FAMILIES OF p-ADIC FIELDS

JORDI GUÀRDIA-RUBIES, JOHN W. JONES, KEVIN KEATING, SEBASTIAN PAULI, DAVID P. ROBERTS, AND DAVID ROE

ABSTRACT. We improve the database of p-adic fields in the LMFDB by systematically using Krasner-Monge polynomials and working relatively as well as absolutely. These improvements organize p-adic fields into families. They thereby make long lists of fields more manageable and various theoretical structures more evident. In particular, the database now includes all degree 16 extensions of $\mathbb{Q}_2$.

CONTENTS

1. INTRODUCTION

In arithmetic parts of mathematics, it is often useful to work one prime at a time. When working at a single prime p, the field $\mathbb{Q}_p$ of p-adic numbers commonly plays a central role. Also important are finite-degree field extensions of $\mathbb{Q}_p$. The number of isomorphism classes of such extensions of a given degree n is finite and given by a formula due to Monge [Mon11, Thm 1]. Some cardinalities are given in Table 1.1.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$p=2$	1	7	2	59	2	47	2	1823	3	158	2	5493	2	590	4	890111
$p=3$	1	3	10	5	2	75	2	8	795	6	2	785	2	6	1172	13
$p=5$	1	3	2	7	26	7	2	11	3	258	2	17	2	6	1012	17
$p=2$	1	3	2	10	2	8	2	49	3	10	2	43	2	12	4	389
$p=3$	1	2	4	3	2	10	2	4	28	4	2	20	2	4	16	5
$p=5$	1	2	2	3	6	4	2	4	3	16	2	6	2	4	20	5

TABLE 1.1. Top: The number of isomorphism classes of degree n field extensions of $\mathbb{Q}_p$. Bottom: The number of degree n families over $\mathbb{Q}_p$. Cases where all ramification is tame are in gray.

An online database giving defining polynomials and various invariants of p-adic fields appeared in 2006, in connection with the paper [JR06]. The original database

quickly expanded via various works [JR04, JR08, Awt12, ABM$^+$15], to include complete detailed tables for many (p, n), including all those listed on Table 1.1 except $(2, 16)$. Another improvement was a migration in 2011 from an *ad hoc* platform to the LMFDB [LMFDB], so that the data can be more easily inspected from a wider variety of perspectives.

The purpose of this paper is to describe a substantial improvement we have recently made to the database in the LMFDB. The starting point for the improvement is the systematic use of certain Eisenstein polynomials. These polynomials were introduced long ago by Krasner [Kra37] and their theory was brought into modern form by Monge [Mon14]. In this approach, fields are naturally organized into families. The number of families for small (p, n) is also given in Table 1.1.

The improved database is at

$$\texttt{https://olive.lmfdb.xyz/padicField/}$$

and has a page for each of the 19585 families with $p < 200$ and $n \leq 47$. In this range, there are about 115 billion fields. Pages for individual fields can be added to the database according to future needs. At present, among the fields which have pages are all the 890111 degree 16 extensions of $\mathbb{Q}_2$. Some supporting code for the database is at $\texttt{https://github.com/roed314/padic\_db}$.

The subsections of this introduction give a first idea of the previous structure of the database and how the systematic introduction of families improves it. Sections 2 and 3 then present the theory necessary for the improvement, with some of the more subtle details and various algorithmic issues deferred to the companion paper [GRJK$^+$]. Sections 4 and 5 encourage the reader to explore and appreciate the database, first by focusing on sample families and then by focusing on connections to various theorems in the Galois theory of p-adic fields.

1.1. **The previous field-by-field approach.** We begin by describing some aspects of the database as it stood before our recent improvements. Degree n fields were presented as $L = \mathbb{Q}_p[x]/f(x)$ with $f(x) \in \mathbb{Z}[x]$ a degree n polynomial obtained from a search over possibilities. Detailed attention was not paid to the choice of $f(x)$. Rather the focus was on the most important invariants of L.

The extension $L/\mathbb{Q}_p$ has a normal closure $L^{\text{gal}}/\mathbb{Q}_p$ and hence a Galois group $\text{Gal}(L^{\text{gal}}/\mathbb{Q}_p)$. The general theory of p-adic fields gives a decreasing filtration of this group by normal subgroups. The successive subquotients Q^s each have a size $|Q^s|$ and also an associated slope s. Here slopes of -1, 0, and positive rational numbers correspond to no ramification, tame ramification, and wild ramification.

The database focused on the filtered group $\text{Gal}(L^{\text{gal}}/\mathbb{Q}_p)$. Filtered groups are somewhat unwieldy objects, so the database gave only associated numerical invariants. To represent the group, it gave its standard label nTj in the list of conjugacy classes of transitive subgroups of the symmetric group S_n [BM83, CHM98, Hul05]. To represent the filtration, it gave the *Galois slope content* W_t^u. Here $u = |Q_{-1}|$, $t = |Q_0|$, and a wild subquotient Q^s of size p^ρ contributes ρ copies of s to the weakly increasing list W of wild slopes. So the word "content" is in the spirit of "Jordan-Hölder content."

As an example, one of the 795 nonic 3-adic fields L was represented by the polynomial

$$(1.1) \qquad f(x) = 21 + 18x + 18x^2 + 21x^3 + 9x^4 + 18x^5 + x^9.$$

The Galois group has $324 = 2^2 3^4$ elements. On the standard list from $9T1 = C_9$ to $9T45 = S_9$, it is $9T24$. The Galois slope content is $[\frac{1}{2}, \frac{1}{2}, \frac{2}{3}, \frac{3}{2}]_2^2$. In general, Galois groups were determined in the above-cited papers by computing and factoring many resolvents over $\mathbb{Q}_p$. The Galois slope content was determined by studying the ramification in the fields defined by these factors.

Previous to our current improvements, the database emphasized Artin slopes $\hat{s}_k = s_k + 1$ rather than our current slopes s_k, displaying e.g. $[\frac{3}{2}, \frac{3}{2}, \frac{5}{3}, \frac{5}{2}]_2^2$ in the above example. Artin slopes $\hat{s}_k$ are indeed often more convenient in global applications. We are now emphasizing the smaller slopes s_k, often called Swan slopes, because they are more natural in detailed local analyses.

1.2. **The new family approach.** The Galois slope content of any finite extension $L/\mathbb{Q}_p$ splits cleanly into the *visible slope content* $[s_1, \ldots, s_w]_e^f$, with associated degree $[L : \mathbb{Q}_p] = f\epsilon p^w$, and the rest, called *hidden slope content*, with associated degree $[L^{\mathrm{gal}} : L]$. In example (1.1), the visible slope content is $[\frac{1}{2}, \frac{3}{2}]_1^1$ and the hidden slope content is $[\frac{1}{2}, \frac{2}{3}]_2^2$. The visible slope content is enormously easier to compute than the hidden slope content. As we will explain, no Galois-theoretic concepts are needed.

We say that two extensions of $\mathbb{Q}_p$ belong to the same *absolute family* if their visible slope contents are the same. The key idea underlying this paper is that one can find defining polynomials for all the extensions in a family by suitably specializing a single *generic polynomial* belonging to the family. These specializations are the previously mentioned Krasner-Monge polynomials.

Continuing the example begun in (1.1), consider the family of 3-adic fields with visible slope content $[\frac{1}{2}, \frac{3}{2}]_1^1$. Following the general recipe we will present, the generic polynomial is

$$(1.2) \qquad f(a_3, a_{10}, b_{11}, b_{13}, \pi, x) = \pi \left(1 + a_{10}\pi x + b_{11}\pi x^2 + a_3 x^3 + b_{13}\pi x^4 \right) + x^9.$$

Specializing via $\pi = 3$, $a_\sigma \in \{1, 2\}$, and $b_\sigma \in \{0, 1, 2\}$ gives thirty-six 3-Eisenstein polynomials in $\mathbb{Z}[x]$. They represent bijectively the thirty-six entries on the list of 795 nonic 3-adic fields which have visible slope content $[\frac{1}{2}, \frac{3}{2}]_1^1$. It couldn't be easier! Moreover, as an important bonus, the coordinates provided by generic polynomials often give rise to clean descriptions of the hidden invariants. In the case of (1.2) there are ten possibilities for the pair consisting of the Galois group and the hidden slope content, one pair being the above $(9T24, [\frac{1}{2}, \frac{2}{3}]_2^2)$. Three fields have this pair, namely the ones with $(a_3, a_{10}, b_{11}) = (1, 2, 2)$. The particular field defined by (1.1) comes from $b_{13} = 2$. The other nine subsets likewise have very elementary descriptions, as can be seen in Table 4.1.

Our sample visible slope content $[\frac{1}{2}, \frac{3}{2}]_1^1$ has two simplifying features: its unramified degree f is 1 and the other data in the visible slope content measuring ramification is *rigid*, as we will explain in §2.3. We broadly describe the general case in this paper, but defer a full treatment of the complications associated with $f > 1$ and nonrigidity to [GRJK$^+$].

Using symbols like $[\frac{1}{2}, \frac{3}{2}]_1^1$ in a naming scheme for families would be unwieldy as part of a URL. The database instead uses labels in the form $p.f.e.cL$, as in `3.1.9.18b` for the example. Here c is the common discriminant-exponent of all the fields in the family and the letter L resolves ambiguity. Similarly, the mathematically ideal Eisenstein coefficients do not work well as labels identifying fields within a family. The database instead appends a subfamily number ℓ followed by

a counter j, so that the example field (1.1) becomes `3.1.9.18b4.1`. In (1.2), two fields are in the same subfamily if they have the same (a_3, a_{10}). The general notion of subfamily involves residual polynomials and is given in [GRJK$^+$].

1.3. **The new relative context.** The paper [JR06] and the subsequent papers extending the database were aggressively absolute: p-adic fields of degree N were always given by a degree N polynomial with coefficients in $\mathbb{Z}$. However it is often better to build fields in towers and the theory of generic polynomials fits perfectly into this paradigm. The theory of slopes generalizes to this relative context and we say that two extensions L_1/K and L_2/K belong to the same family over K if they have the same relative visible slope content $I = [s_1, \ldots, s_w]_\epsilon^f$. We denote this family, viewed simply as a finite set of isomorphism classes of extensions, by I/K.

Henceforth, we call I a *Herbrand invariant*, because we have other ways of expressing the data in I that do not directly involve slopes, as we will be explaining in the next section. In fact our viewpoint is that p-adic Herbrand invariants are simple combinatorial objects that could be described independently of p-adic fields. To get a family, one combines two objects of different nature, I and K, subject to a numerical compatibility condition.

To continue the example begun in (1.1) yet further, take any finite extension K of $\mathbb{Q}_3$ as ground field, with residual cardinality denoted by q. Consider all extensions L/K with Herbrand invariant $I = [\frac{1}{2}, \frac{3}{2}]_1^1$. This family I/K is again bijectively indexed by certain specializations of the exact same generic polynomial (1.2). The difference is that π now is specialized to a uniformizer of K, rather than to the uniformizer 3 of $\mathbb{Q}_3$, and the a_i and b_i to elements of K with distinct reductions modulo π. Thus the real purpose of (1.2) is to get all relative extensions L/K of type $[\frac{1}{2}, \frac{3}{2}]_1^1$, for any fixed 3-adic base field K. Directly generalizing the case $K = \mathbb{Q}_3$, this family has cardinality $|I/K| = (q-1)^2 q^2$.

While we work relatively throughout this paper, the improved database keeps the original context of p-adic fields L as one of its two focal points. It has a basic bipartite structure. On the one hand, each p-adic field L within range has, as before, a homepage. On the other hand, each family I/K now also has a homepage. The two homepages are linked if K can be realized as a subfield of L such that L is in the family I/K.

In the case of the example family $[\frac{1}{2}, \frac{3}{2}]_1^1/\mathbb{Q}_3$, each field L in it has exactly one cubic subfield K' having discriminant-exponent 3. The cubic extension L/K' then appears in the relative family $[\frac{7}{2}]_1^1/K'$. There are two possibilities for K', namely `3.1.3.3a1.1` or `3.1.3.3a2.1`, each of which occurs for half of the L. So the fields in the absolute family $[\frac{1}{2}, \frac{3}{2}]_1^1/\mathbb{Q}_3$ come half each from the relative families `3.1.3.3a1.1-1.3.9a` and `3.1.3.3a2.1-1.3.9a`. Here, the syntax for relative families is (base field)-$f.e.c$(tiebreaker). Two fields L in $[\frac{1}{2}, \frac{3}{2}]_1^1/\mathbb{Q}_3$ also have three more cubic subfields, now with discriminant-exponent 5. The index page `olive.lmfdb.xyz/padicField/families/?label_absolute=3.1.9.18b` gives an overview of all possibilities.

1.4. **Notation.** We gather and comment on our most basic notations for the reader's convenience. As already indicated, a prime p is fixed, the symbol K is reserved for a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, and the symbol L is reserved for a finite extension of K. We let $\mathcal{O}$ be the ring of integers of K, Π its

maximal ideal, $\kappa = \mathcal{O}/\Pi$ its residue field, and $q = |\kappa|$ its residual cardinality. We usually view K as fixed and L as varying.

Many fields and numbers are associated to a given L/K. The most basic come from its standard tower

$$(1.3) \qquad K \overset{f}{\subseteq} L_{\mathrm{ur}} \overset{\epsilon}{\subseteq} L_0 \overset{p^w}{\subseteq} L.$$

Here L_{ur} is the maximal unramified subextension and L_0 is the maximal tamely ramified subextension. The superscripts indicate relative degrees so that the entire degree $n = [L : K]$ comes with a canonical factorization, $f\epsilon p^w$.

The most familiar quantity capturing ramification in L/K is the discriminant $\mathrm{disc}(L/K) = \Pi^c$. We are emphasizing the importance of the discriminant-exponent c in our LMFDB labeling scheme. But for deeper analysis we prefer to switch to the *mean m* via the transformation equation

$$(1.4) \qquad c = f(e - 1 + em).$$

So in the continuing nonic 3-adic example, the focus on $c = 18$ is shifted onto $m = 10/9$.

Most of our attention is focused on a discrete invariant W measuring the wild ramification present in the extension L/L_{ur}. One way to describe W is by the vector $[s_1, \ldots, s_w]$ already emphasized. Two similar ways are given in (2.4) and (2.5) and relations are summarized either by (2.6) and (2.7) or, in a different manner, by (3.6) and (3.7). The invariant W is the wild part of the Herbrand invariant $I = \mathrm{Inv}(L/K) = W_\epsilon^f$.

The set of all extensions L/K sharing a given I is denoted I/K. We think of I as a discrete invariant of L/K. In contrast, we view the invariants necessary to distinguish fields inside of I/K as continuous. They have their own complicated notation, introduced in Section 3.

All the notation for L/K has its analog for $K/\mathbb{Q}_p$, starting with $\mathbb{Q}_p \subseteq K_{\mathrm{ur}} \subseteq K_0 \subseteq K$. If we were to name everything, we would have to take care to avoid notation clashes. Fortunately, our considerations here make very little use of the internal structure of K, as we are focused mainly on extensions of K. The invariants of K which enter our considerations most often are its absolute ramification index $e_K = [K : K_{\mathrm{ur}}] = \mathrm{ord}_\Pi(p)$ and the above-mentioned residual cardinality $q = |\kappa|$.

In Sections 2 and 3 we work completely constructively, making no mention of any algebraic closure of $\mathbb{Q}_p$. In Sections 4 and 5 the attention shifts to Galois theory. There we fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and view the ground field K as in $\overline{\mathbb{Q}}_p$. Given an abstract extension L/K of degree n, we let L^{gal} be the compositum of the images of the n different K-linear embeddings of L into $\overline{\mathbb{Q}}_p$. So the Galois group $\mathrm{Gal}(L^{\mathrm{gal}}/K)$ is a quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$.

1.5. The Laurent series case.

There is an extremely parallel case where one replaces the absolute ground field $\mathbb{Q}_p$ by the field $\mathbb{F}_p((t))$ of Laurent series over $\mathbb{F}_p$. The direct connections between these two cases is of great current interest [Sch14, §2]. As the database contains only extensions of $\mathbb{Q}_p$, we will limit our discussion of the Laurent series case to occasional brief remarks that clarify the p-adic case.

2. Herbrand invariants

Herbrand invariants are fundamental to this paper because they index families. This section explains what they are and how to work with them explicitly.

2.1. **An elementary approach emphasizing canonical subfields.** Serre's standard text [Ser79, IV] associates a Herbrand function $\phi : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ to any Galois extension L/K of p-adic fields. The construction involves filtering $\mathrm{Gal}(L/K)$ by a descending family of subgroups indexed in two ways, by lower and upper numbering. Remark 1 of [Ser79, IV.3] extends the definition of ϕ to general extensions L/K by reduction to the Galois case. Details of this reduction were first explained in print by Deligne in a six-page appendix to [Del84].

It is less widely known that the Herbrand function of a general extension L/K can be understood without any reference to group theory whatsoever. In this subsection, we use the method of *slope polygons* to get relevant numerical quantities. We are following [JR06, §3.4], except that the Artin slopes there are translated to Swan slopes here. Figure 2.1 starts our second continuing example, based on

$$(2.1) \qquad\qquad f(x) = 1 + 6x^4 + x^8.$$

This particular polynomial is chosen because it defines a Galois extension over both $\mathbb{Q}$ and $\mathbb{Q}_2$, with Galois group D_4. The reader can then follow along, using number field software to confirm our statements, e.g. *Pari*'s `nfsubfields` to get subfields and `smalldiscf` to get their discriminants and ultimately their means via (1.4). The fact that this example is Galois is irrelevant for the method we are describing.

Consider towers $L/L'/L_{\mathrm{un}}/K$. For each, one has the degree $e' = [L' : L_{\mathrm{un}}]$, the mean m' of L'/L_{un}, and thus a point $(e', e'm')$ in a Cartesian plane. The *slope polygon* S is the lower boundary of the convex hull of all such points. Over each interval $[\epsilon p^{k-1}, \epsilon p^k]$ the polygon S is just a segment with some slope s_k. The symbol $[s_1, \ldots, s_w]_\epsilon^f$ is then the visible slope content emphasized in the introduction.
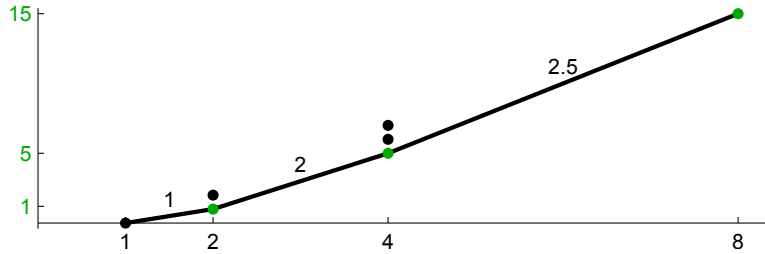

FIGURE 2.1. The slope polygon S associated to the octic extension $L/\mathbb{Q}_2$ defined by (2.1). The slopes $[1, 2, 2.5]$ and means $\langle \frac{1}{2}, \frac{5}{4}, \frac{15}{8} \rangle = \langle 0.5, 1.25, 1.875 \rangle$ are indicated.

Define h to be the function on $[1, e]$ having graph S. For $k = 1, \ldots, w$, define $m_k = \frac{h(\epsilon p^k)}{\epsilon p^k}$. Clearly, the data $\langle m_1, \ldots, m_w \rangle_\epsilon^f$ contains the exact same information as $[s_1, \ldots, s_w]_\epsilon^f$. If the point $P_k = (\epsilon p^k, \epsilon p^k m_k)$ is a turning point or the right endpoint of S then we say that the index k is final. Then P_k comes from exactly one tower $L/L_k/L_{\mathrm{un}}/K$. The standard chain (1.3) can be extended to a more refined chain from K to $L = L_w$ by including all the other *canonical subfields* L_k. Note that for a final index k, the extension L_k/L_{un} has mean m_k. For a non-final index k, there may or may not be a tower mapping to P_k. In the example, the indices $k = 1$, 2, and 3 are all final.

2.2. **Four perspectives on Herbrand invariants.** The *slopes* s_k just introduced are usually called *breaks in the upper numbering*. There is similarly a dual polygon called the ramification polygon in which certain elementary quantities r_k appear along with the means m_k again. These *rams* r_k coincide with the *breaks in the lower numbering*. We will emphasize our elementary and non-Galois-theoretical viewpoint by using these two terms systematically, and not making further reference to breaks or numbering. Even when we bring back Galois groups in the last two sections, we will use the briefer terminology of slopes.

We write the Herbrand invariant of a p-adic extension L/K in four ways, the first classical but the others advantageous in various situations:

$$(2.2) \qquad \mathrm{Inv}(L/K) = (\phi, f) \qquad\qquad (\phi \text{ is the Herbrand function})$$

$$(2.3) \qquad\qquad\qquad = [s_1, \ldots, s_w]_\epsilon^f \qquad\qquad (\text{the } s_k \text{ are the slopes})$$

$$(2.4) \qquad\qquad\qquad = \langle m_1, \ldots, m_w \rangle_\epsilon^f \qquad\qquad (\text{the } m_k \text{ are the means})$$

$$(2.5) \qquad\qquad\qquad = (r_1, \ldots, r_w)_\epsilon^f \qquad\qquad (\text{the } r_k \text{ are the rams}).$$

As a matter of notation, the subscript ϵ and superscript f are allowed to be omitted when they are 1. Our key reference [Mon14] had different aims that did not require emphasis on Herbrand invariants. However it makes essential use of all the quantities s_k, m_k and r_k.
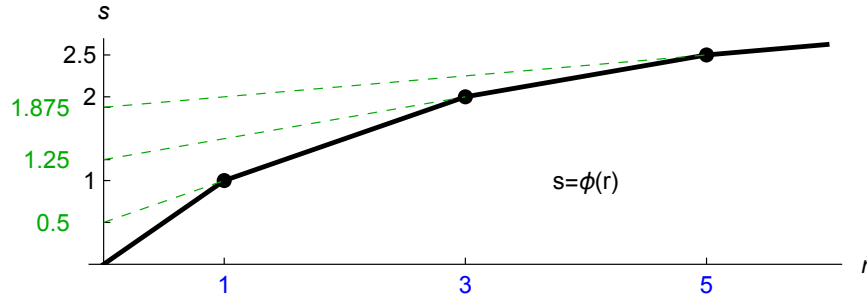

FIGURE 2.2.   The Herbrand function ϕ for the octic extension $L/\mathbb{Q}_2$ defined by (2.1). It takes the rams $(r_1, r_2, r_3) = (1, 3, 5)$ of this extension to its slopes $[s_1, s_2, s_3] = [1, 2, 2.5]$. The means $\langle 0.5, 1.25, 1.875 \rangle$ are obtained by the indicated extensions of segments.

As a convention, we put $s_0 = m_0 = t_0 = 0$. Then (2.3)-(2.5) are related via

$$(2.6) \qquad s_k = \frac{pm_k - m_{k-1}}{p-1}, \qquad\qquad m_k = \sum_{j=1}^{k} \frac{p-1}{p^{k+1-j}} s_j,$$

$$(2.7) \qquad r_k = \epsilon p^k \frac{m_k - m_{k-1}}{p-1}, \qquad\qquad m_k = \sum_{j=1}^{k} \frac{p-1}{\epsilon p^j} r_j.$$

Formulas (2.6) reflect the perspective of slope polygons: each slope s_k is a certain rise-over-run and each mean m_k is a weighted average of slopes, with the formal slope $s_0 = 0$ having coefficient $1/p^w$, so that the coefficients sum to one. Formulas (2.7) reflect the dual perspective of ramification polygons. Direct transformation

formulas between slopes and rams are a little more complicated, and one can just compose two transformations with means in the middle.

Figure 2.2 uses our octic 2-adic continuing example to illustrate how the classical version (2.2) is related to the more numerical versions (2.3)-(2.5). In general, the graph of ϕ starts at $(r_0, s_0) = (0, 0)$ and goes linearly to the (r_k, s_k) in order, with an actual step being taken only if k is a final index, as otherwise we have $(a_k, b_k) = (a_{k+1}, b_{k+1})$. It ends with a ray emanating from (r_w, s_w). If k is 0 or a final index then the slope of the segment leaving (r_k, s_k) is $1/(\epsilon p^k)$. With this strong condition on slopes of the Herbrand segments, just ϕ determines all the s_k, m_k, and t_k.

2.3. **Automorphisms, mass, and rigidity.** An automorphism in $\mathrm{Aut}(L/K)$ necessarily stabilizes all of the canonical subextensions of L/K. Because of this fact, the Herbrand invariant I alone constrains the size of $\mathrm{Aut}(L/K)$. A key input is that if k is a final index, with the ram r_k having been repeated ρ times, then the inertia group associated to $L_k/L_{k-\rho}$ has the form $C_p^\rho \rtimes C_d$, where d is the denominator of the ram r_k. The action is such that the step can only have nontrivial automorphisms if $d = 1$, i.e. if r_k is integral.

Define the *ambiguity number* of a p-adic Herbrand invariant $(r_1, \ldots, r_w)_\epsilon^f$ to be $\mathrm{Amb}(I) = f\epsilon p^i$, where i is the number of integral rams (see §3.5 for further discussion of related notions). Then an extension L/K in any I/K has $|\mathrm{Aut}(L/K)|$ dividing $\mathrm{Amb}(I)$. The *mass* of L/K is by definition $1/|\mathrm{Aut}(L/K)|$ and L/K is called *rigid* if its mass is 1. We say that I is *rigid* if $\mathrm{Amb}(I) = 1$. So all extensions L/K in a family I/K with a rigid I are rigid.

2.4. **Classification of Herbrand invariants.** To classify all Herbrand invariants and say which actually occur over a given ground field K, it is best to use rams as was done in different language in [PS17, Prop 3.10]. First consider totally wildly ramified extensions L/K of degree p^ρ having just a single ram r repeated ρ times. The possibilities for r depend only on the absolute ramification index e_K of the ground field K.

Define first $\mathcal{R}_\rho^\infty$ to be the set of positive rational numbers with denominator dividing $p^\rho - 1$ and numerator not dividing p. Then $\mathcal{R}_\rho^\infty$ is the correct collection of r in the parallel case of Laurent series ground fields $\mathbb{F}_q((t))$. For the characteristic zero fields K on which this paper is focused, the set of possibilities $\mathcal{R}_\rho^{e_K}$ contains all the elements of $\mathcal{R}_\rho^\infty$ which are less than $pe_K/(p-1)$. These elements exhaust $\mathcal{R}_\rho^{e_K}$ except that $\mathcal{R}_1^{e_K}$ also contains $pe_K/(p-1)$. We call this last ram *arithmetic* and all the smaller rams *geometric*.

Now consider all extensions L/K with canonical factorization $f\epsilon p^w$. The Herbrand invariants that can arise are $(r_1, \ldots, r_w)_\epsilon^f$ where the r_k are weakly increasing and each in their allowed set, from the above considerations. For example, to get all strictly increasing sequences, each r_k is chosen from $\mathcal{R}_1^{e_K \epsilon p^{k-1}}$. This description lets one produce any entry on the lower half of Table 1.1. If p is relatively prime to n, then the wild considerations are all vacuous and the possible Herbrand invariants are simply $(\ )_\epsilon^{n/\epsilon}$ as ϵ runs over divisors of n.

Figure 2.3 illustrates the case of Herbrand invariants (r_1, r_2) over 2- and 3-adic fields, with an eye towards giving a visual understanding of the general case. Rather than represent a Herbrand invariant I by a point at (r_1, r_2), we represent I by an integer. This integer is the mass of the family I/K, where K is any ground field
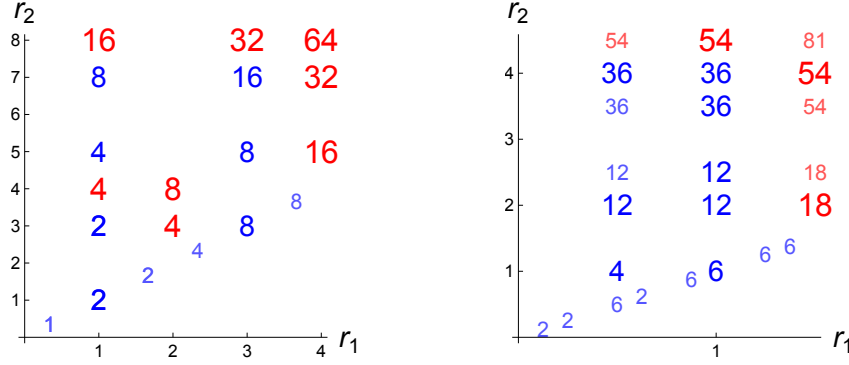
FIGURE 2.3. Herbrand invariants (r_1, r_2) with $r_j \le ep^j/(p-1)$.
Left: $(p, e) = (2, 2)$. Right, $(p, e) = (3, 1)$.

compatible with I and having residue field of size p, as explained around (3.5). Families for which both rams are geometric are presented in blue, and families which have an arithmetic ram are presented in bold red. Making an independent distinction, rigid families are indicated by a smaller font.

One should imagine each of these pictures extended to the entire first quadrant of the (r_1, r_2) plane, so that for each positive integer j there is a bold red hook H_j of entries with upper right corner at $(jp/(p-1), jp^2/(p-1))$. The Herbrand invariants compatible with a given p-adic field K are exactly the arithmetic ones on H_{e_K} and the geometric ones under H_{e_K}.

As a numerical example, consider the total number of families over $\mathbb{Q}_p$ with degree p^2. There is just one family with ramification index $e = 1$, the unramified family $(\ )^{p^2}$. There are p families with $e = p$, the geometric families $(1)^p$, $(2)^p$, ..., $(p-1)^p$ and the arithmetic family $(p)^p$. Guided by Figure 2.3, one can check that there are $p^3 - \frac{p^2}{2} + \frac{p}{2}$ families with $e = p^2$. For $p = 2$ and 3 respectively, the total counts are $1 + 2 + 7 = 10$ and $1 + 3 + 24 = 28$, with 7 and 24 being the numbers of families on or under H_1 on Figure 2.3 and 10 and 28 appearing as entries in the lower half of Table 1.1.

To see the seven and twenty-four families $p.1.p^2.C$ listed as an indexing table, one can search for absolute families with residual characteristic p, residual field degree $f = 1$, and ramification degree $e = p^2$. To see a sixteen-line table corresponding to the $e_K = 2$ case of the left side of Figure 2.3, one can search analogously for relative families. One needs to input an appropriate ground field by its label, say $K = \mathbb{Q}_2(i)$ by 2.1.2.2a1.1, as well as $f = 1$ and $e = 4$ again. The three tables produced in this paragraph contain summary information, such as the masses appearing in Figure 2.3.

2.5. **Explicit composition via sorting.** Let $L/K/Q/\mathbb{Q}_p$ be a tower with

$$(2.8) \quad \text{Inv}(K/Q) = (t_1, \ldots, t_{w'})_{\epsilon'}^{f'} \quad \text{and} \quad \text{Inv}(L/K) = (t_{w'+1}, \ldots, t_{w'+w''})_{\epsilon''}^{f''}.$$

A great virtue of the traditional functional presentation of Herbrand invariants is that one has the simple formula $\phi_{L/Q}(r) = \phi_{K/Q}(\phi_{L/K}(r))$. Here we translate this

formula into the more explicit language of rams, so as to be able to go directly from (2.8) to $\mathrm{Inv}(L/Q) = (r_1, \ldots, r_w)_\epsilon^f$

Of course, $f = f'f''$, $\epsilon = \epsilon'\epsilon''$, and $w = w' + w''$. To do the nontrivial part, we first define $T_k = \epsilon''t_k$ and formally write

$$(2.9) \qquad \mathrm{Inv}(L/Q) = (T_1, \ldots, T_{w''}, t_{w''+1}, \ldots, t_w)_\epsilon^f.$$

Then we change the entries of the w-vector by iterating the following replacement in any order. Whenever there are two adjacent entries (a, b) with $a > b$, replace them with $(b, b + p(a - b))$. When the w-vector becomes weakly increasing, it is the desired ram vector $(r_1, \ldots, r_w)$.

The database uses this procedure to pass from the Herbrand invariant of a general relative extension L/K to the Herbrand invariant of the corresponding absolute extension $L/\mathbb{Q}_p$. If K is a canonical subfield of L, both steps of the process are trivial and, very simply, $r_k = t_k$ for all k.

To see the duality between rams and slopes, one can consider a modification of this process. Step 1 yielding (2.9) is exactly the same. In the modified Step 2, one iteratively replaces adjacent increasing (a, b) by $(b, b - (b - a)/p)$ until the w-vector becomes weakly decreasing. As a new final Step 3, one reverses the w-vector obtained to make it weakly increasing. The kth entry of this final vector is ϵs_k, where s_k is the kth slope of the extension L/Q.

3. EISENSTEIN POLYNOMIALS

This section pictorially describes a well-behaved finite set $\mathrm{Eis}(L/K)$ of Eisenstein polynomials defining any given totally ramified extension L/K. Thus $f = 1$ for the entirety of this section.

3.1. **Set-up.** Let $\mathrm{Eisen}(e/K)$ be the space of Eisenstein polynomials of degree e over K. We write an element of $\mathrm{Eisen}(e/K)$ as

$$(3.1) \qquad f(x) = F_0 + F_1 x + \cdots + F_{e-1} x^{e-1} + x^e.$$

So the F_i run over the maximal ideal Π of the ring of integers $\mathcal{O}$ of K, except that F_0 is not in Π^2. One has decompositions into finitely many parts,

$$(3.2) \qquad \mathrm{Eisen}(e/K) = \sqcup_I \mathrm{Eisen}(I/K), \qquad \mathrm{Eisen}(I/K) = \sqcup_L \mathrm{Eisen}(L/K).$$

On the left, I runs over totally ramified degree e Herbrand invariants that are compatible with K. On the right, L runs over isomorphism classes of extensions of K which have Herbrand invariant I.

To present things as concretely as possible, we choose a generator π of Π. We choose also a set of representatives $\tilde{\kappa}$ containing 0 and 1 for the q-element residue field κ. Rather than work with the F_i, we will work with π-adic expansions, writing each F_i as $\pi \sum_{j=0}^\infty f_{i,j} \pi^j$, with $f_{i,j} \in \tilde{\kappa}$. If K is unramified over $\mathbb{Q}_p$ we always take the uniformizer π to just be p. A theoretically natural choice would be to take the nonzero elements of $\tilde{\kappa}$ to be the $(q-1)^{\mathrm{st}}$ roots of unity in K. However, we make the computationally more convenient choice of $\tilde{\kappa} = \{0, \ldots, q-1\}$ when q is prime.

It will also be convenient to use single-indexing simultaneously with double-indexing, with σ and (i, j) determining each other via $\sigma = je + i$, $j = \lfloor \sigma/e \rfloor$, and $i \in \{0, \ldots, e-1\}$. With this convention, (3.1) is written

$$(3.3) \qquad F(x) = \pi \left(\sum_{\sigma=0}^\infty f_\sigma \pi^j x^i \right) + x^e.$$

The last term x^e will not be mentioned much in our narrative because it does not contain an unspecified coefficient.

A problem with the right part of (3.2) is that the sets involved are infinite. We will be replacing these sets by finite nonempty sets $\mathrm{Eis}(I/K) = \sqcup_L \mathrm{Eis}(L/K)$. In the case when I is rigid, each of the $\mathrm{Eis}(L/K)$ contains just one polynomial.

3.2. **Eisenstein diagrams.** Fix a totally ramified Herbrand invariant $I = [s_1, \ldots, s_w]_\epsilon$. To explicitly describe the sets $\mathrm{Eis}(I/K)$ for all compatible K at once, we consider the *Eisenstein diagram of I* in the vertical strip R with horizontal coordinate $i \in [0, e)$ and vertical coordinate $s \in [0, \infty)$. As indicated by the name, this diagram depends on I only, not on K. Always we draw only $[0, e) \times [0, s_w]$ as there is no useful information associated to the rest of the strip.

Figures 3.1 and 3.2 each show the Eisenstein diagram for a family discussed previously, as described in their captions. Most of our discussion of Eisenstein diagrams is supported by one or both of these figures. We will give links to the database for illustrations of other phenomena.

A spiral with points representing terms. We think of the rectangle R as a cut and unrolled cylinder, with each horizontal line segment of constant level s coming from a circle. We draw the spiral that starts at $(0,0)$ and goes up with slope $1/e$. This spiral wraps every time it meets the right edge of R. The part of the spiral that goes from $(0, j)$ to $(e, j+1)$ is called the jth ramp.

We place conditions on the term $\pi f_\sigma \pi^j x^i$ by referring to the unique point P_σ on ramp j with horizontal coordinate i. Equivalently P_σ is the unique point on the spiral with $s = \sigma/e$. Thus $P_0 = (0,0)$ is the starting point of the spiral, and as one goes up one encounters the points $P_1, \ldots, P_{\lfloor es_w \rfloor}$ in order.
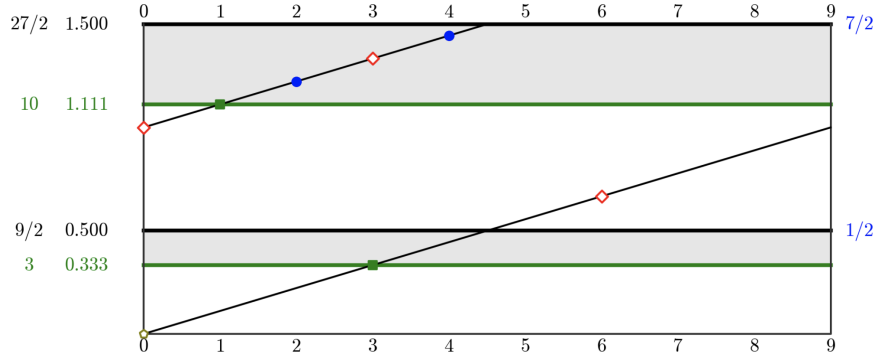

FIGURE 3.1. The Eisenstein diagram of the introductory nonic 3-adic Herbrand invariant with means $\langle \frac{1}{3}, \frac{10}{9} \rangle$, slopes $[\frac{1}{2}, \frac{3}{2}]$, rams $(\frac{1}{2}, \frac{7}{2})$, and generic polynomial (1.2). Various general facts are relatively easy to see here because the two bands do not overlap.

Bands. For $k = 1, \ldots, w$, the band B_k is defined to be the set of points in R satisfying $m_k \leq s < s_k$. As k increases, the m_k strictly increase and so the bottom edges of bands go up. However the s_k only weakly increase. So the top edges of the bands B_k for k in a segment of common s_k agree, even as the widths of these bands successively decrease by a factor of p, as in `2.1.16.30a`, the sample family

summarized in Table 4.3. It will also be convenient to let B_0 denote the bottom edge of the rectangle, i.e. the points with $s = 0$.

We shade bands by gray and indicate overlaps by darkening the gray. We color bottom edges of bands green and the bounding top edges black. In the rare cases where an upper edge agrees with a lower edge we dash this boundary using black and green, as in `2.1.16.79a`, the family highlighted in §5.5. These conventions assist in visually identifying the bands, even when they overlap.

Index and types of points. We say that the *index* of an integer $i \in [0, e)$ is $k = w - \mathrm{ord}_p(\gcd(i, p^w)) \in \{0, 1, \ldots, w\}$. We partition the points P_σ into five types, using colors and shapes to distinguish the types.

The point $P_0 = (0, 0)$ plays a special role. We call it the *D-point* and we mark it by an olive pentagon. A D-point is *critical* and drawn solid if $\epsilon > 1$. Otherwise it is *negligible* and drawn hollow. Here, like with the red diamonds below, the solidness indicates complications in the process of choosing unique distinguished polynomials for fields L/K in the family I/K.

For $\sigma > 0$, we use the band B_k to classify the points P_σ of index k as follows.

- *Z-points* are points beneath B_k. Their associated color is *clear,* meaning we don't draw them.
- *A-points* are the unique points P_σ which are at the bottom edge of geometric bands B_k for which k is final in its segment, meaning that either $k = w$ or $s_{k+1} > s_k$. We draw them as *solid green squares.*
- *B-points* are points in their governing band B_k which are not A-points. They are represented by *solid blue disks.*
- *C-points* are points above their governing band. They are represented by *red diamonds.* A C-point is *critical* and drawn solid if it is on the top border of any band. Otherwise it is *negligible* and drawn hollow.

The infinite set $\mathrm{Eisen}(I/K)$ now has the following explicit description. It is the subset of $\mathrm{Eisen}(e/K)$ where $f_\sigma = 0$ for Z-points and $f_\sigma \neq 0$ for A-points. The key finite set $\mathrm{Eis}(I/K)$ is the subset of $\mathrm{Eisen}(I/K)$ where $f_0 = 1$ if the D-point is negligible and $f_\sigma = 0$ for negligible C-points. The fact that $\mathrm{Eis}(I/K)$ still represents all extensions in I/K is not at all obvious. The proof of a considerably stronger statement is by Monge's reduction algorithm [Mon14, §2]. Basic aspects of this theory will be described in §3.5 below, and the full theory is described in a computational context in [GRJK$^+$].

3.3. Generic polynomials and numerics.

The generic polynomial for a given Herbrand invariant has the form $\left(\pi \sum_\sigma f_\sigma \pi^j x^i\right) + x^e$. Here σ runs over all nonnegative integers for which P_σ is drawn, but not negligible. To make structure more evident, we replace f_σ by d_σ, a_σ, b_σ, or c_σ according to whether P_σ is a D-point, A-point, B-point, or C-point. So when these coefficients run independently over $\tilde{\kappa}$, except for the inequalities $d_0, a_\sigma \neq 0$, one gets the set $\mathrm{Eis}(I/K)$. As an example beyond (1.2), the generic polynomial corresponding the 2-adic Herbrand invariant $[1, 2, 2.5] = (1, 3, 5) = \langle 0.5, 1.25, 1.875 \rangle$ of Figures 2.1, 2.2 and 3.2 is

$$f(a_4, a_{10}, a_{15}, b_{14}, b_{17}, b_{19}, c_8, c_{16}, c_{20}; \pi; x) = (\pi + \pi^2 c_8 + \pi^3 c_{16}) + \pi^3 b_{17} x +$$

(3.4) $$\pi^2 a_{10} x^2 + \pi^3 b_{19} x^3 + (\pi a_4 + \pi^3 c_{20}) x^4 + \pi^2 b_{14} x^6 + \pi^2 a_{15} x^7 + x^8.$$

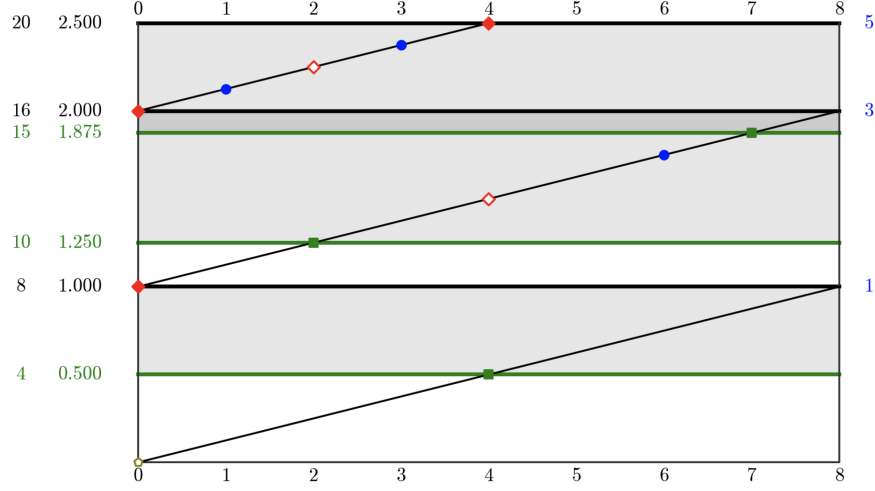Other examples are given in the next sections.

FIGURE 3.2. Eisenstein diagram for the octic 2-adic Herbrand invariant with means $m = \langle 1, \frac{5}{2}, \frac{15}{8} \rangle$, slopes $s = [1, 2, \frac{5}{2}]$, and rams $r = (1, 3, 5)$.

Let $\delta \in \{0,1\}$ be the number of critical D-points, and let α, β, and γ be the number of A-points, B-points, and critical C-points respectively. Clearly $|\mathrm{Eis}(I/K)| = (q-1)^{\delta+\alpha} q^{\beta+\gamma}$. Monge reduction (see §3.5) says that $|\mathrm{Eis}(L/K)| = (q-1)^\delta q^\gamma / |\mathrm{Aut}(L/K)|$. Accordingly, one gets a mass formula

$$(3.5) \qquad M(I) := \sum_{L/K \in I/K} \frac{1}{|\mathrm{Aut}(L/K)|} = (q-1)^\alpha q^\beta.$$

In the rigid case $\delta = \gamma = 0$ where $|\mathrm{Aut}(L/K)| = 1$ is forced, (3.5) becomes a cardinality formula. As a non-rigid example, from `2.1.8.22d` there are 32 fields in the family (3.4), with (3.5) becoming $8(\frac{1}{8}) + 20(\frac{1}{4}) + 4(\frac{1}{2}) = 8$.

The numbers $M(I)$ in Figure 2.3 come from (3.5) with q set equal to either 2 or 3. A clarifying check on various numbers is to view the space $\mathrm{Eisen}(e/K)$ of degree e Eisenstein polynomials over K as an infinite product $\mathbb{F}_q^\times \times \mathbb{F}_q \times \mathbb{F}_q \times \cdots$, with the successive factors corresponding to the variables f_0, f_1, f_2, ... Giving each factor its uniform probability measure turns $\mathrm{Eisen}(e/K)$ into a probability space. Serre proved in [Ser78, Thm. 2] that the chance that a random polynomial in $\mathrm{Eisen}(e/K)$ is in $\mathrm{Eisen}(I/K)$ is the Serre mass $SM(I) = M(I)/q^{em_w}$. Figure 2.3 lets one see the terms in the resulting formula $\sum_{I/K} SM(I) = 1$ for three different (p, e_K). Taking the easiest case $(2, 1)$ as an example, there are seven families, and one can use $em_2 = 2r_1 + r_2$. The sum is the dot product $(1, 2, 2, 2, 4, 4, 8) \cdot 2^{-(1,3,5,5,6,7,8)}$ and it is indeed 1.

3.4. **Slopes, means, and rams on Eisenstein diagrams.** When drawing Eisenstein diagrams, both here and on the family pages of the database, we indicate the slopes, means, and rams in appropriate places. There is no need to tick the vertical axis at the left of the diagram in the traditional way, because the left endpoint of the jth ramp is the integer j. Instead we give decimal approximations to lower edges m_k and upper edges s_k. In the leftmost column, we also give the scaled versions

em_k and es_k. These scaled versions make the subscripts on the marked points P_σ more immediately identifiable.

The ram r_k is printed to the immediate right of the upper boundary of the band B_k. It gives two point counts as follows. First, keeping in mind that B_k includes its lower boundary but not its upper boundary, the number of drawn points in B_k of index at most k is $\lceil r_k \rceil$. Second, the total number of red diamonds on or below the top edge of B_k is $\lfloor r_k \rfloor$.

We have just given two interpretations of rams, but there are two easier ones. For these further interpretations, it is useful to scale rams to

$$(3.6) \qquad \textit{small rams } r_k^* = \frac{(p-1)r_k}{\epsilon p^k} \qquad \text{and } \textit{tiny rams } \quad r_k' = \frac{r_k}{\epsilon p^k}.$$

Then

$$(3.7) \qquad r_k^* = m_k - m_{k-1} \qquad \text{and} \quad r_k' = s_k - m_k.$$

Together with the standing convention $s_0 = m_0 = r_0 = 0$, these simple equations give the complete relations between slopes, means, and rams. So the tiny ram r_k' is immediately visible as the vertical width of the kth band.

The set of Herbrand invariants $I = (r_1, \ldots, r_w)_\epsilon^f$ compatible with a given ground field K has an appealing geometric description if one uses small rams. Namely $(r_1^*, \ldots, r_w^*)$ must be in the cube $(0, e_K]^w$, with all r_k geometric if it is in the interior $(0, e_K)^w$. The hook H_j of §2.4 indicates a part of the boundary of $[0, j]^2$. In our Eisenstein diagrams, arithmetic bands, meaning the ones where $r_k^* = (p-1)r_k'$ is an integer, as discussed in §2.4, are marked by a black segment at their right end. Thus the bottom two bands in `3.1.27.99c` are marked, while the top one is not.

3.5. **The Herbrand function and Monge reduction.** Of the four versions (2.2)-(2.5) of totally ramified Herbrand invariants, the only one that is not immediately evident from an Eisenstein diagram is the first one, involving the classical Herbrand function ϕ. To read ϕ off from an Eisenstein diagram, one can think of a particle starting at time $r = 0$ at the point $P_0 = (0, 0)$ and moving up the spiral. The particle starts at a speed of p^w steps per second, where moving from P_σ to $P_{\sigma+1}$ counts as a step. Every time the particle crosses the top edge of a band it decreases its speed by a factor of p. This is a natural definition of speed, because the particle encounters C-points exactly at positive integral times. At any time $r \in \mathbb{R}_{\geq 0}$, the particle has traveled some number of ramps $s \in \mathbb{R}_{\geq 0}$. Then, as in Figure 2.2, $s = \phi(r)$.

The Monge reduction algorithm iteratively simplifies a given Eisenstein polynomial without changing the field it defines. Its general nature can be understood in terms of the moving particle. At the initial D-point a change of variables is made trying to make $f_0 = 1$. At each subsequent C-point P_σ a change of variables is made trying to make $f_\sigma = 0$. These changes to f_σ also change some of the $f_{\sigma'}$ for $\sigma' > \sigma$. When the particle passes out of the drawn window, the complicated process can be stopped. Instead one can just turn all the f_σ with $\sigma > es_w$ to 0, as this change does not affect the field defined, by an effective version of Krasner's Lemma.

The reduction process is completely successful at negligible points but only partially successful at critical points. If one simply does not make the coordinate change at critical points, then one gets a surjection from the infinite set $\text{Eisen}(L/K)$ to the $(q-1)^\delta q^\gamma$-element set $\text{Eis}(L/K)$. If one makes the coordinate changes at

the critical points as well, then the ambiguity from a critical D-point reduces from $q - 1$ to $\gcd(q - 1, \epsilon)$, and the ambiguity from a critical C-point at the top of ρ bands reduces from q to at most $\gcd(q, p^\rho)$. Multiplying these bounds together gives an ambiguity constant $\mathrm{Amb}(I/K)$. It depends on K only through q and is a divisor of the integer $\mathrm{Amb}(I)$ introduced in §2.3. The full reduction algorithm gives a surjection from $\mathrm{Eisen}(L/K)$ to a subset of $\mathrm{Eis}(L/K)$ of size a divisor of $\mathrm{Amb}(I/K)/|\mathrm{Aut}(L/K)|$. The sequel [GRJK$^+$] implements the full algorithm, and moreover deterministically chooses a distinguished polynomial from the set of outputs.

4. Sample families

This section is aimed at facilitating the reader's exploration of the database. It summarizes the internal structure of several families, emphasizing topics which support the more theoretical discussions of the next section.

4.1. **Partitions of the introductory family** $[\frac{1}{2}, \frac{3}{2}]/\mathbb{Q}_3$. All absolute families are naturally partitioned in two related ways, into subfamilies and into packets. The subfamilies are determined by using the coefficients corresponding to points at the bottoms of bands; these are d_0, the a_σ, and sometimes also some b_σ, as discussed in [GRJK$^+$] in the context of residual polynomials. Our naming convention for fields incorporates subfamilies, because subfamilies are both elementary and important.

a_3	a_{10}	b_{11}	b_{13}	HSC	G	a_3	a_{10}	b_{11}	b_{13}	HSC	G
1	1	1	0	$[\ ]_2$	$9T5$	2	1	2	2	$[\ ]_2$	$9T3$
1	1	$0, 2$	$0, 1, 2$	$[1]_2$	$9T10$	2	1	2	$0, 1$	$[\ ]_2^3$	$9T10$
1	1	1	$1, 2$	$[\ ]_2^3$	$9T11$	2	1	0	$0, 1, 2$	$[1]_2$	$9T10$
1	2	1	$0, 1, 2$	$[1]_2^2$	$9T18$	2	1	1	$0, 1, 2$	$[1]_2$	$9T11$
1	2	2	$0, 1, 2$	$[\frac{1}{2}, \frac{2}{3}]_2^2$	$9T24$	2	2	1	$0, 1, 2$	$[\ ]_2^2$	$9T8$
1	2	0	$0, 1, 2$	$[\frac{1}{2}, 1]_2^2$	$9T24$	2	2	$0, 2$	$0, 1, 2$	$[\frac{1}{2}, 1]_2^2$	$9T24$

TABLE 4.1. Partitions of the introductory family $[\frac{1}{2}, \frac{3}{2}]/\mathbb{Q}_3 =$ 3.1.9.18b into four subfamilies and ten packets.

Giving a name to a concept introduced in §1.2, we say that two fields are in the same *packet* if they have the same Galois group G and the same hidden slope content HSC. The database has (G, HSC) for all its fields in degree ≤ 15. However since G and particularly HSC can be hard to compute in higher degrees, packets are not incorporated into our labeling scheme.

As the sample family of this subsection, we reconsider the family $[\frac{1}{2}, \frac{3}{2}]/\mathbb{Q}_3$ of the introduction. Its generic polynomial from (1.2) is $3 + 9a_{10}x + 9b_{11}x^2 + 3a_3x^3 + 9b_{13}x^4 + x^9$. Table 4.1 breaks the 36 fields into four subfamilies of nine fields each, according to the values of (a_3, a_{10}). The canonical cubic subfield is defined by the Eisenstein polynomial $3 + 3a_3y + y^3$, so the relative families discussed at the end of §1.3 correspond to the left and right halves of Table 4.1. In a more complicated way, the table breaks the family into its ten packets. Thus the packet discussed in §1.2 is given in the second from bottom line in the left half.

4.2. **Easy linear packets in** $[\frac{3}{2}]_5/\mathbb{Q}_3$. The family $[\frac{3}{2}]_5/\mathbb{Q}_3$ with LMFDB label `3.1.15.29a` has a very simple packet structure as follows. The generic polynomial is $3 + 9(b_{16}x + b_{17}x^2 + b_{19}x^4 + b_{20}x^5 + b_{22}x^7) + x^{15}$. Specializing via $b_\sigma \in \{0, 1, 2\}$ gives $3^5 = 243$ polynomials bijectively representing the 243 fields of the family. If the list $(b_{16}, b_{17}, b_{19}, b_{22})$ starts with exactly 0, 1, 2, or 3 zeros, then the hidden slope content is $[j/10, j/10, j/10, j/10]_2^4$ for $j = 13, 11, 7, 1$, and the Galois group is $15T64 = C_3^4 : (S_3 \times F_5)$. If the list is simply $(0, 0, 0, 0)$, then the hidden slope content is $[\ ]_2^4$, and the Galois group is $15T11 = S_3 \times F_5$. The fact that the coordinates b_σ render the packet structure transparent is an example of the "important bonus" mentioned after (1.2).

4.3. **Complicated linear packets in** $[2]_7/\mathbb{Q}_2$. The family $[2]_7/\mathbb{Q}_2$ with LMFDB label `2.1.14.27a` has generic polynomial

$$(2 + 4b_{14} + 8c_{28}) + 4\left(b_{15}x + b_{17}x^3 + b_{19}x^5 + b_{21}x^7 + b_{23}x^9 + b_{25}x^{11} + b_{27}x^{13}\right) + x^{14}.$$

There are sixteen packets (G, HSC), with the hidden slope content HSC always determining the Galois group G. The possibilities for the wild slopes are indexed by the set $\{13, 5, 3, \emptyset\} \times \{11, 9, 1, \emptyset\}$. Here an index j generically contributes $[j/7, j/7, j/7]$ but $\emptyset$ contributes the empty list. Inspecting the database shows that the list of wild slopes does not depend on b_{21} and c_{28}. Table 4.2 shows the dependence on the remaining coefficients. In the displayed vectors, each $\star$, v, or d can be independently 0 or 1, except that the d's must sum to an odd number and the v's to an even number.

	11	9	1	$\emptyset$
13	$(1, 0, \star, \star, \star, \star)$	$(1, 1, 1, \star, \star, \star)$	$(1, 1, 0, d, d, d)$	$(1, 1, 0, v, v, v)$
5	$(0, 1, \star, \star, 0, \star)$	$(0, 0, 1, 1, \star, \star)$	$(0, 0, 0, 1, \star, 1)$	$(0, 0, 0, 1, \star, 0)$
3	$(0, 1, d, 1, d, \star)$	$(0, 0, 1, 0, 0, \star)$	$(0, 0, 0, 0, 1, 1)$	$(0, 0, 0, 0, 1, 0)$
$\emptyset$	$(0, 1, v, 1, v, \star)$	$(0, 0, 1, 0, 0, \star)$	$(0, 0, 0, 0, 0, 1)$	$(0, 0, 0, 0, 0, 0)$

TABLE 4.2. The hidden slope stratification of the family $[2]_7/\mathbb{Q}_2$, with vectors $(b_{15}, b_{17}, b_{19}, b_{23}, b_{25}, b_{27})$ indicating coefficients.

4.4. **Families** $[1, \ldots, 1]/\mathbb{Q}_p$. Families where $\epsilon = 1$ and there is just a single wild slope s repeated w times are easier, because there are no hidden wild slopes and Galois groups can be completely determined as in Theorem 8.2 of [GP12]. The case where $s = 1$ is particularly interesting for several reasons. This subsection focuses on the families $[1, \ldots, 1]/\mathbb{Q}_p$, there being one for each prime power p^w, using the particular family $[1, 1, 1, 1]/\mathbb{Q}_2$ as an example.

The generic polynomial for the 2-adic Herbrand invariant $[1, 1, 1, 1]$ is

$$(4.1) \qquad \pi\left((1 + \pi c_{16}) + b_8 x^8 + b_{12}x^{12} + b_{14}x^{14} + a_{15}x^{15}\right) + x^{16}.$$

A field $L/\mathbb{Q}_2$ in $[1, 1, 1, 1]/\mathbb{Q}_2$ has one or two representing polynomials according to whether $b_8 + b_{12} + b_{14}$ is even or odd. In the latter case, the two polynomials differ only in the coefficient c_{16}. The polynomial with $c_{16} = 0$ is our choice of distinguished polynomial. Table 4.3 presents information directly available on the family page for $[1, 1, 1, 1]/\mathbb{Q}_2$, in a form slightly modified to support the discussion here. In the first column, ℓ indexes the subfamily and i indexes the field within

$\ell.i$	b_8	b_{12}	b_{14}	c_{16}	Associated polynomial	a	u	$[j_0,\ j_1,\ j_2,\ j_3,\ j_4]$
1.1	0	0	0	0	$(y+1)^4$	2	4	$[1,\ 3,\ 7,\ 15,\ 30]$
1.2	0	0	0	1	$(y+1)^4$	2	4	$[1,\ 3,\ 7,\ 15,\ 32]$
2.1	0	0	1	0	y^4+y+1	1	15	$[1,\ 3,\ 7,\ 14,\ 31]$
3.1	0	1	0	0	$\left(y^2+y+1\right)^2$	1	6	$[1,\ 3,\ 6,\ 12,\ 31]$
4.1	0	1	1	0	$(y+1)\left(y^3+y^2+1\right)$	2	7	$[1,\ 3,\ 6,\ 15,\ 30]$
4.2	0	1	1	1	$(y+1)\left(y^3+y^2+1\right)$	2	7	$[1,\ 3,\ 6,\ 15,\ 32]$
5.1	1	0	0	0	y^4+y^3+1	1	15	$[1,\ 2,\ 4,\ 8,\ 31]$
6.1	1	0	1	0	$(y+1)^2\left(y^2+y+1\right)$	2	6	$[1,\ 2,\ 4,\ 15,\ 30]$
6.2	1	0	1	1	$(y+1)^2\left(y^2+y+1\right)$	2	6	$[1,\ 2,\ 4,\ 15,\ 32]$
7.1	1	1	0	0	$(y+1)\left(y^3+y+1\right)$	2	7	$[1,\ 2,\ 7,\ 15,\ 30]$
7.2	1	1	0	1	$(y+1)\left(y^3+y+1\right)$	2	7	$[1,\ 2,\ 7,\ 15,\ 32]$
8.1	1	1	1	0	$y^4+y^3+y^2+y+1$	1	5	$[1,\ 2,\ 7,\ 14,\ 31]$

TABLE 4.3. Information on the 12 fields `2.1.16.30a`$\ell.i$ in the family `2.1.16.30a`

the subfamily. The jump sets $[j_0, j_1, j_2, j_3, j_4]$ are discussed in general in §5.2. Commonly, a family gives rise to just a very few jump sets, often just one. This family, and conjecturally all the $[1, \ldots, 1]/\mathbb{Q}_2$, have the unusual feature that the jump set determines the field.

The general case $[1, \ldots, 1]/\mathbb{Q}_p$ has a generic polynomial of a form similar to (4.1). Write $v_w = a_{p^w-1}$ and $v_j = b_{p^w-p^{w-j}}$ for $j = 1, \ldots, w-1$. Then the parameters in the generic polynomial are $v_1, \ldots, v_w$ and also c_{p^w}. Let $L/\mathbb{Q}_p$ be the field defined by the parameters $(v_1, \ldots, v_w; c_{p^w})$. Let g be an element of $GL_w(\mathbb{F}_p)$ with characteristic polynomial

$$(4.2) \qquad f(y) = y^w + \sum_{j=0}^{w-1} v_{w-j} y^j.$$

Then the Galois group of $L^{\mathrm{gal}}/\mathbb{Q}_p$ is the semidirect product $\mathbb{F}_p^w \rtimes \langle g \rangle$ [GP12, Theorem 8.2]. Here the wild inertial group is $\mathbb{F}_p^w$, the tame quotient of inertia has order one, and the unramified quotient is $\langle g \rangle$. Thus the hidden slope content is simply $[\ ]^u$, where u is the order of g. For the case $p^w = 2^4$, Table 4.3 gives these polynomials in factored form. The residual polynomials given in the database can be obtained from $f(y)$ by replacing each y^i with z^{2^i} and dividing by z. The database gives the Galois groups in the usual way, from the smallest group $16T166 = \mathbb{F}_2^4 \rtimes C_4 = C_2 \wr C_4$ to the largest group $16T447 = \mathbb{F}_2^4 \rtimes C_{15} = F_{16}$.

The various phenomena discussed in the example of 2^4 generalize to p^w. A field $L/\mathbb{Q}_p$ has either one or p representing polynomials according to whether $f(1)$ is different from or equal to zero in $\mathbb{F}_p$. In the latter case, the polynomials again differ only in the coefficient c_{p^w} and again $c_{p^w} = 0$ gives our choice of distinguished polynomial. So, as illustrated on the table for 2^4, the automorphism number $a = |\mathrm{Aut}(L/\mathbb{Q}_p)|$ is p if $f(y)$ has a factor $(y-1)$ and 1 otherwise. Going further, the subfields of $L/\mathbb{Q}_p$ are in natural bijection with the factors of $f(y)$ in $\mathbb{F}_p[y]$, with

the field coming from a degree k factor having degree p^k. So there are all together $\prod(m_j + 1)$ subfields, where $\prod_j f_j(y)^{m_j}$ is the factorization of $f(y)$ into irreducibles.

5. THEORETICAL CONNECTIONS

Consider finite extensions K of $\mathbb{Q}_p$ inside of a fixed algebraic closure $\overline{\mathbb{Q}}_p$. A natural goal, which seems a long way off or perhaps not obtainable at all, is to find a group-theoretical description of each absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ together with its descending filtration by the higher ramification groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)^s$. There are however many deep theorems towards this goal. In this section, we describe ways in which the database interacts with these theorems, rendering them more explicit.

5.1. **Extensions with a given Galois group.** An overview of many powerful and explicit results on absolute Galois groups is given in [NSW08, VII§5]. Highlights are as follows. Let K^{nil} be the maximal extension of K which for which the Galois group is a pro-p-group; here nil stands for nilpotent. Shafarevich proved in the 1940s that $\mathrm{Gal}(K^{\mathrm{nil}}/K)$ is free on $[K : \mathbb{Q}_p] + 1$ generators if K does not contain p^{th} roots of unity. Demushkin proved in the 1950s that it can always be presented with $[K : \mathbb{Q}_p] + 2$ generators and one explicit relation, with an example being

$$(5.1) \qquad \mathrm{Gal}(\mathbb{Q}_2^{\mathrm{nil}}/\mathbb{Q}_2) = \langle x, y, z | x^2 y^4 x^{-1} y^{-1} xy \rangle.$$

In the 1980s, Jannsen and Wingberg gave a complete description of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ for p odd, and then Diekert did the same for $p = 2$, assuming K contains fourth roots of unity. All these results are silent on the ramification filtration.

For a finite group G, let G/K be the set of Galois extensions L^{gal}/K in $\overline{\mathbb{Q}}_p/K$ with $\mathrm{Gal}(L^{\mathrm{gal}}/K) \cong G$. These presentations let one compute cardinalities $|G/K|$. Many completely explicit examples are given in [Roe19, §4] for $K = \mathbb{Q}_p$. For example, let P_8 be the Sylow 2-subgroup of S_8. Then from (5.1) one eventually gets $|P_8/\mathbb{Q}_2| = 48$. Switching language to our context of general extensions, let nTj/K be the set of isomorphism classes of degree n extensions L/K with $\mathrm{Gal}(L^{\mathrm{gal}}/K) = nTj$. Then one can multiply by a constant associated to nTj to get the cardinality $|nTj/K|$. For example, over any field, each P_8 Galois extension comes from eight isomorphism classes of abstract $8T35$ extensions, and so $|8T35/\mathbb{Q}_2| = 8 \cdot 48 = 384$.

The database lets one search by Galois group and see ramification behavior not covered by the theorems. Continuing the example of $8T35/\mathbb{Q}_2$, the database shows that they are distributed among eight families $2.1.8.C$ as summarized in Table 5.1. The table gives some indication of the nature of each of the families, including its total mass M and the mass m coming from $8T35$ fields. Each $8T35$ field has mass $\frac{1}{2}$ and the sum 192 of the m is indeed $384/2$. The part of the family consisting of $8T35$ fields is always easy to describe. For example, it is the locus where the coefficient $b_4 = 0$ in the first-listed family $21a$. When the number P of packets is at most 3, the remaining mass is evenly split among the remaining possible groups $8Tj$.

In general, the organization of p-adic fields into families provides a framework for further investigation into ramification. There are many resolvent maps $n'Tj'/K \to nTj/K$ coming from Galois theory over arbitrary fields. The coordinates D_0, a_σ, b_σ, and c_σ can be used to describe these maps in a concise and uniform way. Returning to the example, consider an $8T35$ extension $L = K[x]/f(x)$. If $f(x)$ is generically chosen then the degree twenty-eight resolvent corresponding to the

C	M	s_1	s_2	s_3	m	Hidden slopes			P	Other $8Tj$	
21a	32	1	1	2.75	16	2	2.5	2.5	2	$8T38$	
24d	16	1	2.5	2.75	16	1	2	2.5	1		
25b	32	1	2	3.25	16	1	2.5	3	3	$8T21$	$8T31$
26b	32	1	2.5	3.25	16	1	2	3	3	$8T19$	$8T29$
27a	64	1	2.5	3.5	32	1	2	2.5 or 3	7	(five groups)	
29a	64	2	2.5	3.75	32	1	3	3.25	3	$8T28$	$8T30$
30a	64	2	3	3.75	32	1	2.5	3.25	3	$8T27$	$8T30$
31a	128	2	3	4	32	1	2.5	3.25	14	(ten groups)	
					192						

TABLE 5.1. The distribution of the 384 octic extensions of $\mathbb{Q}_2$ with associated Galois group $8T35$ into eight families $2.1.8.C$

subgroup $S_6 \times S_2$ of S_8 factors into irreducibles as $f_4(x)f_8(x)f_{16}(x)$. The extension $L' = K[x]/f_8(x)$ is one of L's seven different siblings, the others then being easily obtainable either by a degree 35 resolvent construction or by certain quadratic twists [JR08, Figure 3.1]. The horizontal lines in Table 5.1 indicate that for $K = \mathbb{Q}_2$ one has family interchanges $21a \leftrightarrow 24d$, $25b \leftrightarrow 26b$ and $29a \leftrightarrow 30a$ under this operation $L \leftrightarrow L'$. Note that the set of six wild slopes is preserved in each of the three family interchanges as it must be. The $8T35$ parts of the families $27a$ and $31a$ are closed under operation $L \leftrightarrow L'$.

5.2. **Making cyclic cases explicit via jump sets.** The natural goal of identifying the filtered group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ was reached nearly a century ago at the much simpler level of understanding the filtered abelianization $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Namely local class field theory identifies $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the profinite completion of the multiplicative group $K^\times$ with the inertia group being sent to the unit group $U = \mathcal{O}^\times$. For j a positive integer and $s \in (j, j+1]$, the group $\mathrm{Gal}(K^{\mathrm{ab}}/K)^s$ is sent to the j-unit group $U_j = 1 + \Pi^j$.

However this theoretically ideal solution does not immediately answer some very basic concrete questions. One such question is, *what is the set $C_w(K)$ of Herbrand invariants $[s_1, \ldots, s_w]$ coming from cyclic extensions of K of degree p^w?* In other words, for what families $[s_1, \ldots, s_w]/K$ is $(G, HSC) = (C_{p^w}, [\,])$ one of the packets. One certainly needs the s_k to form a strictly increasing sequence of positive integers. But to go beyond this statement, one needs to understand the filtered group U_1.

Suppose the p-primary torsion in U_1 has order p^v. Then U_1 is isomorphic to $(\mathbb{Z}/p^v) \times \mathbb{Z}_p^{n_K}$. Thus the free vs. one-relator distinction from the beginning of §5.1 is visible at this abelian level. In the free case $v = 0$, the set $C_w(K)$ depends only on e_K and is given below. In the one-relator case $v \geq 1$, the situation is much more complicated and $C_w(K)$ depends on an invariant j_K extracted from the abelianization of the relation given in (5.2) below. The database tabulates j_K, with instances having been given in Table 4.3.

The description of $C_w(K)$ involves combinatorial notions, as follows. For a prime p and and a positive integer e, define $\rho_{p,e} : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ by $\rho_{p,e}(i) = \min(pi, i + e)$. Table 5.2 draws $\rho_{p,e}$ in three cases by organizing $\mathbb{Z}_{\geq 1}$ into e columns. Always $\rho_{p,e}(i)$ is the number immediately above i in its column. Let $T_{p,e}$ be the set of non-images of $\rho_{p,e}$, thus the e numbers underlined and in bold at the bottom of

columns. A *jump set* of length w is a sequence $[s_1, \ldots, s_w]$ satisfying the initial condition $s_1 \in T_{p,e}$ and an inductive condition. The inductive condition requires that for $k \geq 2$ one has $s_k \geq \rho_{p,e}(s_{k-1})$, with $s_k \in T_{p,e}$ if strict inequality holds. Let $J_w(p, e)$ be the set of jump sets of length w. If $p - 1$ divides e there is also a notion of *extended jump set*. Here $T_{p,e}$ is simply replaced by $T^*_{p,e} = T_{p,e} \cup \{pe/(p-1)\}$, the extra point being indicated by bold italic in Table 5.2.

The set $J_w(p, e)$ of jump sets and the set $J^*_w(p, e)$ of extended jump sets can be understood as the set of ways of climbing a "rock wall." There are choices at the very beginning, but as soon as one reaches $e_K/(p-1)$, marked by a light band in the table, the rest of the climbing path is forced to be vertical. The diagram splits into a part beneath $e_K p/(p-1)$, marked by a dark band, and the part on or above $e_K p/(p-1)$. We call the lower part *geometric*, because it agrees with the case (p, ∞) corresponding to $\mathbb{F}_q((t))$, and the upper part *arithmetic*. Table 5.2 also gives some sample counts, for $w = 1, 2, 3, \ldots$. The count for the last printed w also holds for all subsequent w.

$(p, e) = (3, 6)$ $(p, e) = (2, 8)$ $(p, e) = (3, 9)$

$|J_w(3, 6)| = 6, 12$ $|J_w(2, 8)| = 8, 24, 42, 53$ $|J_w(3, 9)| = 9, 22, 26$

$|J^*_w(3, 6)| = 7, 15$ $|J^*_w(2, 8)| = 9, 23, 53, 69$

TABLE 5.2.   Arrangements of the positive integers into e columns for understanding jump sets. Bands are actually just convenient thickenings of the lines at heights $e_K/(p-1)$ and $e_K p/(p-1)$, and they are drawn as lines when these heights are not integral.

The desired identification for $v = 0$ is $C_w(K) = J_w(p, e_K)$. As a trivial example, for $p > 2$ one has the familiar $C_w(\mathbb{Q}_p) = J_w(p, 1) = \{[1, \ldots, w]\}$. A partial answer for $v \geq 1$ is that $C_w(K) \subseteq J^*_w(p, e_K)$. As a simple example, $J^*_w(\mathbb{Q}_2) = \{[1, 2, \ldots, w], [2, 3, \ldots, w+1]\}$. While $C_1(\mathbb{Q}_2) = \{[1], [2]\}$ is all of $J^*_1(\mathbb{Q}_2)$, otherwise $C_w(\mathbb{Q}_2) = \{[2, 3, \ldots, w+1]\}$.

In the $v \geq 1$ case where K contains a primitive p^{th} root of unity ζ_p, the next step towards a complete answer goes as follows. Building on Hasse [Has02, Ch. 15], Miki [Mik81, Lem 17] showed that one can write

$$(5.2) \qquad \zeta_p = \alpha_0^{p^w} \alpha_1^{p^{w-1}} \ldots \alpha_{w-1}^p \alpha_w$$

with each α_i satisfying one of the following conditions:

- $v_K(\alpha_i) < pe_K/(p-1)$ and $p \nmid v_K(\alpha_i)$,
- $v_K(\alpha_i) = pe_K/(p-1)$ and α_i is not a pth power,
- $\alpha_i = 1$.

Pagano [Pag22, §1.2] defined the extended jump set associated to K by setting $j_i = v_K(\alpha_i - 1)$ for all $0 \le i \le w$ such that $\alpha_i \neq 1$; these values are independent of the choice of $\alpha_0, \alpha_1, \ldots, \alpha_w$. Undefined values in the sequence $j = [j_0, j_1, \ldots, j_w]$ are filled in using the recursion $j_{i+1} = \rho_{p,e_K}(j_i)$. The remaining steps are to use u_K to identify $C_w(K)$ as a subset of $J_w^*(p, e_K)$. This is difficult to make explicit in general, but Pagano works out many special cases.

Pagano [Pag22, Thm. 1.11] also gave a formula for j_K in terms of a defining Eisenstein polynomial for certain cases where $p \neq 2$ and all slopes of K are less than one. The tabulation of invariants in the database using the factorization of ζ_p suggests that j_K might always be directly expressible in terms of Eisenstein polynomials. For the case $[1, \ldots, 1]/\mathbb{Q}_2$ recall from §4.4 that the generic polynomial is written

$$2((1 + 2c_{2^w}) + v_1 x^{2^w - 2^{w-1}} + \cdots + v_{w-1} x^{2^w - 2^1} + v_w x^{2^w - 2^0}) + x^{2^w},$$

with $v_w = 1$. For $0 \le k \le w$ set $V_k = \sum_{i=1}^k v_i \in \mathbb{F}_2$. Then we expect

$$j_k = \begin{cases} 2^{k+1} - 1 & \text{if } V_k = 0, \\ 2j_{k-1} & \text{if } V_k = 1 \text{ and } k < w, \\ 2^{w+1} + 2c_{2^w} - 2 & \text{if } V_k = 1 \text{ and } k = w. \end{cases}$$

We also observe the simple statement that $j_K = [j_i]$ with $j_i = \epsilon(p^i - p + 1)/(p-1)$ when all slopes are greater than 1. For the case $(\epsilon, p) = (1, 2)$ this formula gives $j_i = 2^i - 1$. In particular, if $w = 4$ then the jump set is $[1, 3, 7, 15, 31]$.

5.3. Nonabelian quotients with known filtrations.

The complications resolved by jump sets in the previous subsection only became serious for $w \ge 2$. Applying the easy special case of $w = 1$ to tame extensions K' of a fixed field K gives a large class of extensions of K which are nonabelian and wild, but still very well understood. This situation has been studied from the point of view of primitive extensions of K by Del Corso, Dvornicich, and Monge in [DCDM17].

To briefly summarize [DCDM17] with some more specificity about slopes, let $K^{\mathrm{prim}} \subset \overline{\mathbb{Q}}_p$ be the composita of all primitive extensions of K. It contains the maximal tame extension K^{tame} of K. What makes the group $\mathrm{Gal}(K^{\mathrm{prim}}/K)$ tractable is that its wild inertia subgroup $\mathrm{Gal}(K^{\mathrm{prim}}/K^{\mathrm{tame}})$ has exponent p. The wild slopes are exactly the positive rational numbers less than $e_K p/(p-1)$ with numerator and denominator prime to p, and then $e_K p/(p-1)$ itself. The former occur with infinite multiplicity but the latter occurs just with multiplicity 1. The quotient $\mathrm{Gal}(K^{\mathrm{tame}}/K)$ is the closure of a subgroup $\langle \tau, \sigma | \sigma \tau \sigma^{-1} = \tau^q \rangle$, where τ generates tame inertia and σ is a Frobenius element. The full group is a semidirect product $\mathrm{Gal}(K^{\mathrm{prim}}/K^{\mathrm{tame}}) \rtimes \mathrm{Gal}(K^{\mathrm{tame}}/K)$ with a known action.

Consider now families $I = [s, \ldots, s]_\epsilon^f/K$ with just one visible wild slope, such as $[\frac{3}{2}]_5/\mathbb{Q}_3$, $[2]_7/\mathbb{Q}_2$, and $[1, \ldots, 1]/\mathbb{Q}_p$ of §4.2, §4.3 and §4.4, respectively. The joint splitting field $K^I \subset K^{\mathrm{prim}}$ of all the fields L/K in I/K is governed by the group theory just summarized. So the packets (G, HSC) that can occur can be group-theoretically calculated.

As an example of how group theory can explain otherwise mysterious patterns, consider the orbits of multiplication by p on $\mathbb{Z}/(p^\rho-1)\mathbb{Z}$, with representatives taken in $[\frac{p^\rho-1}{p-1}, \frac{p(p^\rho-1)}{p-1})$. In the case of $p^\rho = 2^3$, two orbits are $\{8, 9, 11\}$, and $\{10, 12, 13\}$. Corresponding to dropping to the bottom of a column in a $(p, p^\rho - 1)$ table like Table 5.2, remove all factors of p. The orbits in the example then become $\{1, 9, 11\}$, and $\{3, 5, 13\}$. The two triples contain the numbers in the previously mysterious borders of Table 4.2, where one has to divide by 7 to get the hidden slopes for $[2]_7/\mathbb{Q}_2$. The general recipe involves dividing by $p^\rho - 1$ at the end. In the example of $[\frac{3}{2}]_5/\mathbb{Q}_3$ from §4.2, $p^r = 3^4$ and the orbit $\{56, 88, 104, 72\}$ becomes, via the drop $72 = 2^3 3^2 \to 8$, the hidden slopes $\frac{7}{10}$, $\frac{11}{10}$, $\frac{13}{10}$, and $\frac{1}{10}$ mysteriously appearing there. In general, the relatively elementary nature of $\mathrm{Gal}(K^{\mathrm{prim}}/K)$ makes us hopeful that the explicit description of packets in the families of §4.2, §4.3, and §4.4 will ultimately be specializations of the same uniform description for any $[s, \ldots, s]_\epsilon^f$.

As a second example of a nonabelian quotient with a known filtration, consider the group $\mathrm{Gal}(K^{\mathrm{nil}}/K)$ defined just before (5.1) and let $\mathrm{Gal}(K^{\mathrm{nil},p}/K)$ be its maximal quotient of nilpotency class $p-1$ and exponent p. In the strongest result of its type, Abrashkin [Abr17] has identified the filtration on $\mathrm{Gal}(K^{\mathrm{nil},p}/K)$ under the assumption that K contains a primitive pth root of unity. For $p \geq 3$, Abrashkin's result, when it applies, goes well past the local class field theory of the previous subsection. However it leaves a lot of cases uncovered, as for example the Sylow p-subgroup of S_{p^2} already has nilpotency class p. Thus for most of the families in the database, there is not yet a theoretical description of packets, even in principle.

5.4. **Comparing families I/K for varying K.** For s a real number and K a finite degree subfield of $\overline{\mathbb{Q}}_p$, let $K^s \subset \overline{\mathbb{Q}}_p$ be the union of subextensions L/K with all relative slopes less than s. Say that two such fields K and K' are j-close if there is an isomorphism of finite rings $\mathcal{O}_K/\Pi_K^j \to \mathcal{O}_{K'}/\Pi_{K'}^j$. As an example, take K' to have the same residual cardinality q as K, and with ramification index at least e_K. Then K and K' are e_K-close, because both finite rings are isomorphic to $\mathbb{F}_q[t]/t^{e_K}$. Deligne proved in [Del84, Th. 2.8] that if K and K' are j-close then $\mathrm{Gal}(K^s/K)$ and $\mathrm{Gal}(K'^s/K')$ are isomorphic as filtered groups. Thus many instances of the problem of describing filtered Galois groups have the same answer, even if we do not as yet know the answer.

To get a particular isomorphism between the Galois groups, well-defined up to conjugation, one needs to choose a particular isomorphism between the finite rings. Suppose the choices of uniformizers and residue representatives made in §3.1 are compatible with this ring isomorphism. Then the extensions L/K and L'/K' given by the same specialization of the generic polynomial correspond. While Deligne's proof is complicated, he presents its basic idea in [Del84, §1.3] as being this correspondence of Eisenstein polynomials. In terms of the database, the relative parts of the family pages for I/K and I/K' look extremely similar, for any I with top slope less than j.

As one of the simplest possible examples, consider the Herbrand invariant $I = [\frac{1}{3}, \frac{1}{3}]$ over 2-adic fields. Its generic polynomial is $\pi + \pi a_1 x + x^4$. Restricting attention to K with residual cardinality 2, there is just one field L/K in the family I/K, the one obtained by setting $a_1 = 1$. For $\mathbb{Q}_2$, the field $L_0 = \mathbb{Q}_2[x]/(2 + 2x + x^4)$ has associated Galois group S_4 with hidden slope content $[\ ]_3^2$. So for any K, the relative Galois group is likewise S_4 and the relative hidden slope content is likewise

$[\ ]_3^2$. When one passes to absolute invariants, one naturally gets strong dependence on K. For example, taking K to be one of the six ramified extensions of $\mathbb{Q}_2$ yields trivial behavior: L is the compositum $K \otimes L_0$ with Herbrand invariant $[\frac{1}{3}, \frac{1}{3}, s]$, Galois group $S_4 \times C_2$, and hidden slope content $[\ ]_3^2$. Here $s \in \{1, 2\}$ comes from the Herbrand invariant $[s]$ of $K/\mathbb{Q}_2$. The unique ramified cubic extension $K = \mathbb{Q}_2[x]/(2 - x^3)$ of $\mathbb{Q}_2$ yields completely different behavior. Here the unique field L is 2.1.12.12a1.1 with Galois group $C_2^6.C_9.C_6$ and slope content $[\frac{1}{9}, \frac{1}{9}, \frac{1}{9}, \frac{1}{9}, \frac{1}{9}, \frac{1}{9}]_9^6$.

As a more complicated example, take $I = [\frac{1}{2}, \frac{2}{3}]$ with generic polynomial $\pi(1 + a_3 x^3 + a_5 x^5 + c_6 x^6) + x^9$. The page for 3.1.9.13b $= [\frac{1}{2}, \frac{2}{3}]/\mathbb{Q}_3$ says that there are eight fields, as c_6 is required to be 0 in the parameter list (a_3, a_5, c_6) whenever $a_3 \neq a_5$. The parameters $(1, 2, 0)$ and $(2, 1, 0)$ give fields having the same Galois closure, with Galois group 9T18 and Galois slope content $[\frac{1}{2}, \frac{1}{2}, \frac{2}{3}]_2^2$. The remaining six fields from (a_4, a_4, c_6) all have Galois group 9T20 and Galois slope content $[\frac{1}{2}, \frac{1}{2}, \frac{2}{3}]_2^3$, with the splitting field depending only on a_4. Since all slopes are less than one, Deligne's comparison theorem says that all the facts just summarized also hold over any K with residual cardinality 3. Going further, one can compute via resolvent constructions that the joint splitting field $\mathbb{Q}_3^I$ has $\mathrm{Gal}(\mathbb{Q}_3^I/\mathbb{Q}_3)$ with order $2^4 3^8$ and slope content $[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{5}{9}, \frac{2}{3}, \frac{2}{3}]_2^6$. So any $\mathrm{Gal}(K^I/K)$ has the same structure as a filtered group.

To see §5.2 in the light of the comparison theorem, let $C_w^s(K)$ be the subset of $C_w(K)$ consisting of Herbrand invariants $[s_1, \ldots, s_w]$ with $s_w < s$. Deligne's theorem says that $C_w^s(K) = C_w^s(\mathbb{F}_p((t)))$ holds for $s = e_K$, but in the easy case $v = 0$ the explicit descriptions says it holds for the larger integer $s = pe_K/(p-1)$. It fails for even larger integers s, as one has entered the arithmetic regime. Similarly, consider $I = [s, \ldots, s]_e^f$. Then Deligne's theorem says the filtered group $\mathrm{Gal}(K^I/K)$ is isomorphic with its geometric analog $\mathrm{Gal}(\mathbb{F}_q((t))^I/\mathbb{F}_q((t)))$ if $s < e_K$. The explicit description of $\mathrm{Gal}(K^I/K)$ indicated in §5.3 says that the isomorphism holds for $s < pe_K/(p-1)$.

5.5. **Canonical globalization.** Our complete tabulation of degree sixteen extensions of $\mathbb{Q}_2$ shows that the number of fields with automorphism group of size 1, 2, 4, 8, and 16 is respectively 9080, 833736, 44752, 2292, and 251. These newly-determined numbers sum to the previously known total 890111. The complete tabulation also gives the corresponding counts within each family. For the most ramified family 2.1.16.79a $= [2, 3, 4, 5]$, the numbers are 0, 63488, 968, 240, and 32, for a total of 67728.

The next step in our general approach to populating the database is to determine the Galois group G and the hidden slope content HSC for each field. This is an ongoing process: we have computed almost all the Galois groups using Doris' programs [Dor20], but identifying HSC is harder. We describe here a completed part that is of particular interest in terms of applications to number fields.

For r an odd prime, let $\mathbb{Q}^r \subset \mathbb{C}$ be the union of all finite degree Galois extensions of $\mathbb{Q}$ with Galois group having order a power of 2 and ramification within $\{\infty, 2, r\}$. Then a special case [Koc02, Example 11.18] of theorems of Koch gives two related very strong results on $\mathbb{Q}^r$ for $r \equiv 3, 5$ modulo 8. Let $D_\infty = \{1, c\}$ where c is complex conjugation. Let D_r be the corresponding decomposition group at the prime r, namely $D_r = \langle \tau, \sigma | \sigma \tau \sigma^{-1} = \tau^r \rangle$ understood in the category of pro-2-groups, so that D_r has a semidirect product structure $\mathbb{Z}_2 \rtimes \mathbb{Z}_2$. The first result is that $\mathrm{Gal}(\mathbb{Q}^r/\mathbb{Q})$ is the free product $D_\infty * D_r$ in the category of pro-2-groups. The

second result is that its 2-decomposition subgroup D_2 is the entire global Galois group $\mathrm{Gal}(\mathbb{Q}^r/\mathbb{Q})$.

For $r \equiv 3, 5$ (8) fixed, Koch's result says that an extension $L/\mathbb{Q}_2$ with $G = \mathrm{Gal}(L^{\mathrm{gal}}/\mathbb{Q}_2)$ a 2-group globalizes either 0 or 1 times to a number field with discriminant $\pm 2^a r^b$ and Galois group G. Typically a given field has no globalizations, as the governing local group (5.1) has three generators and one relation, while the governing global group also has three generators, but now has two relations, $c^2 = 1$ and $\sigma \tau \sigma^{-1} = \tau^r$.

For w a positive integer, consider the subfield $\mathbb{Q}^{r,w}$ generated by the subfields of $\mathbb{Q}^r$ of degree dividing 2^w. Its r-decomposition group is a quotient $D_{r,w}$ of D_r having 2^{2w} elements and depending only on $r \bmod 2^w$. So the abstract group $\mathrm{Gal}(\mathbb{Q}^{r,w}/\mathbb{Q}) = D_\infty * D_{r,w}$ depends only on $r \bmod 2^w$. Our calculations here show that the globalizing 2-adic fields for 3 and 19 agree and the globalizing fields for 13 and 29 also agree. This extends an observation made in [JR14, §8] for octic 2-adic fields and we do not have a proof that it holds for all r and w.

Table 5.3 illustrates the frequency of globalization. It counts the fields that globalize exactly for the extra prime r being in the indicated subset R of $\{3, 5, 11, 13\}$. There are 1131 2-adic fields that globalize to fields with discriminant $\pm 2^a$, of which 274 have $a = 79$. So the bottom right entries, corresponding to $R = \{3, 5, 11, 13\}$, include many more always-globalizing fields.

	All 677795 fields					Fields in $[2, 3, 4, 5]/\mathbb{Q}_2$			
	$\emptyset$	$\{3\}$	$\{11\}$	$\{3, 11\}$		$\emptyset$	$\{3\}$	$\{11\}$	$\{3, 11\}$
$\emptyset$	505520	9952	9952	61158	$\emptyset$	50614	1888	1888	8734
$\{5\}$	15072	0	0	0	$\{5\}$	256	0	0	0
$\{13\}$	15072	0	0	0	$\{13\}$	256	0	0	0
$\{5, 13\}$	58076	0	0	2993	$\{5, 13\}$	3384	0	0	708

TABLE 5.3. Statistics of globalization for degree sixteen extensions $L/\mathbb{Q}_2$ with Galois group $\mathrm{Gal}(L^{\mathrm{gal}}/\mathbb{Q}_2)$ having 2-power order.

The purely-local relevance of globalization is that it allows easier mechanical computation of Galois groups and it facilitates the identification of hidden slopes. Both G and HSC are in the database for all the canonically globalizing fields just discussed. Generally speaking, the database is designed so that it can present partial results. As of this writing, the database shows 156 packets inside the family $[2, 3, 4, 5]$. The numbers appearing as hidden wild slopes so far are 2, 3, 3.5, 4, 4.25, 4.5, 4.75, 5.125, 5.25, 5.375, and 5.625.

Let $\mathbb{Q}_2^{\mathrm{nil},w}$ be the subfield of $\mathbb{Q}_2^{\mathrm{nil}}$ generated by subfields of degree 2^w, so that $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{nil},w}/\mathbb{Q}_2)$ is a finite quotient of the infinite group $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{nil}}/\mathbb{Q}_2)$ of (5.1). Write its order as 2^{j_w}. A group-theoretical calculation says that $(j_1, j_2, j_3, j_4) = (3, 8, 25, 204)$. Corresponding numbers for $\mathrm{Gal}(\mathbb{Q}^{r,w}/\mathbb{Q})$ begin independently of r, being $(3, 7, 18)$. For $w = 4$, there is dependence on $r \bmod 8$, with $p = 3$ and 5 yielding 97 and 101.

We have long known the twenty-five slopes appearing in compositum $\mathbb{Q}_2^{\mathrm{nil},3}$ of all nilpotent octic extensions of $\mathbb{Q}_2$. There are three -1's coming from the unramified octic extension of $\mathbb{Q}_2$, which is famously known not to globalize. The wild slopes

are then

$$1,\ 1,\ 1,\ 1\tfrac{1}{2},\ 1\tfrac{1}{2},\ \ 2,\ 2,\ 2,\ 2\tfrac{1}{2},\ 2\tfrac{1}{2},\ 2\tfrac{5}{8},\ 2\tfrac{3}{4},\ \ 3,\ 3,\ 3\tfrac{1}{4},\ 3\tfrac{1}{4},\ 3\tfrac{3}{8},\ 3\tfrac{1}{2},\ 3\tfrac{1}{2},\ 3\tfrac{3}{4},\ 3\tfrac{3}{4},\ \ 4.$$

The eighteen slopes that survive to the quotient group $\mathrm{Gal}(\mathbb{Q}^{r,3}/\mathbb{Q})$ are given for $r = 3, 5$ in [JR14, §8].

The basic reason for constructing a large database is that many concrete facts about ramification are not yet known and seem resistant to theoretical investigation. To underscore that much is not known, we conclude by asking a very concrete question: *what are the* 204 *slopes of* $\mathrm{Gal}(\mathbb{Q}_2^{\mathrm{nil},4}/\mathbb{Q}_2)$*?* Basic theory says that four of them are -1, and the rest are in $[1, 5]$ with all denominators being powers of 2. Analyzing high-degree composita of the new degree sixteen fields in the database will give many of these 204 numbers. We expect that a complete answer to the question may be out of reach without further theoretical advances, but computational progress can be measured by the number of slopes found.

Acknowledgements

References

[ABM+15] Chad Awtrey, Brett Barkley, Nicole E. Miles, Christopher Shill, and Erin Strosnider, *Degree 12 2-adic fields with automorphism group of order 4*, Rocky Mountain J. Math. **45** (2015), no. 6, 1755–1764. MR 3473152

[Abr17] Victor Abrashkin, *Groups of automorphisms of local fields of period p and nilpotent class < p, II*, Internat. J. Math. **28** (2017), no. 10, 1750066, 32. MR 3699165

[Awt12] Chad Awtrey, *Dodecic 3-adic fields*, Int. J. Number Theory **8** (2012), no. 4, 933–944. MR 2926553

[BM83] Gregory Butler and John McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911. MR 695893 (84f:20005)

[CHM98] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8 (electronic).

[DCDM17] Ilaria Del Corso, Roberto Dvornicich, and Maurizio Monge, *On wild extensions of a p-adic field*, J. Number Theory **174** (2017), 322–342. MR 3597393

[Del84] P. Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0, Representations of reductive groups over a local field, Travaux en Cours, Hermann, Paris, 1984, pp. 119–157. MR 771673 (86g:11068)

[Dor20] Christopher Doris, *Computing the Galois group of a polynomial over a p-adic field*, Int. J. Number Theory **16** (2020), no. 8, 1767–1801. MR 4143684

[GP12] Christian Greve and Sebastian Pauli, *Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials*, International Journal of Number Theory **8** (2012), no. 6, 1401–1424. MR 2965757

[GRJK+] Jordi Guàrdia-Rubies, John W. Jones, Kevin Keating, Sebastian Pauli, David P. Roberts, and David Roe, *Pseudo canonical generating polynomials for extensions of local fields*, in preparation.

[Has02] Helmut Hasse, *Number theory*, german ed., Classics in Mathematics, Springer-Verlag, Berlin, 2002, Reprint of the 1980 English edition [Springer, Berlin; MR0562104 (81c:12001b)], Edited and with a preface by Horst Günter Zimmer. MR 1885791

[Hul05] Alexander Hulpke, *Constructing transitive permutation groups*, Journal of Symbolic Computation **39** (2005), no. 1, 1–30.

[JR04] John W. Jones and David P. Roberts, *Nonic 3-adic fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 293–308. MR 2137362 (2006a:11156)

[JR06]   _____, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)

[JR08]   _____, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. MR 2419170 (2009d:11163)

[JR14]   _____, *A database of number fields*, LMS J. Comput. Math. **17** (2014), no. 1, 595–618. MR 3356048

[Koc02]   Helmut Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer. MR 1930372

[Kra37]   Marc Krasner, *Sur la primitivité des corps p-adiques*, Mathematica (Cluj) **13** (1937), 72–191.

[LMFDB]   The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2025, [Online; accessed 17 January 2025].

[Mik81]   Hiroo Miki, *On the ramification numbers of cyclic p-extensions over local fields*, J. Reine Angew. Math. **328** (1981), 99–115. MR 636198

[Mon11]   Maurizio Monge, *Determination of the number of isomorphism classes of extensions of a $\mathfrak{p}$-adic field*, J. Number Theory **131** (2011), no. 8, 1429–1434. MR 2793885

[Mon14]   _____, *A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields*, Int. J. Number Theory **10** (2014), no. 7, 1699–1727. MR 3256847

[NSW08]   Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026

[Pag22]   C. Pagano, *Jump sets in local fields*, J. Algebra **593** (2022), 398–476. MR 4349285

[PS17]   Sebastian Pauli and Brian Sinclair, *Enumerating extensions of (π)-adic fields with given invariants*, Int. J. Number Theory **13** (2017), no. 8, 2007–2038 (English).

[Roe19]   David Roe, *The inverse Galois problem for p-adic fields*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 393–409. MR 3952024

[Sch14]   Peter Scholze, *Perfectoid spaces and their applications*, Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. II, Kyung Moon Sa, Seoul, 2014, pp. 461–486. MR 3728623

[Ser78]   Jean-Pierre Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 22, A1031–A1036. MR 500361 (80a:12018)

[Ser79]   _____, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

Universitat Politècnica de Catalunya
Email address: jordi.guardia-rubies@upc.edu

Arizona State University
Email address: jj@asu.edu

University of Florida
Email address: keating@ufl.edu

University of North Carolina Greensboro
Email address: s_pauli@uncg.edu

University of Minnesota Morris
Email address: roberts@morris.umn.edu

Massachusetts Institute of Technology
Email address: roed@mit.edu