I_K^{ij}|_p = \begin{cases} 1 & \text{if } i \neq 0 \\ p^{-1} & \text{if } i = 0,\ j \neq 0 \\ p^{-3}|I_K(y, z)|_p & \text{if } i = j = 0 \end{cases}, \tag{3.2}$$

and thus we have,

$$\begin{aligned} I &= p^{-2}(p(p-1) + p^{-1}(p-1) + p^{-3}I) \\ &= \frac{p^2(p-1) + p - 1}{p^3}\frac{1}{1-p^{-5}} = \frac{p^2(p-1)(p^2+1)}{p^5-1}, \end{aligned} \tag{3.3}$$

so finally

$$m_{\mathbb{Q}_p}(K) = \frac{1}{3}\frac{(p-1)(p^2+1)}{p^5-1}, \quad \text{for } K = \mathbb{Q}_p(\sqrt[3]{ap}). \tag{3.4}$$

Case $p \equiv 2 \bmod 3$

In this case, every element of $\mathbb{F}_p$ is a cube. The unique totally ramified extension K can be generated by $\sqrt[3]{p}$. Since it has Galois group S_3, $w(K) = 1$. Besides this, the rest follows exactly as in the previous computation. So we have,

$$m_{\mathbb{Q}_p}(K) = \frac{(p-1)(p^2+1)}{p^5-1}, \quad \text{for } K = \mathbb{Q}_p(\sqrt[3]{p}). \tag{3.5}$$

Case $p = 3$

In this case, Table 3.2 gives a list of polynomials that generate the various nonisomorphic extensions of $\mathbb{Q}_3$. The right-hand side of this table is taken from [6], p. 66.

Polynomial	$d(K)$	Polynomial	$d(K)$
Unique Unramified C_3 Extension		Totally Ramified S_3 Extensions	
x^3+2x+1	0	x^3+3x+3	3
Totally Ramified C_3 Extensions		x^3-3x-3	3
x^3+3x^2-3	4	x^3+3x^2+3	4
x^3-3x^2-6	4	x^3+9x+3	5
x^3-6x^2+6	4	x^3-9x+3	5
		x^3+3	5

Table 3.2: Generating Polynomials of Cubic Extensions of $\mathbb{Q}_3$

We proceed just as in the above cases, and again, leaving the unramified case for later. In fact, the analysis of the index forms of the totally ramified extensions is exactly as in Equation 3.2, and thus the integral computation is exactly as in Equation 3.3. The only differences here are the discriminants and the number of automorphisms of the extensions. For each totally ramified cubic extension K over $\mathbb{Q}_3$ we have,

$$m_{\mathbb{Q}_3}(K) = \frac{1}{w(K)q^{d(K)}}\frac{2\cdot 3^2\cdot 5}{11^2}. \tag{3.6}$$

Reducible Polynomials

Case p odd

In this case, the set of isomorphism classes of quadratic extensions is $\mathcal{A}_2(\mathbb{Q}_p) = \{\mathbb{Q}_p(\sqrt{a}),\ \mathbb{Q}_p(\sqrt{p},\ \mathbb{Q}_p(\sqrt{ap})\}$ for some nonsquare a mod p. Let $A = \mathbb{Q}_p \oplus \mathbb{Q}(\sqrt{d})$, where d is equal to a, p, or ap. The volume $m_{\mathbb{Q}_p}(A)$ can be computed similarly as above. By Table 3.1, we have $I_A(x,y,z) = z(x^2+y^2-dz^2-2xy)$, so by Equation 3.1,

$$m_{\mathbb{Q}_p}(A) = \frac{1}{2\cdot 2^{-d(A)}}\int_{\mathbb{Z}_p^3} |I_A(x,y,z)|_p\, dx\, dy\, dz = \frac{1}{2\cdot 2^{-d(A)}} I.$$

Again, using the standard decomposition, we have,

$$I = \sum_{(i,j,k)\in\{0,\ldots,p-1\}^3} I_{ijk},$$

where we define

$$\begin{aligned} I_A^{ijk} &= I_A(i+px, j+py, k+pz) \\ &= (k+pc)\{(i-j)^2 - dk^2 + 2p((j-i)y + (i-j)x - dkz) \\ &\qquad +p^2 I_A(x,y,z)\}. \end{aligned} \tag{3.7}$$

Case where $d = a$ is a nonquadratic residue modulo p

In this case, $\sqrt{d}$ generates the unramified extension over $\mathbb{Q}_p$, and generates $\mathcal{O}_K$ over $\mathbb{Z}_p$, and

$$|I_A^{ijk}|_p = \begin{cases} 1 & \text{if} \quad k \neq 0 \\ p^{-1}|c|_p & \text{if} \quad k = 0,\ i \neq j \\ p^{-3}|I_A(x,y,z)|_p & \text{if} \quad k = 0,\ i = j \end{cases}.$$

To see this, note that in Equation 3.7, if $k \neq 0$, then we need consider only the "inside" term, and

$$(i-j)^2 \equiv dk^2 \bmod p, \tag{3.8}$$

is impossible since d is a nonquadratic residue modulo p, so in this case, $|I_A^{ijk}|_p = 1$. If $k = 0$, but $i \neq j$, then again Equation 3.8 applies and the "inside" term has valuation 0, so we are left with just $|pc|_p$. When $k = 0$ and $i = j$, Equation 3.7 reduces to $I_A^{000} = p^3 I_A(x,y,z)$, thus we have, recalling the calculation in Example 15,

$$I = q^{-3}\left(p^2(p-1) + (p^2-p)\cdot p^{-1}\frac{p}{p+1} + p\cdot p^{-3} I\right) = \frac{p^3(p-1)(p^2+p+1)}{(p+1)(p^5-1)},$$

and so finally,

$$m_{\mathbb{Q}_p}(A) = \frac{1}{2}\frac{p^3(p-1)(p^3-1)}{(p^2-1)(p^5-1)}, \quad \text{for } A = \mathbb{Q}_p \oplus \mathbb{Q}_p(\sqrt{a}). \tag{3.9}$$

Case where $d = p, ap$

In this case, $\sqrt{d}$ generates a totally ramified extension, and

$$|I_A^{ijk}|_p = \begin{cases} 1 & \text{if} \quad k \neq 0,\ i \neq j \\ p^{-1} & \text{if} \quad k \neq 0,\ i = j \\ p^{-1}|c|_p & \text{if} \quad k = 0,\ i \neq j \\ p^{-3}|I_A(x,y,z)|_p & \text{if} \quad k = 0,\ i = j \end{cases}.$$

To see this, let t be either 1 or a, and stare at

$$I_A^{ijk} = (k+pc)\{(i-j)^2 + p(2(j-i)y + 2(i-j) + tk^2) + p^2(tk + I_A(x,y,z)\}.$$

Thus we have, again recalling the calculation in Example 15,

$$\begin{aligned} I &= p^{-3}\left((p-1)(p^2-p) + (p-1)p\cdot p^{-1} + (p^2-p)\cdot p^{-1}\frac{p}{p+1} + p\cdot p^{-3}I\right) \\ &= \frac{p^2(p-1)(p^3+p+1)}{(p+1)(p^5-1)}, \end{aligned}$$

and so finally

$$m_{\mathbb{Q}_p}(A) = \frac{1}{2}\frac{p(p-1)(p^3+p+1)}{(p+1)(p^5-1)}, \quad \text{for } A = \mathbb{Q}_p \oplus \mathbb{Q}_p(\sqrt{tp}),\ t = 0, a. \tag{3.10}$$

Case $p = 2$

This case is special because of the exceptional structure of the quadratic extensions of $\mathbb{Q}_2$, we have $\mathcal{A}(\mathbb{Q}_2) = \{\mathbb{Q}_2^2\} \cup \{\mathbb{Q}_2(\sqrt{a}) : a = 2, 3, 5, 6, 7, 10, 14\}$.

Recalling the discussion after Corollary 40, the unique unramified quadratic extension $K = \mathbb{Q}_2(\sqrt{5})$ has ring of integers $\mathcal{O}_K$ generated over $\mathbb{Z}_2$ by a root of $x^2 - x - 1$. By Table 3.1 we have $I_A(x,y,z) = z(x^2 + y^2 - z^2 - 2xy - xz + yz)$, and so

$$m_{\mathbb{Q}_2}(A) = \frac{1}{2}\int_{\mathbb{Z}_2^3} |I_A(x,y,z)|_2 \, dx\, dy\, dz = \frac{1}{2}I,$$

where we make the similar definitions

$$I = \sum_{(i,j,k)\in\{0,1\}^3} I_{ijk},$$

and

$$\begin{aligned} I_A^{ijk} &= I_A(i+2x, j+2y, k+2z) \\ &= (k+2z)(i^2+j^2-k^2-ik+jk+2(-ij-kx-iz+ky+jz) \\ &\quad +4((i-j)a + (j-i)b + I_A(x,y,z))). \end{aligned} \tag{3.11}$$

By Equation 3.11, we have

$$|I_A^{ijk}|_2 = \begin{cases} 1 & \text{if } k \neq 0 \\ 2^{-1}|z|_2 & \text{if } k = 0,\ (i,j) \neq (1,1) \\ 2^{-3}|I_A(x,y,z)|_2 & \text{if } (i,j,k) = (0,0,0),\ (1,1,0) \end{cases},$$

and so it follows, again recalling the calculation in Example 15, that

$$I = 2^{-3}\left(4 + 2\cdot 2^{-1}\frac{2}{3} + 2\cdot 2^{-3}I\right) = \frac{2^3\cdot 7}{3\cdot 31},$$

and so

$$m_{\mathbb{Q}_2}(A) = \frac{2^2 \cdot 7}{3 \cdot 31}, \quad \text{for } A = \mathbb{Q}_2 \oplus \mathbb{Q}_2(\sqrt{a}). \tag{3.12}$$

The rest of the volumes are computed similarly to the odd p totally ramified cases, since the generating element is still a square root. Only the discriminants of the extensions and the number of them is different.

Finally, we compile all this data into Table 3.3. We will compute the volume for completely split polynomials and for polynomials generating the unramified extension in general in Chapter 4, but will include the data here for completeness. Let $\mathbb{Q}_p(\zeta)$ denote the cubic unramified extension of $\mathbb{Q}_p$. Quite expectedly, the sum over all of $\mathcal{A}_3(\mathbb{Q}_p)$ of these formulae, given as rational functions in p, is 1. When checking this, make sure to count for the multiplicity of extensions in each line of the table.

Cubic algebra A over $\mathbb{Q}_p$	Generating polynomial	$w(A)$	$d(A)$	$m_{\mathbb{Q}_p}(A)$
$p=2$				
$\mathbb{Q}_2^3$	$(x-A)(x-B)(x-C)$	6	0	$\frac{2^2}{3\cdot 31}$
$\mathbb{Q}_2 \times \mathbb{Q}_2(\sqrt{5})$	$(x-A)(x^2-x-1)$	2	0	$\frac{2^2\cdot 7}{3\cdot 31}$
$\mathbb{Q}_2 \times \mathbb{Q}_2(\sqrt{d})$, $d=3,7$	$(x-A)(x^2-d)$	2	2	$\frac{11}{2\cdot 3\cdot 31}$
$\mathbb{Q}_2 \times \mathbb{Q}_2(\sqrt{d})$, $d=2,6,10,14$	$(x-A)(x^2-d)$	2	3	$\frac{11}{2^2\cdot 3\cdot 31}$
$\mathbb{Q}_2(\zeta)$	x^3+x-1	3	0	$\frac{2^3}{31}$
$\mathbb{Q}_2(\sqrt[3]{2})$	x^3-2	1	2	$\frac{5}{31}$
$p=3$				
$\mathbb{Q}_3^3$	$(x-A)(x-B)(x-C)$	6	0	$\frac{3^2\cdot 7}{2^3\cdot 11^2}$
$\mathbb{Q}_3 \times \mathbb{Q}_3(\sqrt{2})$	$(x-A)(x^2-2)$	2	0	$\frac{3^3\cdot 13}{2^3\cdot 11^2}$
$\mathbb{Q}_3 \times \mathbb{Q}_3(\sqrt{3t})$, $t=1,2$	$(x-A)(x^2-3t)$	2	1	$\frac{3\cdot 31}{2^3\cdot 11^2}$
$\mathbb{Q}_3(\zeta)$	x^3+2x+1	3	0	$\frac{2^2\cdot 3^2}{11^2}$
$\mathbb{Q}_3(\pi_i)$, $i=1,2,3$ (C_3)	see Table 3.2	3	4	$\frac{2\cdot 5}{3^3\cdot 11^2}$
$\mathbb{Q}_3(\pi_i)$, $i=1,2$ (S_3)	see Table 3.2	1	3	$\frac{2\cdot 5}{3\cdot 11^2}$
$\mathbb{Q}_3(\pi)$ (S_3)	x^3+3x^2+3	1	4	$\frac{2\cdot 5}{3^2\cdot 11^2}$
$\mathbb{Q}_3(\pi_i)$, $i=1,2,3$ (S_3)	see Table 3.2	1	5	$\frac{2\cdot 5}{3^3\cdot 11^2}$
$p \equiv 1 \mod 3$				
$\mathbb{Q}_p^3$	$(x-A)(x-B)(x-C)$	6	0	$\frac{1}{6}\frac{p^3(p-1)(p^2-p+1)}{(p+1)(p^5-1)}$
$\mathbb{Q}_p \times \mathbb{Q}_p(\sqrt{a})$	$(x-A)(x^2-a)$	2	0	$\frac{1}{2}\frac{p^3(p-1)(p^2+p+1)}{(p+1)(p^5-1)}$
$\mathbb{Q}_p \times \mathbb{Q}_p(\sqrt{tp})$, $t=1,a$	$(x-A)(x^2-ap)$	2	1	$\frac{1}{2}\frac{p(p-1)(p^3+p+1)}{(p+1)(p^5-1)}$
$\mathbb{Q}_p(\zeta)$	Irred. cubic mod p	3	0	$\frac{1}{3}\frac{p^3(p-1)(p+1)}{p^5-1}$
$\mathbb{Q}_p(\sqrt[3]{ap})$, $a=1,b,b^2$	x^3-ap	3	2	$\frac{1}{3}\frac{(p-1)(p^2+1)}{p^5-1}$
$p \equiv 2 \mod 3$				
$\mathbb{Q}_p^3$	$(x-A)(x-B)(x-C)$	6	0	$\frac{1}{6}\frac{p^3(p-1)(p^2-p+1)}{(p+1)(p^5-1)}$
$\mathbb{Q}_p \times \mathbb{Q}_p(\sqrt{a})$	$(x-A)(x^2-a)$	2	0	$\frac{1}{2}\frac{p^3(p-1)(p^2+p+1)}{(p+1)(p^5-1)}$
$\mathbb{Q}_p \times \mathbb{Q}_p(\sqrt{tp})$, $t=1,a$	$(x-A)(x^2-ap)$	2	1	$\frac{1}{2}\frac{p(p-1)(p^3+p+1)}{(p+1)(p^5-1)}$
$\mathbb{Q}_p(\zeta)$	Irred. cubic mod p	3	0	$\frac{1}{3}\frac{p^3(p-1)(p+1)}{p^5-1}$
$\mathbb{Q}_p(\sqrt[3]{p})$	x^3-p	1	2	$\frac{(p-1)(p^2+1)}{p^5-1}$

Table 3.3: Volumes for Cubic Étale Algebras over $\mathbb{Q}_p$

Chapter 4

General Volume Computations

Fix a local field F with ring of integers $\mathcal{O}$, prime ideal $\mathfrak{p}$, separable closure F^{sep}, and let $\mathcal{A}_n(F)$ be the set of isomorphism classes of étale algebras of degree n over F inside a fixed F^{sep}. Recall that $\mathcal{P}_n(F) = \mathcal{P}_n \subset \mathcal{O}[x]$ is the set of monic degree n polynomials with coefficients in $\mathcal{O}$. Let $\tilde{\mathcal{P}}_n \subset \mathcal{P}_n$ be those polynomials with nonzero discriminant, and for $A \in \mathcal{A}_n(F)$ define $\mathcal{P}^A \subset \tilde{\mathcal{P}}_n$ to be those polynomials that generate A, i.e. such that $A \cong F[x]/(f)$.

The set of polynomials $\mathcal{P}_n$ has a natural compact group structure under the isomorphism

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \mapsto (a_1, \ldots, a_n) \in \mathcal{O}^n : \mathcal{P}_n \to \mathcal{O}^n,$$

with normalized Haar measure $\mu = \mu_F^{\otimes n}$ inherited from F^n. We have $\mu(\mathcal{P}_n) = \mu(\tilde{\mathcal{P}}_n)$, since the set of polynomials with zero discriminant has measure zero. Also define $\tilde{\mathcal{O}}^n \cong \tilde{\mathcal{P}}^A$ by the above isomorphism. By Krasner's Lemma (Lemma 36), the set $\mathcal{P}^A$ is an open subset inside $\mathcal{P}_n$. Indeed, let $\alpha \in A$ generate A over F. Since each coefficient of the generating polynomial of α is a polynomial function of its conjugates (and hence is a continuous function of α), another generating element β, which is nearby by Krasner's Lemma, has coefficients of its minimal polynomial nearby to those of α.

Definition 46. Let K be a separable extension F of degree n. Call $\alpha \in K$ a *primitive element* if $K = F(\alpha)$ or equivalently, if α is not contained in any proper separable subfield of K, and denote by $\tilde{K}$ the set of all primitive elements of K, $\tilde{\mathcal{O}}_K = \tilde{K} \cap \mathcal{O}_K$, and define the corresponding notions $\tilde{A}$ and $\tilde{\mathcal{O}}_A$ for an étale algebra $A \in \mathcal{A}_n$.

Note once more that since separable subfields are lower dimensional vector subspaces, we have $\mu(\tilde{\mathcal{O}}_A) = \mu(\mathcal{O}_A) = 1$.

4.1 The Index Form of an Algebraic Extension

We restrict to the case when $A = K$ is an extension of F. Then define the mapping, taking elements to their minimal polynomials, $\varphi_K : \tilde{\mathcal{O}}_K \to \mathcal{P}^K$, given by

$$\varphi_K(\alpha) = N_{K/F}(x - \alpha) = \prod_{\sigma \in H} (x - \sigma\alpha), \quad \text{for all } \alpha \in \tilde{\mathcal{O}}_K,$$

where $H = \mathrm{Hom}_F(K, F^{\mathrm{sep}})$ is the set of embeddings of K into a fixed F^{sep} . Note that indeed $\mathrm{discr}(\varphi_K(\alpha)) \neq 0$ for all $\alpha \in \tilde{\mathcal{O}}_K$, and that φ_K is a surjective $w(K)$-to-1 mapping (since $\varphi_K(\alpha) = \varphi_K(\alpha')$ if and only if $\alpha' = \sigma\alpha \in K$ for some $\sigma \in \mathrm{Aut}_F(K)$). The mapping is also F-analytic since it is a polynomial mapping as we shall see. Now under the natural isomorphisms $\mathcal{O}_K \xrightarrow{\sim} \mathcal{O}^n$, and $\mathcal{P}_n(F) \xrightarrow{\sim} \mathcal{O}^n$ we have the induced mapping

$$\begin{array}{ccc} \tilde{\mathcal{O}}^n & \xrightarrow{\varphi_K} & \tilde{\mathcal{O}}^n \\ \wr\uparrow & & \wr\uparrow \\ \tilde{\mathcal{O}}_K & \xrightarrow{\varphi_K} & \mathcal{P}^K \end{array}$$

so that $m_F(K) = \mu(\mathcal{P}_K) = \mu(\varphi_K(\tilde{\mathcal{O}}^n))$. By the change of variables theorem (Theorem 18),

$$m_F(K) = \int_{\varphi_K(\tilde{\mathcal{O}}^n)} \mathbf{1}\, d\mu = \frac{1}{w(K)} \int_{\mathcal{O}^n} |\det(J\varphi_K)|_F \, d\mu. \tag{4.1}$$

To compute $\det(J\varphi_K)$, we first note that $\varphi_K : \tilde{\mathcal{O}}_K \to \tilde{\mathcal{O}}^n$ is given by,

$$\varphi_K(\alpha) = \boldsymbol{e}(\boldsymbol{\sigma}(\alpha)), \quad \text{for all } \alpha \in \tilde{\mathcal{O}}_K,$$

where $\boldsymbol{e} : \mathcal{O}_K^n \to \mathcal{O}_K^n$ is the elementary symmetric function mapping defined by

$$\boldsymbol{e}(x) = (e_1(x), \ldots, e_n(x)), \quad \text{for all } x \in \mathcal{O}_K^n,$$

and $\boldsymbol{\sigma} : \mathcal{O}_K \to \mathcal{O}_K^n$ is defined by

$$\boldsymbol{\sigma}(\alpha) = (\sigma_1\alpha, \ldots, \sigma_n\alpha), \quad \text{for all } \alpha \in \mathcal{O}_K,$$

where $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_F(K, F^{\mathrm{sep}})$.

Now, by Theorem 22, choose a generating element $\beta \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O}[\beta] \cong \mathcal{O}^n$. Then we have

$$\boldsymbol{\sigma}(\alpha) = \boldsymbol{\sigma}(a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}) = (\sigma_i\beta^j)a,$$

where $a = (a_1, \ldots, a_n) \in \mathcal{O}^n$, and where $(\sigma_i\beta^j)$ denotes the obvious $n \times n$ Vandermonde matrix. Thus the induced mapping $\boldsymbol{\sigma} : \mathcal{O}_K \cong \mathcal{O}^n \to \mathcal{O}_K^n$ is linear, and we have

$$\varphi_K(a) = \boldsymbol{e}((\sigma_i\beta^j)a), \quad \text{for all } a \in \tilde{\mathcal{O}}^n.$$

Lemma 47. For all $x \in \mathcal{O}_K^n$, we have

$$\det(J\boldsymbol{e}(x)) = \Delta(x) = \prod_{i<j}(x_i - x_j).$$

We will give the proof shortly. Now, in coordinates, $\varphi_K : \tilde{\mathcal{O}}^n \cong \tilde{\mathcal{O}}_K \to \mathcal{P}^K \hookrightarrow \mathcal{O}^n$, and we compute using the chain rule,

$$\begin{aligned}
\det(J\varphi_K(a)) &= \det(J\boldsymbol{e}((\sigma_i\beta^j)a)\cdot(\sigma_i\beta^j)) = \Delta((\sigma_i\beta^j)a)\,\Delta(\boldsymbol{\sigma}(\beta)) \\
&= \prod_{i<j}(\sigma_i\beta - \sigma_j\beta)\prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha), \quad \text{for } \alpha \in \tilde{\mathcal{O}}_K \qquad (4.2)\\
&= \sqrt{D}_K \prod_{i<j}\left(\sum_{k=0}^{n-1} a_k\sigma_i\beta^k - \sum_{k=0}^{n-1} a_k\sigma_j\beta^k\right) \\
&= D_K \prod_{i<j}\left(\sum_{k=1}^{n-1} a_k\left(\sum_{l=0}^{k-1}\sigma_i\beta^l\sigma_j\beta^{k-l-1}\right)\right),
\end{aligned}$$

for $a \in \tilde{\mathcal{O}}^n$. Aside from the factor of the discriminant D_K, this is the index form of the extension K.

Definition 48. Let K be an algebraic extension of a local field F. We define the *index form* I_K of K by

$$\det(J\varphi_K(a)) = D_K I_K(a), \quad \text{for all } a \in \tilde{\mathcal{O}}^n.$$

The index form is a homogeneous polynomial of degree $n(n-1)/2$ in $n-1$ variables with coefficients in $\mathcal{O}$, and is given explicitly by the formula,

$$I_K(a) = \prod_{i<j}\left(\sum_{k=1}^{n-1} a_k\left(\sum_{l=0}^{k-1}\beta_i^l\,\beta_j^{k-l-1}\right)\right), \qquad (4.3)$$

where $\beta_i = \sigma_i\beta$.

In general we see that the index form is cumbersome to work with, and as shown by our examples in Chapter 3, is increasingly difficult to integrate directly. Thus we retreat a bit, and assume that K over F is a Galois extension,

$$\begin{aligned}
|\det(J\varphi_K(a))|_F &= \left|\sqrt{D}_K\Delta((\sigma_i\beta^j)a)\right|_F = q^{-d(K)/2}\prod_{i<j}|\sigma_i\alpha - \sigma_j\alpha|_F \\
&= q^{-d(K)/2}\prod_{i<j}\left|\sigma_j^{-1}\sigma_i\alpha - \alpha\right|_F = q^{-d(K)/2}\prod_{i=2}^{n}|\sigma_i\alpha - \alpha|_F^{n/2} \\
&= q^{-d(K)/2}\prod_{\sigma\in H^*}|\sigma\alpha - \alpha|_K^{1/2},
\end{aligned}$$

where $H^* = \mathrm{Hom}_F(K, F^{\mathrm{sep}})\backslash\{1\}$, and using Remark 24. Now recalling that $\mathcal{O}^n \cong \mathcal{O}_K$ under the map $a \mapsto \alpha = \sum_{i=0}^{n-1} a_i \beta^i$, we have,

$$\begin{aligned} m_F(K) &= \frac{1}{w(K)} \int_{\mathcal{O}_n} |\det(J\varphi_K(a))|_F \; da \\ &= \frac{1}{w(K)} \frac{1}{q^{d(K)/2}} \int_{\mathcal{O}_K} \prod_{\sigma \in H^*} |\sigma\alpha - \alpha|_K^{1/2} \; d\alpha, \end{aligned} \tag{4.4}$$

where $da = da_1\, da_2 \cdots da_n$ and $d\alpha$ are the normalized Haar measures on $\mathcal{O}^n$ and $\mathcal{O}_K$, respectively. Now we finally prove Lemma 47.

Proof of Lemma 47. First note that the claim holds trivially when the entries in $x \in \mathcal{O}_K^n$ are not distinct. We will first illustrate the proof with the case $n = 3$. In that case,

$$\boldsymbol{\sigma}(a, b, c) = (a + b + c, ab + ac + bc, abc), \quad \text{for all } (a, b, c) \in \mathcal{O}_K^3.$$

Now given $(x, y, z) \in \mathcal{O}_K^3$ with distinct entries, define the affine transformation $T_{(x,y,z)} : \mathcal{O}_K^3 \to \mathcal{O}_K^3$ by

$$T_{(x,y,z)}(a, b, c) = (x^3 - ax^2 + bx - c, y^3 - ay^2 + by - c, z^3 - az^2 + bz - c),$$

for all $(a, b, c) \in \mathcal{O}_K^3$. Now note that

$$\begin{aligned} &(T_{(x,y,z)} \circ \boldsymbol{\sigma})(a, b, c) \\ &\quad = (x^3 - (a + b + c)x^2 + (ab + ac + bc)x - abc, \\ &\qquad y^3 - (a + b + c)y^2 + (ab + ac + bc)y - abc, \\ &\qquad z^3 - (a + b + c)z^2 + (ab + ac + bc)z - abc) \\ &\quad = ((x - a)(x - b)(x - c), (y - a)(y - b)(y - c), (z - a)(z - b)(z - c)), \end{aligned}$$

and so,

$$J(T_{(x,y,z)} \circ \boldsymbol{\sigma})(a, b, c) = -\begin{pmatrix} (x-b)(x-c) & (x-a)(x-c) & (x-a)(x-b) \\ (y-b)(y-c) & (y-a)(y-c) & (y-a)(y-b) \\ (z-b)(z-c) & (z-a)(z-c) & (z-a)(z-b) \end{pmatrix},$$

$$J(T_{(x,y,z)} \circ \boldsymbol{\sigma})(x, y, z) = -\begin{pmatrix} (x-y)(x-z) & 0 & 0 \\ 0 & (y-x)(y-z) & 0 \\ 0 & 0 & (z-x)(z-y) \end{pmatrix},$$

and finally,

$$\det(J(T_{(x,y,z)} \circ \boldsymbol{\sigma})(x, y, z)) = (x - y)^2(x - z)^2(y - z)^2.$$

But now,

$$\det(J(T_{(x,y,z)} \circ \boldsymbol{\sigma})(a, b, c)) = \det(JT_{(x,y,z)}(\boldsymbol{\sigma}(a, b, c))) \det(J\boldsymbol{\sigma}(a, b, c)),$$

and we have,

$$\begin{aligned}\det(JT_{(x,y,z)}) &= \det\begin{pmatrix} -x^2 & x & -1 \\ -y^2 & y & -1 \\ -z^2 & z & -1 \end{pmatrix} \\ &= (x-y)(x-z)(y-z),\end{aligned}$$

and so

$$(x-y)^2(x-z)^2(y-z)^2 = (x-y)(x-z)(y-z)J\boldsymbol{\sigma}(x,y,z).$$

Solving, we have,

$$J\boldsymbol{\sigma}(x,y,z) = (x-y)(x-z)(y-z).$$

In general, for each $x = (x_1, \ldots, x_n) \in \mathcal{O}_K^n$ with distinct entries, define the affine transformation $T_x : \mathcal{O}_K^n \to \mathcal{O}_K^n$ given by

$$T_x(a) = (x_1^n - a_1 x_1^{n-1} + \cdots + (-1)^n a_n, \ldots, x_n^n - a_1 x_n^{n-1} + \cdots + (-1)^n a_n),$$

for all $a = (a_1, \ldots, a_n) \in \mathcal{O}_K^n$. Now note that

$$(T_x \circ \boldsymbol{\sigma})(a) = \left(\prod_{k=1}^{n} (x_1 - a_k), \ldots, \prod_{k=1}^{n} (x_n - a_k) \right),$$

and that

$$(J(T_x \circ \boldsymbol{\sigma})(a))_{ij} = -\prod_{\substack{k=1 \\ k \neq j}}^{n} (x_i - a_k),$$

$$J(T_x \circ \boldsymbol{\sigma})(x) = -\begin{pmatrix} \prod_{k=2}^{n}(x_1 - x_k) & & 0 \\ & \ddots & \\ 0 & & \prod_{k=1}^{n-1}(x_n - x_k) \end{pmatrix}.$$

So finally,

$$\det(J(T_x \circ \boldsymbol{\sigma})(x)) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{(n^2+n)/2} \Delta(x)^2,$$

since there are n sign changes from the -1 multiplying the entire matrix and $(n^2 - n)/2$ more from negating each term $(x_i - x_j)$ once, $1 \leq i < j \leq n$. But now,

$$J(T_x \circ \boldsymbol{\sigma})(a) = JT_x(\boldsymbol{\sigma}(a)) J\boldsymbol{\sigma}(a),$$

so we have,

$$JT_x = \begin{pmatrix} (-1)^1 x_1^{n-1} & (-1)^2 x_1^{n-2} & \cdots & (-1)^n \\ (-1)^1 x_2^{n-1} & (-1)^2 x_2^{n-2} & \cdots & (-1)^n \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^1 x_n^{n-1} & (-1)^2 x_n^{n-2} & \cdots & (-1)^n \end{pmatrix},$$

and thus

$$\det(JT_x) = (-1)^{(n^2+n)/2}\Delta(x),$$

since there are $1 + 2 + \cdots + n = (n^2 + n)/2$ total sign changes. Finally, we have,

$$J\boldsymbol{\sigma}(x) = \prod_{1\leq i<j\leq n}(x_i - x_j) = \Delta(x).$$

□

4.2 Serre's "mass formula"

In a 1978 paper [18], Jean-Pierre Serre introduced his "mass formula" for totally ramified extensions of local fields. By restricting attention to Eisenstein polynomials (which generate only totally ramified extensions by Proposition 28) the necessary volume integral computations become easy. The current work generalizes Serre's techniques and is motivated in part by a hope to generalize his formula to all étale algebras over a local field. Thus for completeness, I will include a derivation of Serre's "mass formula" here.

As always, fix a local field F with ring of integers $\mathcal{O}$, prime ideal $\mathfrak{p}$, and finite residue field of order q. For a positive integer n, let $\mathcal{A}_n^{\mathrm{tr}}(F) = \mathcal{A}_n^{\mathrm{tr}}$ be the set of isomorphism classes of totally ramified extensions K of F of degree n inside a fixed F^{sep}. For any extension $K \in \mathcal{A}_n^{\mathrm{tr}}$, let

$$c(K) = d(K) - n + 1.$$

The number $c(K)$ is sometimes called the valuation of the *wild part* of the discriminant of K. Note that by Example 35, $c(K) \geq 0$ for all $K \in \mathcal{A}_n^{\mathrm{tr}}$ and $c(K) = 0$ for every tamely ramified extension. Serre's "mass formula" is then:

Theorem 49.

$$\sum_{K\in\mathcal{A}_n^{\mathrm{tr}}} \frac{1}{w(K)q^{c(K)}} = 1. \tag{4.5}$$

Note that each isomorphism class $K \in \mathcal{A}_n^{\mathrm{tr}}$ consists of $n/w(K)$ extensions. If we let Σ_n^{tr} be the set of all totally ramified extensions of F of degree n, we may restate Theorem 49 as

$$\sum_{K\in\Sigma_n^{\mathrm{tr}}} \frac{1}{q^{c(K)}} = n,$$

which is the canonical form of Serre's formula.

Proof of Theorem 49. Let $\mathcal{E}_n \subset \mathcal{P}_n$ be the set of monic Eisenstein polynomials of degree n (see Definition 27), i.e.

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n,$$

with $a_i \in \mathfrak{p}$, but $a_n \notin \mathfrak{p}^2$. Under the isomorphism $\mathcal{P}_n \cong \mathcal{O}^n$, we have,

$$\mathcal{E}_n \cong \mathfrak{p}^{n-1} \times \mathfrak{p}\backslash\mathfrak{p}^2,$$

and thus by Equation 1.2, we have,

$$\mu(\mathcal{E}_n) = q^{-n+1}(q^{-1} - q^{-2}) = q^{-n}(1 - q^{-1}).$$

Let $\tilde{\mathcal{E}}_n = \mathcal{E}_n \cap \tilde{\mathcal{P}}_n$ consist of those polynomials with nonzero discriminant. As always, $\mu(\tilde{\mathcal{E}}_n) = \mu(\mathcal{E}_n)$. Every $f \in \tilde{\mathcal{E}}_n$ generates a totally ramified extension, so for $K \in \mathcal{A}_n^{\mathrm{tr}}$, let $\mathcal{E}_n^K = \tilde{\mathcal{E}}_n \cap \mathcal{P}^K$. Recall that by Proposition 28 each $f \in \mathcal{E}_n^K$ is the minimal polynomial of a uniformizing parameter π of K. Letting

$$\Pi_K = \mathfrak{p}_K \backslash \mathfrak{p}_K^2 \tag{4.6}$$

denote the set of uniformizing parameters of K, the restriction $\varphi_K : \Pi_K \to \mathcal{E}_n^K$ is a surjective $w(K)$-to-1 mapping. Also recall that each uniformizing parameter $\pi \in \Pi_K$ generates $\mathcal{O}_K$ over $\mathcal{O}$, so fix $\pi_K \in \Pi_K$ such that $\mathcal{O}_K = \mathcal{O}[\pi_K]$. Then by Equation 4.2, we simply have,

$$\det(J\varphi_K(\pi)) = \prod_{i<j}(\sigma_i\pi_K - \sigma_j\pi_K)\prod_{i<j}(\sigma_i\pi - \sigma_j\pi) = D_K, \quad \text{for all } \pi \in \Pi_K \hookrightarrow \mathcal{O}^n.$$

Comparing with Definition 48, we see that the index form of a totally ramified extension K over F is trivial. Thus we can easily evaluate the volume integral (similarly as in Equation 4.1),

$$\mu(\mathcal{E}_n^K) = \frac{1}{w(K)q^{d(K)}}\int_{\Pi_K} \mathbf{1}\, d\alpha = \frac{1}{w(K)q^{d(K)}}(q^{-1} - q^{-2}).$$

Now, we have the disjoint union,

$$\tilde{\mathcal{E}}_n = \bigcup_{K \in \mathcal{A}_n^{\mathrm{tr}}} \mathcal{E}_n^K,$$

and by taking volumes,

$$q^{-n}(1 - q^{-1}) = \sum_{K \in \mathcal{A}_n^{\mathrm{tr}}} \frac{1 - q^{-1}}{w(K)q^{d(K)+1}}.$$

After dividing through by $q^{-n}(1 - q^{-1})$, we arrive at

$$\sum_{K \in \mathcal{A}_n^{\mathrm{tr}}} \frac{1}{w(K)q^{d(K)-n+1}} = 1,$$

which is exactly Serre's formula. □

4.3 Completely Split Polynomials

The derivation of Serre's formula works because of the connection between Eisenstein polynomials and totally ramified extensions. Most importantly, the discriminant of

any Eisenstein polynomial is equal to the discriminant of the extension it generates, which makes the index form of the extension trivial. In this section, we compute the volume of polynomials that split completely over a local field F, i.e. that generate the étale algebra F^n.

Throughout this section let $A = F^n \in \mathcal{A}_n(F)$. The mapping, taking roots to the polynomial with those roots, $\varphi_{F^n} : \tilde{\mathcal{O}}^n \to \mathcal{P}^A$ is simply given by

$$\varphi_{F^n}(a) = \prod_{i=1}^{n}(x - a_i), \quad \text{for all } a = (a_1, \ldots, a_n) \in \tilde{\mathcal{O}}^n,$$

where here, $\tilde{\mathcal{O}}^n = \{(a_1, \ldots, a_n) \in \mathcal{O}^n : \text{the } a_i \text{ are distinct}\}$. The mapping φ_{F^n} is invariant under permutation of the "roots", i.e. the automorphisms of F^n just permute the coordinates of a point, thus $w(F^n) = n!$. Also, in accordance with Definition 43, we also have $D_{F^n} = 1$. In coordinates, $\varphi_{F^n} : \tilde{\mathcal{O}}^n \to \tilde{\mathcal{O}}^n$ is given by the elementary symmetric function mapping $\varphi_{F^n}(a) = \boldsymbol{e}(a)$, and so by Lemma 47,

$$\det(J\varphi_{F^n}(a)) = \prod_{i<j}(a_i - a_j), \quad \text{for all } a \in \tilde{\mathcal{O}}^n.$$

Thus we have,

$$m_F(F^n) = \frac{1}{n!}\int_{\tilde{\mathcal{O}}^n}\prod_{i<j}|a_i - a_j|_F \, da = \frac{1}{n!}\int_{\mathcal{O}^n}\prod_{i<j}|a_i - a_j|_F \, da. \tag{4.7}$$

To compute this integral, let $R = \{\rho_1, \ldots, \rho_q\}$ be a set of representatives for $\overline{F}$ and decompose

$$\mathcal{O}^n = \bigcup_{r \in R^n}(r_1 + \mathfrak{p}) \times \cdots \times (r_n + \mathfrak{p}) = \bigcup_{r \in R^n}(r + \mathfrak{p}^n), \quad \text{for } r = (r_1, \ldots, r_n) \in R^n.$$

Changing variables by the mapping $(a_1, \ldots, a_n) \mapsto (r_1 + \pi a_1, \ldots, r_n + \pi a_n)$, we have

$$\begin{aligned}\int_{\mathcal{O}^n}\prod_{i<j}|a_i - a_j|_F \, da &= \sum_{r \in R^n}\int_{r+\mathfrak{p}^n}\prod_{i<j}|a_i - a_j|_F \, da \\ &= \sum_{r \in R^n}\int_{\mathcal{O}^n}\prod_{i<j}|r_i - r_j + \pi(a_i - a_j)|_F|\pi^n|_F \, da.\end{aligned}$$

Note that for each factor in the above integrand,

$$|r_i - r_j + \pi(a_i - a_j)|_F = \begin{cases} 1 & \text{if } r_i \neq r_j \\ q^{-1}|a_i - a_j| & \text{if } r_i = r_j \end{cases}.$$

To see what is happening here, take for instance the "ordered" vector

$$r = (r_{11}, \ldots, r_{\lambda_1 1}, r_{12}, \ldots, r_{\lambda_2 2}, \ldots, r_{1q} \ldots, r_{\lambda_q q}),$$

where $\lambda_1 + \cdots + \lambda_q = n$, and where each $r_{ij} = \rho_j$. We have

$$\begin{aligned}\int_{r+\mathfrak{p}^n} \prod_{i<j} |a_i - a_j|_F \, da &= q^{-n} \int_{\mathcal{O}^n} \prod_{k=1}^{q} \prod_{1\le i<j\le \lambda_k} q^{-1} |a_{ik} - a_{jk}|_F \, da \\ &= q^{-n} \prod_{k=1}^{q} q^{-\binom{\lambda_k}{2}} \int_{\mathcal{O}^{\lambda_k}} \prod_{1\le i<j\le \lambda_k} |a_{ik} - a_{jk}|_F \, da \\ &= \prod_{k=1}^{q} q^{-\binom{\lambda_k+1}{2}} \, \lambda_k! \, m_F(F^{\lambda_k}),\end{aligned}$$

where we conveniently set $m_F(F^0) = 1$. Note once more that for any permutation $\tau \in S_n$,

$$\int_{r+\mathfrak{p}^n} \prod_{i<j} |a_i - a_j|_F \, da = \int_{\tau(r)+\mathfrak{p}^n} \prod_{i<j} |a_i - a_j|_F \, da.$$

Thus for any $\lambda = (\lambda_1, \ldots, \lambda_q) \in \mathbb{N}^q$ satisfying $\lambda_1 + \cdots + \lambda_q = n$, form the corresponding "ordered vector" r_λ as above, then we have the decomposition,

$$R^n = \bigcup_{\lambda} \bigcup_{r \sim r_\lambda} \{r\}$$

where the union is taken over all such λ, and where $r \sim r_\lambda$ if there exists some permutation $\tau \in S_n$ such that $\tau(r) = r_\lambda$. For a given λ, the number of vectors equivalent to r_λ is given by the multinomial,

$$\frac{n!}{\lambda!} = \binom{n}{\lambda_1, \ldots, \lambda_q} = \frac{n!}{\lambda_1! \cdots \lambda_q!},$$

and so we arrive at the recursion,

$$n! \, m_F(F^n) = \sum_{\lambda} \frac{n!}{\lambda!} \prod_{k=1}^{q} q^{-\binom{\lambda_k+1}{2}} \lambda_k! \, m_F(F^{\lambda_k}).$$

Theorem 50. Let F be a local field with residue field of order q, then we have the recursion,

$$m_F(F^n) = \sum_{\lambda} \prod_{k=1}^{q} q^{-\binom{\lambda_k+1}{2}} m_F(F^{\lambda_k}),$$

where the sum is over all $\lambda = (\lambda_1, \ldots, \lambda_q) \in \mathbb{N}^q$ such that $\lambda_1 + \cdots + \lambda_q = n$. We define $m_F(F^0) = 1$, and note that $m_F(F^1) = 1$ holds trivially.

We list $m_F(F^n)$ as rational functions in q for a few values of n in Table 4.1, and note that we may partially factor them into the *cyclotomic polynomials* Φ_n and again into the polynomials $\phi_n = q^n - 1$. There is oftentimes an irreducible polynomial in the numerator with neither of these shapes which we call f_n, and which is of high degree, thus we don't show very many. The structure of these factorizations is still somewhat mysterious.

n	Φ	ϕ
1	1	1
2	$\frac{1}{2!}\frac{q}{\Phi_2}$	$\frac{1}{2!}\frac{\phi_1 q}{\phi_2}$
3	$\frac{1}{3!}\frac{\Phi_6 q^3}{\Phi_2\Phi_5}$	$\frac{1}{3!}\frac{\phi_1^3\phi_6 q^3}{\phi_2^2\phi_3\phi_5}$
4	$\frac{1}{4!}\frac{f_4\ q^6}{\Phi_2^2\Phi_3\Phi_5\Phi_9}$	$\frac{1}{4!}\frac{\phi_1^4 f_4\ q^6}{\phi_2^2\phi_5\phi_9}$
5	$\frac{1}{5!}\frac{f_5\ q^{10}}{\Phi_2^2\Phi_3\Phi_5\Phi_7\Phi_9\Phi_{14}}$	$\frac{1}{5!}\frac{\phi_1^4\ f_5\ q^{10}}{\phi_2\phi_5\phi_9\phi_{14}}$
6	$\frac{1}{6!}\frac{f_6\ q^{15}}{\Phi_2^3\Phi_3\Phi_4\Phi_5^3\Phi_7\Phi_9\Phi_{10}\Phi_{14}\Phi_{20}}$	$\frac{1}{6!}\frac{\phi_1^6\ f_6\ q^{15}}{\phi_2\phi_5^2\phi_9\phi_{14}\phi_{20}}$
7	$\frac{1}{7!}\frac{f_7\ q^{21}}{\Phi_2^3\Phi_3^2\Phi_4\Phi_5^3\Phi_7\Phi_9^2\Phi_{10}\Phi_{14}\Phi_{20}\Phi_{27}}$	$\frac{1}{7!}\frac{\phi_1^7\ f_7\ q^{21}}{\phi_2\phi_5^2\phi_9\phi_{14}\phi_{20}\phi_{27}}$
8	$\frac{1}{8!}\frac{f_8\ q^{28}}{\Phi_2^4\Phi_3^2\Phi_4\Phi_5^4\Phi_7^2\Phi_9^2\Phi_{10}\Phi_{14}\Phi_{20}\Phi_{27}\Phi_{35}}$	$\frac{1}{8!}\frac{\phi_1^9\ f_8\ q^{28}}{\phi_2^2\phi_5^2\phi_9\phi_{14}\phi_{20}\phi_{27}\phi_{35}}$
9	$\frac{1}{9!}\frac{f_9\ q^{36}}{\Phi_2^4\Phi_3^2\Phi_4^2\Phi_5^4\Phi_7^2\Phi_9^2\Phi_{10}\Phi_{11}\Phi_{14}\Phi_{20}\Phi_{22}\Phi_{27}\Phi_{35}\Phi_{44}}$	$\frac{1}{9!}\frac{\phi_1^9\ f_9\ q^{36}}{\phi_2\phi_5^2\phi_9\phi_{14}\phi_{20}\phi_{27}\phi_{35}\phi_{44}}$
10	$\frac{1}{10!}\frac{f_{10}\ q^{45}}{\Phi_2^5\Phi_3^3\Phi_4^2\Phi_5^4\Phi_6\Phi_7^2\Phi_9^3\Phi_{10}\Phi_{11}\Phi_{14}^2\Phi_{18}\Phi_{20}\Phi_{22}\Phi_{27}^2\Phi_{35}\Phi_{44}\Phi_{54}}$	$\frac{1}{10!}\frac{\phi_1^9\phi_7\ f_{10}\ q^{45}}{\phi_5^2\phi_9\phi_{14}^2\phi_{20}\phi_{27}\phi_{35}\phi_{44}\phi_{54}}$
	f_n	
4	$q^8-2q^7+q^6+2q^5-q^4+2q^3+q^2-2q+1$	
5	$q^{16}-6q^{15}+14q^{14}-14q^{13}+9q^{12}-4q^{11}-4q^{10}-6q^9$ $+5q^8-6q^7-4q^6-4q^5+9q^4-14q^3+14q^2-6q+1$	

Table 4.1: Volumes for completely split polynomials as rational functions in q and factored into cyclotomic polynomials Φ_n and into $\phi_n = q^n - 1$.

Asymptotics of $m_F(F^n)$

One wonders if there exists a closed formula for the numbers $m_F(F^n)$, though at this time this seems doubtful. Instead, we will describe some asymptotic results. We show that the asymptotic limit as $q \to \infty$ might have been guessed from staring at Table 4.1.

Theorem 51. For any $n \in \mathbb{N}$ we have,

$$m_F(F^n) \to \frac{1}{n!}, \quad \text{as} \quad q \to \infty.$$

Proof. For the duration of this proof, let $s_n(q) = m_F(F^n)$, and let

$$G(x) = \sum_{n=0}^{\infty} s_n(q) x^n, \qquad g(x) = \sum_{n=0}^{\infty} q^{-\binom{n+1}{2}} s_n(q) x^n$$

be generating functions. Then the recursion in Theorem 50 says (see [19], Chp. 2.2 for example),

$$G(x) = g(x)^q.$$

Since $|s_n(q)| \leq 1$ for all $n \in \mathbb{N}$, the coefficients of $g(x)$ are very rapidly decreasing, thus $g(x)$ and hence $G(x)$ represent analytic functions on $\mathbb{C}$. Now writing out the first few terms,

$$g(x) = 1 + \frac{1}{q}x + \frac{1}{2}\frac{1}{q^3}\frac{q}{q+1}x^2 + \cdots,$$

and thus

$$G(x) = \left(1 + \frac{x}{q} + O(q^{-2})\right)^q \to e^x, \quad \text{as } q \to \infty,$$

by a well-known calculus limit, which proves the theorem. □

For the case $q = 2$, the recursion in Theorem 50 gives

$$m_F(F^n) = \sum_{i+j=n} 2^{-\binom{i+1}{2}-\binom{j+1}{2}} m_F(F^i) m_F(F^j),$$

where the sum is taken over all nonnegative integers i and j, with $i + j = n$. As a side note, letting $c_n = 2^{-\binom{n+1}{2}} m_F(F^n)$, this can be rewritten as

$$2^{\binom{n+1}{2}} c_n = \sum_{k=0}^{n} c_k c_{n-k}.$$

It is still an open problem to find a closed form for this seemingly simple recursion. We now describe some of the asymptotic behavior as $n \to \infty$.

Theorem 52. For all $n \in \mathbb{N}$, we have the lower bound,

$$-\frac{1}{2}\frac{1}{q-1}n^2 - \frac{1}{2}n\log_q n + \frac{1}{2}\frac{1}{q-1}n \leq \log_q m_F(F^n)$$

Furthermore, for $q = 2$ we have the upper bound,

$$\log_2 m_F(F^n) \leq -\frac{1}{2}n^2 - \frac{1}{2}n\log_2 n + 1.1n - 0.6. \tag{4.8}$$

Proof. By induction on n. For the duration of the proof, fix q, let $s_n = m_F(F^n)$, and for some $A \in \mathbb{R}$ to be decided later, let

$$S(n) = -\frac{1}{2}\frac{1}{q-1}n^2 - \frac{1}{2}n\log_q n + An.$$

Now suppose that for all $k < n$, $\log_q s_n \geq S(n)$. We will approximate s_n by the "middle" (and dominant) terms. To this end, let $n = aq + b$ where $0 \leq b < q$, and in the sum describing s_n in Theorem 50, we keep only the q terms involving λ with $q-1$ entries equal to a and one entry equal to $a+b$. Throwing away the rest, we have

$$s_n \geq q\, q^{-(q-1)\binom{a+1}{2}-\binom{a+b+1}{2}} s_a^{q-1} s_{a+b},$$

and using the fact that $q \leq n/q$, and the induction hypothesis,

$$\begin{aligned}
\log_q s_n &\geq -\frac{q}{2}a(a+1) + q\log_q s_a + E(n) \\
&\geq -\frac{1}{2}\frac{n^2}{q} - \frac{n}{2} - \frac{1}{2}\frac{n^2}{q(q-1)} - \frac{1}{2}n\log_q(n/q) + A\frac{n}{q} + E(n) \\
&= S(n) + E(n),
\end{aligned}$$

where the error term is

$$\begin{aligned}
E(n) &= \log_q s_{a+b} - \log_q s_a + \binom{a+1}{2} - \binom{a+b+1}{2} \\
&= a^2 + a + \frac{b}{2} + Ab + \frac{1}{2}a\log_q a - \frac{1}{2}(a+b)\log_q(a+b) \geq 0
\end{aligned}$$

by elementary estimates. Now $\log_q s_1 = 0$ so setting $A = \frac{1}{2}\frac{1}{q-1}$ gives equality for the base case estimate. Thus by induction, we have proved the first part of the theorem.

For the second part of the theorem, we fix $q = 2$, and again we proceed by induction on n. Suppose that the upper bound holds in Equation 4.8 for all natural numbers $0 \leq j < n$, i.e. that

$$\log_2 s_j \leq -\frac{1}{2}j^2 - \frac{1}{2}j\log_2 j + Aj + B,$$

for some constants $A, B \in \mathbb{R}$ to be determined later. Then for all $0 \leq j < n$ we have,

$$\log_2(2^{-j^2+nj} s_j s_{n-j}) \leq -2(j - \frac{n}{2})^2 + An + 2B - \frac{1}{2}[j\log_2 j + (n-j)\log_2(n-j)].$$

First solving for s_n, we have

$$s_n = \frac{1}{1 - 2^{-\binom{n+1}{2}+1}} \sum_{j=1}^{n-1} 2^{-\binom{j+1}{2}-\binom{n-j+1}{2}} s_j s_{n-j}.$$

Now for $n > 1$ we calculate,

$$\begin{aligned} s_n &= \frac{1}{1-2^{-\binom{n+1}{2}+1}} \sum_{j=1}^{n-1} 2^{-\binom{j+1}{2}-\binom{n-j+1}{2}} s_j s_{n-j} \\ &= \frac{1}{1-2^{-\binom{n+1}{2}+1}} 2^{-\frac{1}{2}n^2-\frac{1}{2}n} \sum_{j=1}^{n-1} 2^{-j^2+nj} s_j s_{n-j} \\ &\leq 2^{-\frac{1}{2}n^2-\frac{1}{2}n\log_2 n+An+B} E(n), \end{aligned}$$

where the error term is

$$E(n) = \frac{1}{1-2^{-\binom{n+1}{2}+1}} 2^{-\frac{1}{2}n+\frac{1}{2}n\log_2 n+B} \sum_{j=1}^{n-1} 2^{-2(j-\frac{n}{2})^2} 2^{-\frac{1}{2}(j\log_2 j+(n-j)\log_2(n-j))}.$$

First we note that the minimum of $L(j) = j\log_2 j + (n-j)\log_2(n-j)$ occurs at $j = n/2$. To see this, first differentiate

$$L'(j) = \log_2 j - \log_2(n-j).$$

Thus we see that on the interval $[1, n-1]$, $L(j)$ reaches a minimum at $j = n/2$. Using this we have,

$$E(n) \leq \frac{1}{1-2^{-\binom{n+1}{2}+1}} 2^{-\frac{1}{2}n+\frac{1}{2}n\log_2 n+B}\ 2^{-\frac{n}{2}\log_2\left(\frac{n}{2}\right)} \sum_{j=1}^{n-1} 2^{-2(j-\frac{n}{2})^2}.$$

We also estimate for, $n > 3$,

$$\begin{aligned} \sum_{j=1}^{n-1} 2^{-2(j-\frac{n}{2})^2} &\leq 1 + 2\sum_{j=1}^{n/2} 2^{-2j^2} = 1 + 2\left(2^{-2}+2^{-8}\right) + \sum_{j=3}^{n/2} 2^{-2j^2} \\ &\leq 1.51 + 2\sum_{j=3}^{n/3} 2^{-2j} = 1.51 + 2^{-5} \sum_{j=0}^{n/2-3} 2^{-2j} \\ &= 1.51 + 2^{-5}\frac{4}{3}(1-2^{-n+4}) \leq 1.51 + \frac{1}{24} \leq 1.6, \end{aligned}$$

and thus finally,

$$E(n) \leq \frac{1.6}{1-2^{-\binom{n+1}{2}+1}} 2^B \leq 1 \quad \Leftrightarrow \quad B \leq -\log_2 1.6 + \log_2\left(1-2^{-\binom{n+1}{2}+1}\right).$$

To satisfy the base case $n = 1$ and to avoid contradicting the lower bound we need $\frac{1}{2}n \leq An + B$ for all $1 \leq n$, and thus A and B must satisfy

$$\left(\frac{1}{2} - A\right) n \leq B \leq -\log_2 1.6 + \log_2\left(1-2^{-\binom{n+1}{2}+1}\right), \quad \text{for all } n \geq 1.$$

The minimal uniform solution is $A = 1.1$ and $B = -.6$, though one should note that asymptotically as $n \to \infty$, $A \to \frac{1}{2}$ should be the case. □

We conjecture that the first two terms of the upper and lower bounds in the above theorem actually represents the dominant terms of the asymptotic limit for general q, as $n \to \infty$ but cannot currently show it.

Note that one can give another form for the recursion in Theorem 50. Using the generating functions from Theorem 51, we have

$$\begin{aligned} G(x) = g(x)^q &\Rightarrow \frac{G'(x)}{G(x)} = q\frac{g'(x)}{g(x)} \Rightarrow g(x)G'(x) = qg'(x)G(x) \\ &\Rightarrow \sum_{i+j=n} q^{-\binom{i+1}{2}} s_i(j+i)s_j = \sum_{i+j=n} q(i+1)q^{-\binom{i+2}{2}} s_i s_j \\ &\Rightarrow \sum_{i+j=n} jq^{-\binom{i+1}{2}} s_i s_j = \sum_{i+j=n} iq\, q^{-\binom{i+1}{2}} s_i s_j \\ &\Rightarrow (1 - q^{-\binom{n+1}{2}+1})s_n = \sum_{i=1}^{n-1} \left(\frac{q+1}{n} i - 1\right) q^{-\binom{i+1}{2}} s_i s_{n-i}, \end{aligned}$$

which may be useful for proving these asymptotic limits.

4.4 Unramified Extensions

Throughout this section let $K = A \in \mathcal{A}_n(F)$ denote an unramified algebraic extension of F, which is always a Galois extension of F with cyclic group of automorphisms. For the computation of $m_F(A)$ it is more convenient to alter our setup. Namely, fix a local field K with residue field $\mathbb{F}_q$, and let K_n be a subfield of K such that K is an unramified extension of K_n of degree n. We will then calculate $m_{K_n}(K)$.

In this case, $d(K) = 0$, and let $G_n = \mathrm{Aut}_F(K) = C_n$ be the cyclic Galois group of order n. By Equation 4.4,

$$m_{K_n}(K) = \frac{1}{n} \int_{\mathcal{O}_K} \prod_{s \in G_n^*} |s\alpha - \alpha|_K^{1/2}\, d\alpha = \frac{1}{n} U_n.$$

Now to compute this integral, choose the unique set of *multiplicative* or *Teichmüller* representatives R for K (see [5], Chp. I.7), i.e. such that $R\backslash\{0\}$ is the cyclic group of $q-1$ roots of unity. Letting π be a G_n stable uniformizing parameter of K, we have,

$$\begin{aligned} U_n &= \int_{\mathcal{O}_K} \prod_{s \in G_n^*} |s\alpha - \alpha|_K^{1/2}\, d\alpha = \sum_{r \in R} \int_{r + \mathfrak{p}_K} \prod_{s \in G_n^*} |s\alpha - \alpha|_K^{1/2}\, d\alpha \\ &= \sum_{r \in R} q^{-1} \int_{\mathcal{O}_K} \prod_{s \in G_n^*} |sr - r + \pi(s\alpha - \alpha)|_K^{1/2}\, d\alpha. \end{aligned}$$

Now if $sr - r \equiv 0 \bmod \mathfrak{p}_K$, i.e. if $\overline{sr} = \overline{r}$, then by the uniqueness of multiplicative

representatives, in fact, $sr = r$. Thus for each factor in the above product we have,

$$|sr - r + \pi(s\alpha - \alpha)|_K = \begin{cases} q^{-1}|s\alpha - \alpha|_K & \text{if } sr = r \\ \\ 1 & \text{if } sr \neq r \end{cases}.$$

Now for a given $r \in R$, $sr = r$ if and only if $\overline{r}$ is contained in a subfield of $\mathbb{F}_q$ which the subgroup $\langle \overline{s} \rangle$ fixes. More precisely, r is fixed by the subgroup $G_d \subset G_n$ of order $d|n$ and by no smaller subgroup if and only if $\overline{r}$ is a primitive element of the subfield K_d over K_n.

$$\begin{array}{ccc} K & & \mathbb{F}_q \\ \big| G_d & & \big| \overline{G}_d \\ K_d & & \mathbb{F}_{q^{1/d}} \\ \big| & & \big| \\ K_n & & \mathbb{F}_{q^{1/n}} \end{array}$$

Thus we calculate

$$\begin{aligned} U_n &= \sum_{r \in R} q^{-1} \int_{\mathcal{O}_K} \prod_{s \in G_n^*} |sr - r + \pi(s\alpha - \alpha)|_K^{1/2} \, d\alpha \\ &= \sum_{d|n} a(d,n) q^{-1} \int_{\mathcal{O}_K} \prod_{s \in G_d^*} q^{-1/2} |s\alpha - \alpha|_K^{1/2} \, d\alpha \\ &= \sum_{d|n} a(d,n) q^{-(d+1)/2} U_d, \end{aligned} \tag{4.9}$$

where $a(d,n)$ is the number of primitive elements of $\mathbb{F}_{q^{1/d}}$ over $\mathbb{F}_{q^{1/n}}$. We also note that $U_1 = 1$. We will give a closed formula for the combinatorial numbers $a(d,n)$.

Lemma 53. The number of primitive elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by

$$\sum_{d|n} \mu(n/d) q^d,$$

where μ is the Möbius function.

Proof. We decompose $\mathbb{F}_{q^n}$ as

$$\mathbb{F}_{q^n} = \bigcup_{d|n} \tilde{\mathbb{F}}_{q^d},$$

where $\tilde{\mathbb{F}}_{q^d}$ is the set of primitive elements of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$. Letting $a_d = \#\tilde{\mathbb{F}}_{q^d}$, we have

$$q^n = \sum_{d|n} a_d \quad \Leftrightarrow \quad a_n = \sum_{d|n} \mu(n/d) q^d,$$

by Möbius inversion (see [11], Chp. 3.2). □

Now we can write $a(d,n)$ as the number of primitive elements of $\mathbb{F}_{q^{(n/d)/n}}$ over $\mathbb{F}_{q^{1/n}}$, and thus by the Lemma 53,

$$a(d,n) = \sum_{e|\frac{n}{d}} \mu(n/de) q^{e/n}. \tag{4.10}$$

Letting $b(d,n) = \frac{d}{n} a(d,n)$, note that $b(d,n)$ is the number of irreducible polynomials of degree n/d over $\mathbb{F}_{q^{1/n}}$, again, see [11], Chp. 3.2.

Theorem 54. Let K be the unramified extension of degree n of a local field K_n, then

$$m_{K_n}(K) = \frac{1}{n} U_n = \sum_{d|n} b(d,n) q^{-(d+1)/2} m_{K_d}(K), \tag{4.11}$$

where $b(d,n)$ is the number of irreducible polynomials of degree n/d over $\mathbb{F}_{q^{1/n}}$.

To revert back to our old notation, we fix a field F with residue field of order q, and let K be the unramified extension of F of degree n. By Figure 1.1, K has residue field of order q^n, and thus to recover $m_F(K)$ we just need to make the substitution $q \mapsto q^n$ in the *final formula* for $m_{K_n}(K)$ (this last point is important), i.e. $m_F(K) = \frac{1}{n} U_n(q^n)$. Solving the recursion for $n = 2$ and making the substitution $q \mapsto q^2$ recovers our original formula in Equation 2.2,

$$m_F(K) = \frac{1}{2} \frac{q}{q+1},$$

for an unramified extension K of F of degree 2. More generally, for any prime n we can also easily solve the recursion in Equation 4.9 (now with the fixed K notation),

$$\begin{aligned} U_n &= a(1,n) q^{-1} U_1 + a(n,n) q^{-(n+1)/2} U_n \\ &= \frac{q - q^{1/n}}{q} \frac{1}{1 - q^{1/n} q^{-(n+1)/2}}. \end{aligned}$$

Substituting $q \mapsto q^n$, we have

$$U_n(q^n) = \frac{q^n - q}{q^n} \frac{1}{1 - q\, q^{-\binom{n+1}{2}}},$$

and thus, for an unramified K over F of degree n,

$$m_F(K) = \frac{1}{n} \frac{(q^{n-1} - 1) q^{\binom{n}{2}}}{q^{\binom{n+1}{2}-1} - 1} = \frac{1}{n} \frac{\phi_{n-1}\, q^{\binom{n}{2}}}{\phi_{\binom{n+1}{2}-1}}, \tag{4.12}$$

whenever n is prime.

Again with our fixed K regime, we solve the recursion in Equation 4.9 when $n = p^2$ for a prime p. In this case we have,

$$\begin{aligned} U_n &= a(1,n) q^{-1} U_1 + a(p,n) q^{-\frac{p+1}{2}} U_p + a(n,n) q^{-\frac{n+1}{2}} \\ &= \left(q - q^{1/p}\right) q^{-1} + \left(q^{1/p} - q^{1/n}\right) q^{-\frac{p+1}{2}} \frac{\left(q - q^{1/p}\right) q^{-1}}{1 - q^{1/p}\, q^{-\frac{p+1}{2}}} + q^{1/n}\, q^{\frac{n+1}{2}} U_n, \end{aligned}$$

using our previous formula for $n = p$. Now we can let $q \mapsto q^n$, and we have

$$\begin{aligned} U_n(q^n) &= \frac{1}{1 - q\, q^{-\binom{n+1}{2}}} \left((q^n - q^p)\, q^{-n} + (q^p - q)\, q^{-n\frac{p+1}{2}} \frac{(q^n - q^p)\, q^{-n}}{1 - q^p\, q^{-n\frac{p+1}{2}}} \right) \\ &= \frac{\phi_{n-p}\, q^{\binom{n}{2}+p-1}}{\phi_{\binom{n+1}{2}-1}} \frac{\phi_{p\binom{p+1}{2}-p} + q^{1-p}\, \phi_{p-1}}{\phi_{p\binom{p+1}{2}-p}} = \frac{\phi_{n-p}\, q^{\binom{n}{2}}}{\phi_{\binom{n+1}{2}-1}} \frac{q^{p-1}\, \phi_{p\binom{p+1}{2}-p} + \phi_{p-1}}{\phi_{p\binom{p+1}{2}-p}}. \end{aligned}$$

Noting that $q^s\, \phi_r + \phi_s = \phi_{r+s}$ for any $r, s \in \mathbb{N}$, we finally have

$$m_F(K) = \frac{1}{p^2} \frac{\phi_{p^2-p}\, \phi_{p\binom{p+1}{2}-1}\, q^{\binom{p^2}{2}}}{\phi_{p\binom{p+1}{2}-p}\, \phi_{\binom{p^2+1}{2}-1}}, \tag{4.13}$$

in the case that K has degree p^2 over F, and F has residue field of order q.

In Table 4.2, we list a few values of $m_{K_n}(K)$ as rational functions in q where we make the substitution $q \mapsto q^n$. Again we notice that these have factorizations into the cyclotomic polynomials Φ_n and into the polynomials $\phi_n = q^n - 1$, where again, the strange irreducible polynomial in the numerator will be called f_n. These factorizations are also mysterious.

Asymptotics of $m_{K_n}(K)$

Again, one wonders if there exists a closed formula for the numbers $m_{K_n}(K)$. We will end by providing some asymptotic results in this case.

Theorem 55. We have

$$m_{K_n}(K) \to \frac{1}{n}, \quad \text{as} \quad q \to \infty,$$

and

$$m_{K_n}(K) \sim \frac{1}{n}, \quad \text{as} \quad n \to \infty.$$

Proof. We show these both by showing that $U_n \to 1$ as $q \to \infty$ for arbitrarily large n. First note that $a(1, n) = q + O(q^{1/2})$ and so the $d = 1$ term is dominant in the sum

$$U_n = \sum_{d|n} a(d, n) q^{-(d+1)/2} U_d.$$

Also note that if $\mathrm{char}(\mathbb{F}_q) = p$, then n is bounded above by the condition $q^{1/n} \geq p$. Now by a gracious estimate

$$|a(d, n)| \leq \sum_{j=0}^{n/d} q^{j/n} = \frac{q^{(n/d+1)/n} - 1}{q^{1/n} - 1} \leq \frac{q^{(n/d+1)/n}}{p - 1} \leq c q^{1/n} q^{1/d},$$

for some positive constant c depending only on q, and thus we have

$$\begin{aligned} |U_n - 1| &= |O(q^{-1/2}) + q^{-1/2} \sum_{\substack{d|n \\ d>1}} a(d, n) q^{-d/2} U_d| \\ &\leq O(q^{-1/2}) + q^{-1/2} c q^{1/n} \sum_{\substack{d|n \\ d>1}} q^{1/d} q^{-d/2} U_d \to 0, \end{aligned}$$

as $q \to \infty$ independently of n, for $n > 2$. This proves the theorem. □

n	Φ	ϕ
1	1	1
2	$\frac{1}{2}\frac{q}{\Phi_2}$	$\frac{1}{2}\frac{\phi_1\, q}{\phi_2}$
3	$\frac{1}{3}\frac{\Phi_2\, q^3}{\Phi_5}$	$\frac{1}{3}\frac{\phi_2\, q^3}{\phi_5}$
4	$\frac{1}{4}\frac{\Phi_5\, q^6}{\Phi_3\Phi_4\Phi_9}$	$\frac{1}{4}\frac{\phi_2\phi_5\, q^3}{\phi_4\phi_9}$
5	$\frac{1}{5}\frac{\Phi_4\, q^{10}}{\Phi_7\Phi_{14}}$	$\frac{1}{5}\frac{\phi_4\, q^{10}}{\phi_{14}}$
6	$\frac{1}{6}\frac{f_6\, q^{15}}{\Phi_2\Phi_4\Phi_5^2\Phi_6\Phi_{10}^2\Phi_{20}}$	$\frac{1}{6}\frac{\phi_2^2\phi_3\, f_6\, q^{15}}{\phi_6\phi_{10}\phi_{20}}$
7	$\frac{1}{7}\frac{\Phi_2\Phi_6\, q^{21}}{\Phi_9\Phi_{27}}$	$\frac{1}{7}\frac{\phi_6\, q^{21}}{\phi_{27}}$
8	$\frac{1}{8}\frac{\Phi_{10}\Phi_{19}\, q^{28}}{\Phi_3\Phi_6\Phi_7\Phi_8\Phi_9\Phi_{18}\Phi_{35}}$	$\frac{1}{8}\frac{\phi_4\phi_{10}\phi_{19}\, q^{28}}{\phi_8\phi_{18}\phi_{35}}$
9	$\frac{1}{9}\frac{\Phi_6\Phi_{17}\, q^{36}}{\Phi_4\Phi_5\Phi_{11}\Phi_{15}\Phi_{22}\Phi_{44}}$	$\frac{1}{9}\frac{\phi_6\phi_{17}\, q^{36}}{\phi_{15}\phi_{44}}$
10	$\frac{1}{10}\frac{f_{10}\, q^{45}}{\Phi_2\Phi_3\Phi_7\Phi_9\Phi_{10}\Phi_{14}\Phi_{18}\Phi_{27}\Phi_{28}\Phi_{54}}$	$\frac{1}{10}\frac{\phi_1\phi_4\phi_5\phi_6\, f_{10}\, q^{45}}{\phi_3\phi_{10}\phi_{28}\phi_{54}}$
11	$\frac{1}{11}\frac{\Phi_2\Phi_{10}\, q^{55}}{\Phi_{13}\Phi_{65}}$	$\frac{1}{11}\frac{\phi_{10}\, q^{55}}{\phi_{65}}$
12	$\frac{1}{12}\frac{f_{12}\, q^{66}}{\Phi_4\Phi_5^2\Phi_7\Phi_8\Phi_{10}^2\Phi_{11}\Phi_{12}\Phi_{20}^2\Phi_{27}\Phi_{40}\Phi_{77}}$	$\frac{1}{12}\frac{\phi_0\phi_1\phi_3\phi_4^2\phi_6\, f_{12}\, q^{66}}{\phi_{12}\phi_{20}\phi_{27}\phi_{40}\phi_{77}}$
	f_n	
4	$q^{14}+2q^{12}+2q^{10}+q^9+2q^8+q^7+2q^6+q^5+2q^4+2q^2+1$	

Table 4.2: Volumes for unramified extensions as rational functions in q and factored into cyclotomic polynomials Φ_n and into $\phi_n = q^n - 1$.

Appendix A

Glossary of Terms

$\mathbb{N}$	The set of natural numbers: $0, 1, 2, \ldots$
$\mathbb{Z}$	The set of integers: $\ldots, -2, -1, 0, 1, 2, \ldots$
$\mathbb{Q}$	The set of rational numbers.
$\mathbb{R}$	The set of real numbers.
$\mathbb{C}$	The set of complex numbers.
$\mathbb{F}_q$	The finite field of order q.
$\mathbb{Q}_p$	The set of p-adic numbers.
$\mathbb{Z}_p$	The set of p-adic integers.
$\cong$	Isomorphism of fields or topological groups.
$\hookrightarrow$	Inclusion mapping.
$\oplus$	Direct sum of vector spaces or rings.
$v,\ (v_F)$	A normalized discrete valuation, (on a field F).
F	A local field, (Section 1.1).
F^n	The n-fold Cartesian product $F \times \cdots \times F$.
K	A finite separable extension of F.
F^*	The multiplicative group of a field F.
G^*	A group G without its identity element.
$(F^*)^n$	The multiplicative group of n^{th} powers of elements in F.
$\mathcal{O},\ (\mathcal{O}_F)$	The ring of integers of local field, (of F).
$\mathcal{O}^*,\ (\mathcal{O}_F^*)$	The group of integer units.
$\mathfrak{p},\ (\mathfrak{p}_F)$	The prime ideal of $\mathcal{O}$, (of $\mathcal{O}_F$).
$\overline{F}$	The residue field of a local field F.
$\pi,\ (\pi_F)$	A uniformizing parameter, (of F).
$\lvert\cdot\rvert_F$	The normalized absolute value, (on F), (Section 1.1).

R	A set of residue field representatives of a local field.
$F[x]$	The set of polynomials in x with coefficients in F.
$F(x)$	The set of rational functions in x with coefficients F.
$F((x))$	The set of Laurent series in x with coefficients in F.
$\mu,\ (\mu_F)$	The normalized Haar measure, (on F), (Section 1.2).
$\mu \otimes \lambda$	The product measure of μ and λ, (Section 1.2).
$J\varphi$	The Jacobian matrix of a mapping φ.
$\dim_F(K)$	The degree of the field extension K over F.
$\mathrm{Aut}_F(K)$	The set of F-automorphisms of an extension K.
$\#S$	The cardinality of a set S.
$w(K)$	The cardinality of $\mathrm{Aut}_F(K)$.
F^{sep}	A fixed separable closure of F.
$\mathrm{Hom}_F(K, F^{\mathrm{sep}})$	The set of embeddings of K into F^{sep}.
$\sigma, \sigma_1, \ldots, \sigma_n$	Embeddings of K into F^{sep}.
$N_{K/F}, T_{K/F}$	The norm and trace of K down to F.
$e_1, \ldots, e_n$	The elementary symmetric functions.
$\mathrm{discr}(f)$	The discriminant of a polynomial f.
D_K	The discriminant of an extension K over F
$d(K)$	The number $v_F(D_K)$.
A	An étale algebra over a field F, (Section 1.4).
$\mathcal{A}_n(F)$	Isomorphism classes of étale algebras over F of dimension n.
$\mathcal{A}_n^{\mathrm{tr}}(F)$	Totally ramified extensions in $\mathcal{A}_n(F)$.
$\mathcal{P}_n(F),\ \mathcal{P}_n$	The set of monic polynomials $f \in \mathcal{O}_F[x]$ of degree n.
$\mathcal{P}^A$	The set of monic polynomials which generate A over F.
$m_F(A)$	The volume $\mu(\mathcal{P}^A)$.
φ_A	Mapping that parameterizes the set $\mathcal{P}^A$.
$\tilde{F},\ (\tilde{\mathcal{O}}_F)$	The set of primitive elements of a field F, $(\mathcal{O}_F \cap \tilde{F})$.
I_K	The index form of an extension K over F, (Section 4.1).
S_n	The symmetric group on n letters.
C_n	The cyclic group of order n.
$c(K)$	The wild part of the discriminant, $d(K) - n + 1$.
$\mathcal{E}_n$	The set of Eisenstein polynomials of degree n over F.
λ	A q-tuple, $\lambda \in \mathbb{N}^q$ with $\sum_i \lambda_i = n$, (Section 4.3).
Φ_n	The n^{th} cyclotomic polynomial.
ϕ_n	The polynomial $q^n - 1$.

Bibliography

[1] Emil Artin. *Modern Higher Algebra: (Galois Theory).* Courant Institute of Mathematics, New York University, New York 1947.

[2] Nicolas Bourbaki. *Algèbre.* Éléments de mathématique, Livre I. Hermann, Paris, 1950.

[3] Nicolas Bourbaki. *Intégration.* Éléments de mathématique, Livre VI. Hermann, Paris, 1963.

[4] Nicolas Bourbaki. *Variétés Différentielles et Analytiques.* Éléments de mathématique, Fascicule de résultats, Paragraphes 8 à 15. Hermann, Paris, 1971.

[5] Ivan B. Fesenko and S. V. Vostokov. *Local Fields and their Extensions: a Constructive Approach.* Translations of mathematical monographs, volume 121. American Mathematical Society, Providence, Rhode Island, 1993.

[6] David M. Fudenberg. *Local class field theory: Abelian extensions of local fields.* Thesis (B.A.)–Reed College, 1982.

[7] István Gaál. *Diophantine Equations and Power Integral Bases: New Computational Methods.* Birkhäuser, Boston, 2002.

[8] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction.* Springer-Verlag, Heidelberg, 1993.

[9] Edwin Hewitt and Kenneth A. Ross. *Abstract Harmonic Analysis I.* Springer-Verlag, Berlin, 1963.

[10] Jun-ichi Igusa. *An Introduction to the Theory of Local Zeta Functions.* AMS/IP studies in advanced mathematics, volume 14. American Mathematical Society, Providence, Rhode Island, 2000.

[11] Rudolf Lidl and Harold Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, Cambridge, 1986.

[12] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The Book of Involutions.* Colloquium Publications, Volume 44. American Mathematical Society, Providence, Rhode Island, 1998.

[13] Kurt Mahler. *p-adic Numbers and their Functions.* Cambridge tracts in mathematics, volume 76. Cambridge University Press, Cambridge, 1980.

[14] Jürgen Neukirch. *Algebraic Number Theory.* Springer-Verlag, Berlin, 1999.

[15] Alain M. Robert. *A Course in p-adic Analysis.* Springer-Verlag, New York, 2000.

[16] Walter Rudin. *Fourier Analysis on Groups.* Interscience Publishers, New York, 1962.

[17] Jean-Pierre Serre. *Corps Locaux.* Hermann, Paris, 1962.

[18] Jean-Pierre Serre. Une « formule de masse » pour les extensions totalement ramifiées de degré donné d'un corps local. *C. R. Acad. Sci.*, **286** (1968), série A, 1031–1036.

[19] Herbert S. Wilf. *Generatingfunctionology.* Academic Press, Boston, 1994.