p-adic fields in the LMFDB

David Roe
with Jordi Guàrdia, John Jones, Kevin Keating,
Sebastian Pauli, and David Roberts

Department of Mathematics
Massachusetts Institute of Technology

Bard 6
November 7, 2025

p-adic fields

Goal

Understand field extensions $L/\mathbb{Q}_p$ of degree n.

Key difference from $L/\mathbb{Q}$, $L/\mathbb{F}_p(t)$ and even $L/\mathbb{F}_p((t))$:
for fixed p and n, only finitely many $L/\mathbb{Q}_p$ (Krasner's lemma).

Concrete problems

1. For a fixed set of invariants, compute a set of polynomials $\varphi(x)$ so that every $L/\mathbb{Q}_p$ arises as $\mathbb{Q}_p[x]/(\varphi)$ for some φ (want small set, allow duplicates).
2. Find a reduction algorithm $\texttt{polred}_p$ so that $\mathbb{Q}_p[x]/(\varphi) \cong \mathbb{Q}_p[x]/(\texttt{polred}_p(\varphi))$ and

$$\texttt{polred}_p(\varphi_1) = \texttt{polred}_p(\varphi_2) \Leftrightarrow \mathbb{Q}_p[x]/(\varphi_1) \cong \mathbb{Q}_p[x]/(\varphi_2).$$

Invariants (degrees of subfields)

- The residue characteristic p and degree n;
- Any extension $L/\mathbb{Q}_p$ can be decomposed $L/L_0/L_{\mathrm{ur}}/\mathbb{Q}_p$, where
  - $L_{\mathrm{ur}}/\mathbb{Q}_p$ is unramified (same image of valuations),
  - L/L_{ur} is totally ramified (same residue field),
  - L_0/L_{ur} is tame (degree prime to p),
  - L/L_0 is wild (degree a power of p).

  Write $f = [L_{\mathrm{ur}} : \mathbb{Q}_p]$ for the *inertia degree*, $e = [L : L_{\mathrm{ur}}]$ for the *ramification index*, $\epsilon = [L_0 : L_{\mathrm{ur}}]$ for the *tame ramification index* and $p^w = [L : L_0]$.

There is a unique unramified extension of each degree.

Tame extensions are $L_{\mathrm{ur}}(\sqrt[\epsilon]{up})$ for some $u \in L_{\mathrm{ur}}^\times$.

Invariants (discriminants)

Write $\mathcal{O}_L$ for the maximal order. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of L into $\overline{\mathbb{Q}_p}$ and $\beta_1, \ldots, \beta_n$ a basis of $\mathcal{O}_L$ as a free $\mathbb{Z}_p$-module.

- The *discriminant* Δ of L is $\det(\sigma_i(\beta_j))_{i,j}^2 \in \mathbb{Z}_p$, well defined up to $(\mathbb{Z}_p^\times)^2$. Write $\Delta = p^c u$ with $u \in \mathbb{Z}_p^\times$; c is called the *discriminant exponent*.
- The *mean* $m \in \mathbb{Q}$ of L is defined by $c = f(e - 1 + em)$.

We have $c = 0$ iff $L/\mathbb{Q}_p$ is unramified; $m \geq 0$ with equality iff $L/\mathbb{Q}_p$ is tame. The possible $m > 0$ are known [4]: need $me \in \mathbb{Z}$ and

$$v_p(e(m - \lfloor m \rfloor)) \leq m \leq v_p(e).$$

Invariants (Galois groups)

- Write L^{gal} for the Galois closure of L, and G for $\mathrm{Gal}(L^{\mathrm{gal}}/\mathbb{Q}_p)$.
- Write u for the inertia degree and t for the tame ramification index of $L^{\mathrm{gal}}/\mathbb{Q}_p$.

Given any defining polynomial φ for L, G naturally acts on the roots of φ in L^{gal}; a different choice of φ will yield an isomorphic G-set. We will also write $G = \mathrm{Gal}(L/\mathbb{Q}_p)$ for G equipped with this permutation representation. Since L is a field, it is transitive (only one orbit), and we will label it using the classification of transitive permutation groups with $n \leq 48$.

Example ($x^4 + 2x^3 + 2x^2 + 2$ over $\mathbb{Q}_2$)

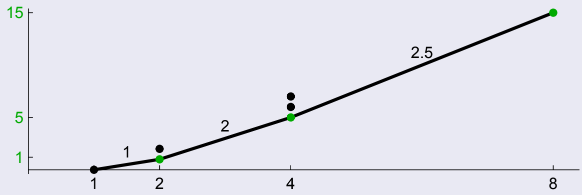
L^{gal} given by $\nu(x)^4 + 2\nu(x)^3 + 2\nu(x)^2 + 2$ where $\nu(x) = x^3 + x + 1$. Have $G \cong A_4$, transitive id 4T4. Field defined by $\nu(x)^2 + (2x + 2)\nu(x) + 2$ has same Galois closure.

Invariants (Swan slopes)

Fix $L/L_{\mathrm{ur}}/\mathbb{Q}_p$, consider $L/L'/L_{\mathrm{ur}}$ with $e' = [L' : L_{\mathrm{ur}}]$ and mean m'. Take the lower convex hull of the points $(e', e'm')$

- The *visible (Swan) slopes* of $L/\mathbb{Q}_p$ are the slopes $[s_1, \ldots, s_w]$ of this function, with multiplicity.
- The *Galois (Swan) slopes* of $L/\mathbb{Q}_p$ are the slopes for $L^{\mathrm{gal}}/\mathbb{Q}_p$, which contain the visible slopes as a sub-multiset.
- The *hidden (Swan) slopes* of $L/\mathbb{Q}_p$ are the complement of the visible slopes within the Galois slopes.

Example ($x^8 + 6x^4 + 1$ over $\mathbb{Q}_2$, with $G \cong D_4$)



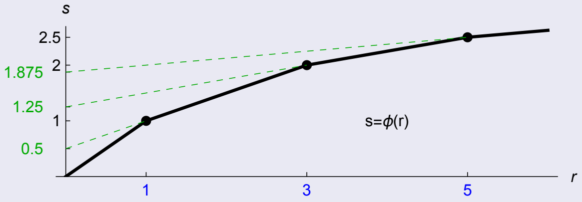
Invariants (means and rams)

Define *means* $m_1, \dots, m_w$ and *rams* $r_1, \dots, r_w$ by

$$m_k = \sum_{j=1}^{k} \frac{p-1}{p^{k+1-j}} s_j \qquad\qquad r_k = \epsilon p^k \frac{m_k - m_{k-1}}{p-1}.$$

Define the *Herbrand function* ϕ to have successive slopes p^{-k}, with breaks at s_k.

Example ($x^8 + 6x^4 + 1$ over $\mathbb{Q}_2$)



Ramification Groups

Classical filtration on G, in terms of uniformer π of L.

- $G_i = \{\sigma \in G : v_K(\sigma(x) - x) \geq i + 1 \forall x \in \mathcal{O}_K\}$ for $i \geq -1$,
- $U_K^{(0)} = \mathcal{O}_K^\times$ and $U_K^{(i)} = 1 + \pi^i \mathcal{O}_K$ for $i \geq 1$.

Proposition ([6, Prop. IV.2.7])

For $i \geq 0$, the map $\theta_i : G_i/G_{i+1} \to U_K^{(i)}/U_K^{(i+1)}$ defined by $\theta_i(\sigma) = \sigma(\pi)/\pi$ is injective and independent of π.

Corollary

- *G/G_0 is cyclic,*
- *G_0/G_1 is cyclic of order prime to p,*
- *G_i/G_{i+1} is an elementary abelian p-group for $i \geq 1$.*

Define upper filtration by $G^{\phi(x)} = G_x$ (better in towers).
We say i is a *break* if $G_i \neq G_{i+1}$, with multiplicity $\log_p \frac{|G_i|}{|G_{i+1}|}$.
Rams are lower breaks, slopes are upper breaks.

Families

Definition

- The *slope content* of $L/\mathbb{Q}_p$ is the symbol $[s_1, \ldots, s_w]_\epsilon^f$.
- We say two fields are in the same *family* if they have the same slope content.

Each family has a *generic polynomial*, and every field in the family arises by specializing the generic polynomial.

We have worked over $\mathbb{Q}_p$, but everything works relatively over an arbitrary p-adic base field.

Demo

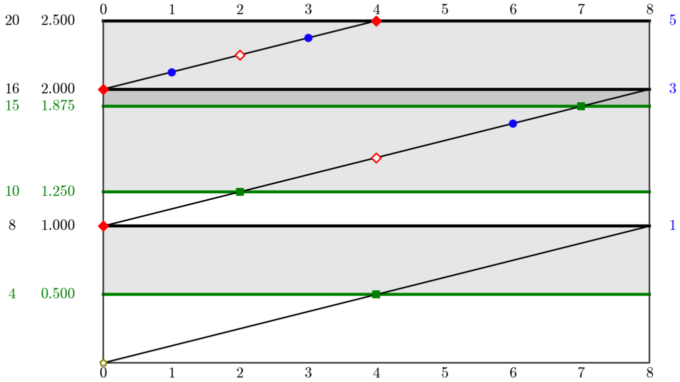
LMFDB!

- Github
- Zulip (email me for an invitation)
- LMFDB Fridays: roughly 8am-11am CST on Zoom.

Eisenstein diagram ($x^8 + 6x^4 + 1$)

$$x^8 + 4a_{15}x^7 + 4b_{14}x^6 + (2a_4 + 8c_{20})x^4 + 8b_{19}x^3 + 4a_{10}x^2 + 8b_{17}x + 4c_8 + 8c_{16} + 2$$

Specialize a_i to $\mathbb{F}_p^\times$, c_i to $\mathbb{F}_p$, b_i to certain subspaces of $\mathbb{F}_p$.



Enumerating families

First consider totally wildly ramified extensions L/K of degree p^ρ with just a single ram r repeated ρ times. The possible r depends only on absolute ramification index e_K.

- Set $\mathcal{R}_\rho^\infty = \{\frac{a}{p^\rho - 1} : a > 0, p \nmid a\}$
- For $\rho > 1$, set $\mathcal{R}_\rho^{e_K} = \{x \in \mathcal{R}_\rho^\infty : x < \frac{pe_K}{p-1}\}$
- Set $\mathcal{R}_1^{e_K} = \{x \in \mathcal{R}_1^\infty : x \le \frac{pe_K}{p-1}\}$

For general extensions L/K of degree $f\epsilon p^w$, enumerate all weakly increasing $r_1 \le \cdots \le r_w$ with each in the allowed set based on the pattern of repetitions. For example, if all are distinct then each r_k is chosen from $\mathcal{R}_1^{e_K \epsilon p^{k-1}}$.

Enumerating fields

To enumerate all fields in a given family, iterate over all specializations of the generic polynomial, and compute the canonical form of each.

Example (2.1.8.14a)

$x^8 + 2a_7x^7 + 2b_6x^6 + 2b_4x^4 + 4c_8 + 2$

Specialization	Canonical form
$x^8 + 2x^7 + 2$	$x^8 + 2x^7 + 2$
$x^8 + 2x^7 + 6$	$x^8 + 2x^7 + 6$
$x^8 + 2x^7 + 2x^4 + 2$	$x^8 + 2x^7 + 2x^4 + 2$
$x^8 + 2x^7 + 2x^4 + 6$	$x^8 + 2x^7 + 2x^4 + 2$
$x^8 + 2x^7 + 2x^6 + 2$	$x^8 + 2x^7 + 2x^6 + 2$
$x^8 + 2x^7 + 2x^6 + 6$	$x^8 + 2x^7 + 2x^6 + 2$
$x^8 + 2x^7 + 2x^6 + 2x^4 + 2$	$x^8 + 2x^7 + 2x^6 + 2x^4 + 2$
$x^8 + 2x^7 + 2x^6 + 2x^4 + 6$	$x^8 + 2x^7 + 2x^6 + 2x^4 + 6$

Polredabs

For number fields, Pari offers `polredabs`, a function that deterministically chooses a defining polynomial.

- To test if two irreducible polynomials define the same number field, check if `polredabs` agrees.
- If you have a database of number fields, and you store their defining polynomials in `polredabs` form, then you can look up polynomials by running `polredabs` on the input and matching. Faster than pairwise isomorphism tests.
- If you have a pool of polynomials, some of which define the same number field, can remove duplicates by using `polredabs`. Faster than pairwise isomorphism tests.

Goal

Do the same for $L/\mathbb{Q}_p$, with a function $\texttt{polred}_p$.

Øystein polynomials

Let $\nu(x) \in \mathcal{O}_L[x]$ be monic and irreducible modulo π_L, and let $\varphi \in \mathcal{O}_L[x]$ by monic.

Definition

We say φ is *ν-Øystein* if

$$\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i$$

with $\varphi_i^* \in \pi_L \mathcal{O}_L[x]$, $\deg \varphi_i^* < \deg \nu$ and $\min_j \varphi_{0,j}^* = 1$.

- Generalizes Eisenstein (case $\nu(x) = x$).
- Any Øystein polyomial is irreducible.
- Any $L/\mathbb{Q}_p$ has an Øystein defining polynomial for any $\nu(x)$ of degree f.

Ramification polygon

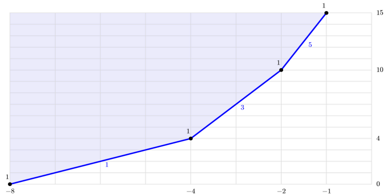
Let $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \in \mathbb{Z}_p[x]$ be Øystein, and let $\alpha \in \overline{\mathbb{Q}_p}$ be one of its roots.

Definition

$$\rho(x) = \frac{\varphi(\nu(\alpha)x + \alpha)}{\nu(\alpha)^e}$$

is the *ramification polynomial* of φ, and its Newton polygon is the *ramification polygon* of φ.

Example ($x^8 + 6x^4 + 1$)



Residual polynomials

Let $\rho(x) = \sum_{i=0}^{n} \rho_i x^i \in \mathcal{O}_L[x]$ and suppose the ramification polygon has a segment $\mathcal{S}$ with endpoints $(-i, v_L(\rho_i))$ and $(-j, v_L(\rho_j))$ of slope $m = \frac{t}{d}$. Let λ be the residue field of L, and $\overline{\alpha}$ denote the reduction of $\alpha \in \mathcal{O}_L$ to λ.

Definition

The *residual polynomial* of $\mathcal{S}$ is

$$\overline{A}_m(z) = \sum_{k=0}^{(i-j)/d} \overline{\rho_{j+kd}\pi_L^{kt-v_L(\rho_j)}} z^k \in \lambda[z].$$

The *additive residual polynomial* of $\mathcal{S}$ is $\overline{A}_m^{+}(z) = z^j \overline{A}_m(z)$.

The nonzero terms correspond to the points of the form $(-i, v_L(\rho_i))$ on the segment of slope m.

Reduction

Suppose given an irreducible polynomial in $\mathbb{Z}_p[x]$. We first find an equivalent Øystein polynomial φ defining the same extension (for fixed set of ν), and let α be a root of φ.

1. Adjust constant term modulo p^2 (scale α by units).
2. Compute the ramification polygon (equivalently rams/slopes/means/ϕ.
3. Adjust residual polynomials to chosen representative (scale α by units).
4. Adjust α to $\alpha + \gamma(\alpha)\nu(\alpha)^{m+1}$ to adjust other p-adic entries of the coefficients of φ. The obstacle to zeroing out coefficients is measured by cokernels of the additive residual polynomials.
5. End up with a set of at most e polynomials in $\mathbb{Z}[x]$. Pick one using a fixed ordering on polynomials.

Explicit inverse Galois problem

The ramification filtration imposes some constraints on what G may arise as p-adic Galois groups. Namely, G must have a filtration $G \supseteq G_0 \supseteq G_1$ with

- G/G_0 cyclic,
- G_0/G_1 cyclic of order prime to p,
- G_1 a p-group.

Even for G satisfying this constraint, there are some groups that do not arise [5].

Problem

Design an efficient algorithm that takes p and a transitive permutation group G as input and outputs the list of $L/\mathbb{Q}_p$ with Galois group G.

Presentation of the absolute Galois group

For $p > 2$, $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ is the profinite group generated by σ, τ, x_0, x_1 with x_0, x_1 pro-p and the following relations (see [3, Thm. 7.5.14])

$$\tau^{\sigma} = \tau^{p}$$

$$\langle x_0, \tau\rangle^{-1} x_0^{\sigma} = x_1^{p}\left[x_1, x_1^{\tau_2^{p+1}} \left\{x_1, \tau_2^{p+1}\right\}^{\sigma_2\tau_2^{(p-1)/2}} \left\{\left\{x_1, \tau_2^{p+1}\right\}, \sigma_2\tau_2^{(p-1)/2}\right\}^{\sigma_2\tau_2^{(p+1)/2}+\tau_2^{(p+1)/2}}\right]$$

$h \in \mathbb{Z}_p$ with mult. order $p-1$, $\quad \mathrm{proj}_p : \hat{\mathbb{Z}} \to \mathbb{Z}_p$

$$\langle x_0, \tau\rangle := (x_0\tau x_0^{h^{p-2}}\tau \ldots x_0^{h}\tau)^{\mathrm{proj}_p/(p-1)}$$

$$\beta : \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p) \to \mathbb{Z}_p^{\times} \qquad \beta(\tau) = h \qquad \beta(\sigma) = 1$$

$$\{x, \rho\} := (x^{\beta(1)}\rho^2 x^{\beta(\rho)}\rho^2 \ldots x^{\beta(\rho^{p-2})}\rho^2)^{\mathrm{proj}_p/(p-1)}$$

$$\sigma_2 := \mathrm{proj}_2(\sigma) \qquad\qquad \tau_2 := \mathrm{proj}_2(\tau)$$

Question

Can you find an analogous description for $p = 2$?

References

[1] J. Guardia, J. Jones, K. Keating, S. Pauli, D. Roberts, D. Roe. *Families of p-adic fields*. arXiv:2507.02360.

[2] J. Guardia, J. Jones, K. Keating, S. Pauli, D. Roberts, D. Roe. *Distinguished defining polynomials for extensions of p-adic fields*. In preparation.

[3] J. Neukirch, A. Schmidt, K. Wingberg. *Cohomology of number fields*. Springer, Berlin, 2015, pg 419.

[4] O. Ore. *Bemerkungen zur Theorie der Differente*. Math. Zeitschr. **25** (1926), pp. 1–8.

[5] D. Roe. *The inverse Galois problem for p-adic fields*. Proceedings of the Thirteenth Algorithmic Number Theory Symposium (ANTS-XIII), Open Book Series 2, Math. Sci. Pub., Berkeley, 2019, pp 393-409.

[6] J.-P. Serre. *Local fields*. Springer, Berlin, 1979, pg 67.

[7] I. Shafarevich. *On p-extensions*. Mat. Sb. **20** (1947), no. 62, 351–363.