## Towards improving the Database of Local Fields

#### David P. Roberts University of Minnesota, Morris

November 12, 2021

#### Two-paragraph summary

The *p*-adic field section of the LMFDB tabulates degree *n* extensions of  $\mathbb{Q}_p$ , including for all  $n \leq 15$  and  $p \leq 199$ . For example, always up to isomorphism, there are 795 nonic extensions  $K/\mathbb{Q}_3$  and 1823 octic extensions  $K/\mathbb{Q}_2$ . Interesting invariants include visible slopes, hidden slopes, and Galois groups.

The main framework for improvement is to focus first on visible slopes. Here there is a strong general theory valid for general K/F, not just the case  $F = \mathbb{Q}_p$ . It centers on Krasner-Monge near-canonical polynomials for totally ramified extensions K/F. These polynomials let one collect all extensions of a given F with given visible slopes into a single parameterized family, and the dependence on F is mild. The family structure then facilitates the investigation of hidden slopes and Galois groups.

### Overview

- 1. Introduction, including a tour of the database.
- 2. The ramification invariant I of an extension K/F, as captured in the totally wild degree  $p^w$  case by

heights	$\langle h_1,\ldots,h_w\rangle$ ,
slopes	$[s_1,\ldots,s_w]$ ,
or <i>rams</i>	$(r_1,\ldots,r_w).$

- 3. The set  $\ensuremath{\mathcal{I}}$  of possible ramification invariants.
- 4. From ramification invariants to pictures.
- 5. From pictures to near-canonical polynomials.
- 6. Hidden slopes and Galois groups in two sample families.

### 1.1. Notation for classifyng extensions

Let  $n \in \mathbb{Z}_{\geq 1}$  and let F be a field. An important problem is to describe the set F(n) of isomorphism classes of separable field extensions K/F of degree n.

Let G run over conjugacy classes of transitive subgroups of  $S_n$ . Then Galois theory gives a natural decomposition

$$F(n) = \coprod_G F(G).$$

One would like to describe each F(G) individually.

Now let F be a p-adic field, i.e. a finite extension of  $\mathbb{Q}_p$  or  $\mathbb{F}_p((t))$ , with uniformizer  $\pi \in \Pi \subset \mathcal{O} \subset F$  as usual. Then every K/F has a discriminant ideal  $\Pi^c$ , giving

$$F(n) = \coprod_G \coprod_c F(G, c).$$

The sets F(G, c) are finite and one would like to describe them individually.

# 1.2. Overview of the 795 nonic 3-adic fields

There are 81 nonzero  $|\mathbb{Q}_3(G, c)|$  with 22 Galois groups G and 16 discriminant exponents c involved. On the table, groups G are sorted first by the number of cubic subfields:  $\geq 2$ , 1, and then 0. In the third column,  $A = \operatorname{Aut}(K/\mathbb{Q}_3)$  is the centralizer of the Galois group G.

G	G	A	0	9	10	12	13	15	16	18	19	20	21	22	23	24	25	26
9	9 <b>T</b> 2	9				1												
18	9 <i>T</i> 4	3		2		1		6, <i>3</i>	3		9							
18	9 <b>T</b> 5									1								
36	978					1		2		3	3							
9	9T1	9	1			2								9				
18	9T3									1				1				3
27	9T6	3				2								6				
27	9T7	3				1			3									
54	9T10								6	11				8				24
54	9T11					2			1	8				9				
54	9T12	3									9		27					
54	9 <i>T</i> 13			2		1		2		3	3		9					
81	9T17	3				9				9				18				
108	9 <i>T</i> 18						2	4		3	12		18	9				
162	9 <i>T</i> 20	3					6	12		9	45			27			81	
162	9 <i>T</i> 21			_		_						27				27		54
162	9/22			6		3		6	_				9	9	27			
324	9 <i>T</i> 24								6	12	9	27	9		27	27	27	
36	979					1			1	_								
72	9/14				1					3								
72	9 <i>1</i> <sup>-</sup> 16			-	1	-	-			3	-							
144	9 <i>T</i> 19			2		2	2	6	2		6							

Bold=Unramified

Italic=partially ramified

Regular=totally ramified

## 1.3. Tour of the p-adic section of the LMFDB

As said earlier, the LMFDB currently contains the sets  $\mathbb{Q}_p(n)$  for all  $p \leq 199$  and all  $n \leq 15$ , with information on each field K. E.g., the field K labeled 3.9.21.20 is defined by  $x^9 + 12x^6 + 18x^4 + 3$ .

The degree *n* of any field factors as  $utp^w$  with *u* and *t* its unramified and tamely ramified parts. There are *w* wild slopes  $\hat{s}_1 \leq \cdots \leq \hat{s}_w$ , as introduced in the next section. The "slope content" of our example (not directly given in the LMFDB) is  $[\hat{s}_1, \hat{s}_2]_t^u = [2, \frac{17}{6}]_1^1 = [2, \frac{17}{6}]$ .

The LMFDB does however always gives the much-harder-to-calculate slope content of the Galois closure *L*. In our example G = 9T24 has  $324 = 2^23^4$  elements and the slope content of *L* is

$$\left[\frac{3}{2}, 2, \frac{5}{2}, \frac{17}{6}\right]_2^2$$
.

At this level, the wild slopes are breaks in the Artin upper numbering of the ramification filtration on G. They consist of the wild slopes already **visible** in K, and also some more *hidden* slopes.

#### 2.1. The canonical filtration of a p-adic extension

Any  $K/F \in F(n)$  has a canonical filtration obtained by climbing from F to K via suitable minimally ramified subextensions. To focus on the main phenomena, we henceforth restrict to u = t = 1 so  $n = p^w$ .



As we'll see, for any 2-adic field F, the picture arises from many octic extensions K/F, e.g. from 32 in the case  $F = \mathbb{Q}_2$ . The filtration takes the form

$$F = K_0 \subset K_1 \subset K_2 \subset K_3 = K$$

with each  $[K_i : K_{i-1}] = 2$ .



The numerical invariants are captured in three equivalent ways:

We switch to focusing on wild ramification only, writing

$$\operatorname{cond}(K_i/K_j) = c(K_i/K_j) - \operatorname{deg}(K_i/K_j) + 1$$

The definitions are then  $h_i = \text{cond}(K_i/K_0)$  and  $r_i = \text{cond}(K_i/K_{i-1})$ . Accordingly, we also switch from the website's Artin-Fontaine slopes  $\hat{s}_i$  to the Serre-Swan slopes  $s_i$  via  $\hat{s}_i = s_i + 1$ . When the canonical filtration has fewer than w steps we keep a uniform notation that refers to nonexistent fields:



Here the filtration is  $F = K_0 \subset K_1 \subset K_2 \subset K_3 = K$ . The invariants are

$$I = \langle 1, \frac{17}{3}, 15 \rangle = \left[1, \frac{7}{3}, \frac{7}{3}\right] = \left(1, \frac{11}{3}, \frac{11}{3}\right).$$

When  $K_i$  is nonexistent,  $h_i$  is no longer forced to be integral. Similarly too, a ram  $r_j$  repeated  $\rho$  times is now only forced to have a denominator dividing  $P_{\rho}(p) := p^{\rho-1} + p^{\rho-2} + \cdots + p + 1$ .

#### 2.2. Conversion formulas

The three ways of describing a ramification invariant I interrelate via

$$h_{k} \stackrel{2a}{=} \sum_{j=1}^{k} \phi(p^{j}) s_{j}, \qquad h_{k} \stackrel{2b}{=} \sum_{j=1}^{k} p^{k-j} r_{j},$$

$$s_{k} \stackrel{1a}{=} \frac{h_{k} - h_{k-1}}{\phi(p^{k})}, \qquad s_{k} \stackrel{3}{=} \frac{r_{k}}{\phi(p^{k})} + \sum_{j=1}^{k-1} \frac{r_{j}}{p^{j}},$$

$$r_{k} \stackrel{1b}{=} h_{k} - ph_{k-1}, \quad r_{k} \stackrel{4}{=} \phi(p^{k}) s_{k} - \phi(p) \sum_{j=1}^{k-1} \phi(p^{j}) s_{j}.$$

1a captures the definition of slope as rise/run. 1b emphasizes that rams measure how  $K_k$  is more ramified than say the algebra  $K_{k-1}^p$ . 2a and 2b are their inversions, each intuitive in their own right. 3 = 1a  $\circ$  2b and 4 = 1b  $\circ$  2a are less directly intuitive. The set of  $r_1$  arising in one-step degree  $p^{\rho}$  extensions of F is very simple and depends only on the ramification index  $e = \operatorname{ord}_{\Pi}(p)!$ 

In the case of  $e = \infty$ , i.e. function fields, it is

$$\mathcal{R}_{
ho,\infty,
ho}=rac{\mathbb{Z}_{\geq 1}-
ho\mathbb{Z}_{\geq 1}}{P_{
ho}(
ho)}=rac{\mathbb{Z}_{\geq 1}-
ho\mathbb{Z}_{\geq 1}}{
ho^{
ho-1}+
ho^{
ho-2}+\cdots
ho+1}.$$

In the case  $e < \infty$ , i.e. extensions of  $\mathbb{Q}_p$ , it is

$$\mathcal{R}_{p,e,
ho} = (\mathcal{R}_{p,\infty,
ho} \cap (0, pe)) \cup \left\{ egin{array}{c} \{pe\} & ext{if } 
ho = 1, \ \{ \ \} & ext{if } 
ho > 1. \end{array} 
ight.$$

The conversion formulas are trivial in the one-step extension context,  $s_1 = \frac{r_1}{p-1}$  and  $h_\rho = P_\rho(p)r_1$ .

### 3.2. Example: One-step extensions for p = 2

From the previous slide for multiplicities  $\rho = 1$  and  $\rho = 2$ ,

The cutoff for e = 1 is indicated and so the corresponding sets are

$$\begin{array}{rcl} \mathcal{R}_{2,1,1} &=& \{ & 1, & 2 \ \}, \\ \mathcal{R}_{2,1,2} &=& \{ & \frac{1}{3}, & 1, & \frac{5}{3} & \}. \end{array}$$

Over  $\mathbb{Q}_2$ , the quadratic fields for the rams 1 and 2 are respectively  $\mathbb{Q}_2(\sqrt{d})$  for  $d \in \{-1, -1*\}$  and  $d \in \{2, 2*, -2, -2*\}$ , with say \* = 5. The quartic fields appear on the LMFDB as

$(r_1, r_2) = (1/3, 1/3)$	$(r_1, r_2)$	=(1,1)	$(r_1, r_2) = (5/3, 5/3)$
$x^4 + 2x + 2 [4/3, 4/3]_3^2 S_4$	$ x^4 + 2x^3 + 2x^2 $	$^{2}+2$ [2,2] <sup>3</sup> $A_{4}$	$x^4 + 4x^2 + 4x + 2 [8/3, 8/3]_3^2 S_4$
	$x^4 + 2x^3$	$+2 \ [2,2]^2 \ D_4$	$x^4 + 4x^2 + 2 [8/3, 8/3]_3^2 S_4$
	$x^{4} + 2x^{3}$	$+ 6 \ [2,2]^2 \ D_4$	

### 3.3. Occurring invariants *I* in general extensions

Fix a ground field F with  $\operatorname{ord}_{\Pi}(p) = e$  and consider its totally ramified extensions of degree  $p^w$ .

Break up this set of extensions according to their multiplicity vector  $m = (m_1, \ldots, m_k)$ . Let  $M_i = \sum_{j=1}^i m_j$ . Let  $\mathcal{I}_{p,e,m}$  be the set of occurring invariants *I*. Then necessarily  $\mathcal{I}_{p,e,m}$  is in

$$\widehat{\mathcal{I}}_{p,e,m} = \{(\overbrace{r(1),\ldots,r(1)}^{m_1},\ldots,\overbrace{r(k),\ldots,r(k)}^{m_k}): r(i) \in \mathcal{R}_{p,ep^{M_{i-1}},m_i}\}.$$

The index gymnastics hide a simple Cartesian product! E.g.  $\widehat{\mathcal{I}}_{p,e,(3,2)}$  consists of 5-tuples  $(r_1, r_1, r_1, r_4, r_4)$  with  $(r_1, r_4) \in \mathcal{R}_{p,e,3} \times \mathcal{R}_{p,p^3e,2}$ .

The set  $\mathcal{I}_{p,e,m}$  is then the subset of  $\widehat{\mathcal{I}}_{p,e,m}$  such that the list of rams  $r(1), \ldots, r(k)$ , or equivalently the list of slopes  $s(1), \ldots, s(k)$ , is strictly increasing. The elementary nature of  $\mathcal{I}_{p,e,w} = \coprod_m \mathcal{I}_{p,e,m}$  is illustrated by the next slide by  $\mathcal{I}_{3,1,2} = \mathcal{I}_{3,1,(1,1)} \coprod \mathcal{I}_{3,1,(2)}$ .

# 3.4. Invariants for tot. ram. nonic 3-adic fields

rams  $(r_1, r_2)$  and slopes  $[\hat{s}_1, \hat{s}_2]$  with m = (1, 1) before m = (2):

(1,1) (1,2)	(2, 1) (2, 2)	(3,1) (3,2)	(0.25, 0.25) (0.50, 0.50)	[1.5, 1.50] [1.5, 1.66]	[2, 1.83] [2, 2.00]	[2.5, 2.16] [2.5, 2.33]	[1.125, 1.125] [1.250, 1.250]
(1,4) (1,5)	(2,4) (2,5)	(3,4) (3,5)	(1.00, 1.00) (1.25, 1.25)	[1.5, 2.00] [1.5, 1.16]	[2, 2.33] [2, 2.50]	[2.5, 2.66] [2.5, 2.83]	[1.500, 1.500] [1.625, 1.625]
(1,7) (1,8) (1,9)	(2,7) (2,8) (2,9)	(3,7) (3,8) (3,9)	(1.75, 1.75) (2.00, 2.00)	[1.5, 2.50] [1.5, 2.66] [1.5, 2.83]	[2, 2.83] [2, 3.00] [2, 3.16]	[2.5, 3.16] [2.5, 3.33] [2.5, 3.50]	[1.875, 1.875] [2.000, 2.000]
			(2.50, 2.50) (2.75, 2.75)			<u> </u>	[2.250, 2.250] [2.375, 2.375]

The	Cartesian	structure	of	$\widehat{\mathcal{I}}_{3,1,(1)}$	.,1)	is	visi	ble
in rar	ms as <mark>{1</mark>	$,2,3\} imes\{1$	., 2,	4, 5,	7,	8,9]	}, ł	out
obscu	red in slop	es.						

The Cartesian structure on the (1, 1) part is still visible in the total masses to the right, where K/F has mass  $|1/\operatorname{Aut}(K/F)|$ .

			2
4			2
12	12	18	6
12	12	18	2
36	36	54	6
36	36	54	6
54	54	81	
L			6
			6

#### 4.1. From an invariant I to its picture

An invariant I = h = s = r for degree  $p^w$  extensions determines a picture in the window  $[0, p^w] \times [0, \hat{s}_w]$ . For example

 $I = \langle 11, 62, 252 \rangle = [5.5, 8.5, 10.\overline{5}] = (11, 29, 66)$ 

determines



(The points in the *u*-column will give constraints on the coefficient  $t_u$  of the  $x^u$  terms in Eisenstein polynomials.)

Q. Can you guess the recipe for passing from I to the picture?

## 4.2. The recipe for drawing the *I*-picture, part 1



There are *w* closed bands. The top edge of the *i*<sup>th</sup> band  $B_i$  goes from  $(0, \hat{s}_i)$  to  $(p^w, s_j)$ . All drawn points (u, v) are integral and, besides (0, 1) and  $(p^w, 0)$ , occur only in the bands. Write  $u' = u/p^w$ . Then an integral point  $(u, v) \in B_i$  is drawn iff its u' has exact denominator  $p^i$  or it's on the boundary. It is drawn solidly iff the first condition holds. There is always a unique point on the lower edge, drawn as  $\circ$  or  $\bullet$ . There is at most one point on the upper edge, drawn as  $\circ$ .

### 4.3. The recipe for drawing the *I*-picture, part 2

Define the scaled heights and scaled rams via  $h'_i = h_i/p^i$  and  $r'_i = r_i/p$ , and indicate these variants by double delimiters. So the current example becomes



 $I = \langle \langle 3\frac{2}{3}, 6\frac{8}{9}, 9\frac{1}{3} \rangle \rangle = [5.5, 8.5, 10.\overline{5}] = ((3\frac{2}{3}, 9\frac{2}{3}, 22)).$ 

The  $i^{\text{th}} \circ \text{or} \bullet \text{is at } (u'_i, v_i) = (\langle h'_i \rangle, \lceil h'_i \rceil) \text{ so that e.g. the first } \bullet \text{ comes from } 3\frac{2}{3} \text{ and is at } (u'_1, v_1) = (\frac{2}{3}, 4).$  Equivalently, the lower edge of  $B_i$  goes through  $(p^w, h'_i)$ . Also,  $B_i$  contains exactly  $\lfloor r'_i \rfloor \bullet$ 's, and then also a  $\bullet$  iff  $r'_i$  is nonintegral.

### 5.1. The Krasner-Monge parametrized polynomial

Index a point (u, v) by the integer  $j = p^w(v - 1) + u$ , so that the *i*<sup>th</sup> • or  $\circ$  becomes  $j = p^w h'_i$ . Introduce variables  $a_j$ ,  $b_j$  and  $c_j$  for drawn points in bands of the form •, •, and •. Form the polynomial

$$\pi + \sum_{(u,v) \text{ as } \bullet} a_j \pi^v x^u + \sum_{(u,v) \text{ as } \bullet} b_j \pi^v x^u + \sum_{(u,v) \text{ as } \circ} c_j \pi^v x^u + x^{p^w}$$

Our earlier example  $I = [1, \frac{11}{6}] = ((\frac{2}{3}, 2\frac{1}{3})) = \langle \langle \frac{2}{3}, 1\frac{4}{9} \rangle \rangle$  yields



For  $\pi = 3$ , it's  $(3 + 9c_9) + 9a_{13}x^4 + 9b_{14}x^5 + 3a_6x^6 + 9b_{16}x^7 + x^9$ .

#### Notation for the Krasner-Monge theorem

Let F be a p-adic field with residue field  $\mathbb{F}_q$  with  $q = p^f$ .

For d a divisor of f, the additive map

$$\mathbb{F}_q o \mathbb{F}_q : k \mapsto k^{p^d} - k$$

has kernel  $\mathbb{F}_{p^d}$  and so image  $T_d \subset \mathbb{F}_q$  of index  $p^d$ .

Choose a uniformizer  $\pi$  and a lift  $\kappa \subset \mathcal{O}$  of  $\mathbb{F}_{p^f}$ . Require  $0 \in \kappa$  and write  $\kappa^{\times} = \kappa - \{0\}$ . For each divisor d of f, choose a lift  $\kappa_d \subset \kappa$  of  $\mathbb{F}_q/T_d$ , so that  $|\kappa_d| = p^d$  and  $\kappa_f = \kappa$ . For  $F = \mathbb{Q}_p$ , we always just take  $\pi = p$  and  $\kappa = \{0, 1, \dots, p-1\}$ .

For a ramification invariant I, let

- $\alpha$  be its number of •'s;
- $\beta$  be its number of •'s;.
- γ = ∑<sub>j</sub> gcd(ρ(j), f) where j runs over indices of o's and ρ(j) it
   the number of times the corresponding slope is repeated.

# Krasner-Monge theorem

#### Theorem

Let F be a p-adic field with absolute ramification index  $e \in \mathbb{Z}_{\geq 1}$  and chosen  $\pi$  and  $\kappa_d$  as on the previous slide. Let  $I \in \mathcal{I}_{p,e,w}$  be a possible ramification invariant for degree  $p^w$  extensions of F. Consider the polynomials in the corresponding Krasner-Monge family

$$\pi + \sum_{(u,v) \text{ as } \bullet} a_j \pi^v x^u + \sum_{(u,v) \text{ as } \bullet} b_j \pi^v x^u + \sum_{(u,v) \text{ as } \circ} c_j \pi^v x^u + x^{p^w}$$

with  $a_j \in \kappa^{\times}$ ,  $b_j \in \kappa$ , and  $c_j \in \kappa_{\text{gcd}(\rho(j),f)}$ . Then the corresponding extensions are in F(I), with each K represented  $\frac{p^{\gamma}}{|\text{Aut}(K/F)|}$  times.

#### Corollary

The total number of extensions in F(I) is  $\geq (q-1)^{\alpha}q^{\beta}$ , with equality if  $\gamma = 0$ .

# 6.1 The case $I = [\hat{s}_1, \hat{s}_2] = [2, \frac{17}{6}]$ over $\mathbb{Q}_3$

The database says there are 36 fields falling in four packets of nine. As said before, the family is

 $\begin{aligned} f(a_6, a_{13}, b_{14}, b_{16}, c_9, x) = \\ (3 + 9c_9) + 9a_{13}x^4 + 9b_{14}x^5 + 3a_6x^6 + 9b_{16}x^7 + x^9, \end{aligned}$ 

Since there is just one c and f = 1, the ambiguity parameter is  $\gamma = 1$  and each field K has  $p^{\gamma} = 3$  near-canonical defining polynomials. The ambiguity is easily resolved by setting a parameter to 0 and the packets are cleanly described:

 $f(1, 2, 0, b_{16}, c_9, x)$   $f(1, 1, b_{14}, b_{16}, 0, x)$   $f(2, 2, 0, b_{16}, c_9, x)$  $f(2, 1, b_{14}, b_{16}, 0, x)$  gives 9713 and hidden slopes  $[5/2]_2$ gives 9718 and hidden slopes  $[5/2]_2^2$ gives 9722 and hidden slopes  $[3/2, 5/2]_2$ gives 9724 and hidden slopes  $[3/2, 5/2]_2$ 

# 6.2 The case $I = [\hat{s}_1, \hat{s}_2] = [\frac{5}{2}, \frac{17}{6}]$ over $\mathbb{Q}_3$

The database says that in this case there are 18 fields falling into two packets of nine. The Krasner-Monge family is

$$g(\alpha_{14},\beta_{12},\beta_{16},x) = 3 + 9\beta_{12} + 9\alpha_{14}x^5 + 9\beta_{16}x^7 + x^9$$

Defining polynomials are in this case unique and

$$\begin{array}{l} g(2,\beta_{12},\beta_{16},x) & \text{gives } 9T11 \text{ and hidden slopes } [2]_2\\ g(1,\beta_{12},\beta_{16},x) & \text{gives } 9T18 \text{ and hidden slopes } [2]_2^2 \end{array}$$

In general, resolvent constructions should have nice descriptions via the universal families. For example, 9T13 from the previous slide and 9T11 are the same abstract group. The bijection between

- the nine 9713 fields defined by  $f(1, 2, 0, b_{16}, c_9, x)$  and
- the nine 9711 fields defined by  $g(2, \beta_{12}, \beta_{16}, x)$

is given by  $c_9 = \beta_{12}$  and  $b_{16} = \beta_{16} + 1 - \beta_{12}^2$ .

# 6.3 The case $I = [\hat{s}_1, \hat{s}_2] = [3/2, \frac{8}{3}]$ over $\mathbb{Q}_3$

The database gives five types of fields. The family is

 $f(a_3, a_{11}, b_{13}, b_{14}, c_{15}) =$  $3 + 9x^2 a_{11} + 3x^3 a_3 + 9x^4 b_{13} + 9x^5 b_{14} + 9x^6 c_{15} + x^9$ 

The five types are

Here  $\star$  can be any element of  $\{0, 1, 2\}$  without changing the field. Otherwise, different parameters give different fields.

#### Commented main references

#### Much of this material has origin in:

M. Krasner, Sur la primitivité des corps p-adiques, Mathematica (Cluj) 13 (1937) 72-191.

Krasner's results were modernized in:

P. Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0*, in Representations of Reductive Groups over a Local Field (1984), pp. 119–157.

The original database from which the LMFDB database grew: J. W. Jones and D. P. Roberts, *A database of local fields*, J. Symbolic Comput. 41(1) (2006) 80–97.

A modernization which, like Krasner, emphasizes polynomials: M. Monge, *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.