Computing local Galois module structure

Kevin Keating
Department of Mathematics
University of Florida

May 26, 2026

Local Fields

Let K be a finite extension of the p-adic field $\mathbb{Q}_p$. Then K is complete with respect to a discrete valuation $v_K : K^\times \to \mathbb{Z}$. Set

$$\begin{aligned}
\mathcal{O}_K &= \{\alpha \in K : v_K(\alpha) \geq 0\} \\
&= \text{ring of integers of } K \\
\pi_K &= \text{uniformizer for } \mathcal{O}_K \text{ (i. e., } v_K(\pi_K) = 1) \\
\mathcal{M}_K &= \pi_K \mathcal{O}_K \\
&= \text{unique maximal ideal of } \mathcal{O}_K \\
\overline{K} &= \mathcal{O}_K / \mathcal{M}_K \\
&= \text{residue field of } K
\end{aligned}$$

Then $\overline{K}$ is a finite field of characteristic p.

Galois Modules

Let L/K be a totally ramified Galois extension of degree n and set $G = \mathrm{Gal}(L/K)$. Define $v_L, \mathcal{O}_L, \pi_L, \mathcal{M}_L$ like we did for K.

Then L is a module over the ring $K[G]$.

In fact, by the normal basis theorem, L is free of rank 1 over $K[G]$.

Let $h \in \mathbb{Z}$. Then $\mathcal{M}_L^h$ is a module over $\mathcal{O}_K[G]$.

If L/K is tamely ramified then $\mathcal{M}_L^h$ is free of rank 1 over $\mathcal{O}_K[G]$.

However, if $p \mid n$ then $\mathcal{M}_L^h$ is (probably) not free over $\mathcal{O}_K[G]$.

Associated Orders

Definition

Let $\mathcal{M}_L^h$ be a (fractional) ideal of $\mathcal{O}_L$. The associated order of $\mathcal{M}_L^h$ is

$$\mathfrak{A}(\mathcal{M}_L^h) = \{\gamma \in K[G] : \gamma(\mathcal{M}_L^h) \subset \mathcal{M}_L^h\}.$$

We have $\mathcal{O}_K[G] \subset \mathfrak{A}(\mathcal{M}_L^h)$, with $\mathcal{O}_K[G] = \mathfrak{A}(\mathcal{O}_L)$ if and only if L/K is tamely ramified. In particular, if L/K has wild ramification then

$$\pi_K^{-1} T \in \mathfrak{A}(\mathcal{O}_L) \setminus \mathcal{O}_K[G],$$

where $T = \sum_{\sigma \in G} \sigma$ is the trace element of $K[G]$.

$\mathcal{M}_L^h$ is a module over $\mathfrak{A}(\mathcal{M}_L^h)$.

Leopoldt Problem: When is $\mathcal{M}_L^h$ a free $\mathfrak{A}(\mathcal{M}_L^h)$-module?

We will focus on the case where L/K is totally ramified of degree $n = p^d$.

Computing the Associated Order of $\mathcal{M}_L^h$

$\mathcal{M}_L^h$ has $\mathcal{O}_K$-basis $\{\pi_L^h, \pi_L^{h+1}, \ldots, \pi_L^{h+n-1}\}$

$K[G]$ has K-basis $G = \{\sigma_i : 1 \leq i \leq n\}$

Let $\gamma = \sum_{k=1}^{n} c_k \sigma_k \in K[G]$. Then $\gamma \in \mathfrak{A}(\mathcal{M}_L^h)$ if and only if

$$\gamma(\pi_L^j) \in \mathcal{M}_L^h \text{ for } h \leq j < h+n. \tag{1}$$

Write $\sigma_k(\pi_L^j) = \sum_{i=h}^{h+n-1} a_{ijk}\pi_L^i$ with $a_{ijk} \in K$. We need $c_i \in K$ such that

$\sum_{k=1}^{n} c_k a_{ijk} \in \mathcal{O}_K$ for all $h \leq i, j < h+n$.

These conditions can be expressed as $A\vec{c} \in \mathcal{O}_K^{n^2}$, with $A \in M_{n^2,n}(K)$.

Using $\mathcal{O}_K$ row operations we get $B \in M_{n,n}(K)$ invertible such that (1) is equivalent to $B\vec{c} \in \mathcal{O}_K^n$. The columns of B^{-1} give the coefficients of n elements of $K[G]$ which form an $\mathcal{O}_K$-basis for $\mathfrak{A}(\mathcal{M}_L^h)$.

Is $\mathcal{M}_L^h$ free over $\mathfrak{A}(\mathcal{M}_L^h)$?

Suppose $\alpha \in \mathcal{M}_L^h$ is such that $\mathfrak{A}(\mathcal{M}_L^h) \cdot \alpha = \mathcal{M}_L^h$.

Let $\beta \in \mathcal{M}_L^h$. Then by Nakayama, $\mathfrak{A}(\mathcal{M}_L^h) \cdot (\alpha + \pi_K \beta) = \mathcal{M}_L^h$. Thus, to determine whether $\mathcal{M}_L^h$ is free over $\mathfrak{A}(\mathcal{M}_L^h)$, it suffices to compute $\mathfrak{A}(\mathcal{M}_L^h) \cdot \alpha$ for a set of nonzero coset representatives α for $\mathcal{M}_L^h / \pi_K \mathcal{M}_L^h$.

Let $c \in \mathcal{O}_K^\times$. Then $\mathfrak{A}(\mathcal{M}_L^h) \cdot (c\alpha) = c\mathcal{M}_L^h = \mathcal{M}_L^h$. Hence the number of $\alpha \in \mathcal{M}_L^h$ we need to consider is $\dfrac{q^n - 1}{q - 1}$, where $q = |\overline{K}|$.

This leads to an algorithm for determining whether $\mathcal{M}_L^h$ is free over $\mathfrak{A}(\mathcal{M}_L^h)$. We implemented this algorithm using Magma [Mag].

Brute force can be slow

```
> Q3:=pAdicField(3,20);
> Q3x<x>:=PolynomialRing(Q3);
> f:=x^9 + 9*x^7 + 6*x^6 + 18*x^5 + 75;
> KG,G,phi,L<piL>:=GroupRing(f);
> G;
Permutation group G acting on a set of cardinality 9
Order = 9 = 3^2
    (1, 7, 4, 3, 9, 6, 2, 8, 5)

> time ModuleGenerator(KG,phi,2);
piL^2 + O(piL^182)
Time: 0.100

> time ModuleGenerator(KG,phi,1);
0
Time: 207.730
```

Some nonabelian examples

```
> Q2:=pAdicField(2,20);
> Q2y<y>:=PolynomialRing(Q2);
> g:=y^4+2*y^2+2;
> KG,G,phi,L<piL>:=GroupRing(g);
> time ModuleGenerator(KG,phi,0);
0
Time: 2.240

> h:=y^8+4*y^4+16*y^3+2;
> KG,G,phi,L<piL>:=GroupRing(h);
> time ModuleGenerator(KG,phi,0);
piL^5 + piL^2 + piL + 1 + O(piL^320)
Time: 11.520
```

The Abelian Case

Suppose $G = \mathrm{Gal}(L/K)$ is abelian. There are standard formulas for computing the primitive idempotents in $K[G]$. The primitive idempotents in $\mathfrak{A}(\mathcal{M}_L^h)$ are sums of primitive idempotents in $K[G]$.

Let $\mathcal{E}_h$ be the set of primitive idempotents in $\mathfrak{A}(\mathcal{M}_L^h)$, and let $e \in \mathcal{E}_h$. Then $e\mathfrak{A}(\mathcal{M}_L^h)$ is an $\mathcal{O}_K$-subalgebra of $\mathfrak{A}(\mathcal{M}_L^h)$, and $e \cdot \mathcal{M}_L^h$ is an $e\mathfrak{A}(\mathcal{M}_L^h)$-submodule of $\mathcal{M}_L^h$.

Furthermore, we have

$$\mathfrak{A}(\mathcal{M}_L^h) = \bigoplus_{e \in \mathcal{E}_h} e\mathfrak{A}(\mathcal{M}_L^h), \qquad \mathcal{M}_L^h = \bigoplus_{e \in \mathcal{E}_h} e \cdot \mathcal{M}_L^h.$$

Hence $\mathcal{M}_L^h$ is free over $\mathfrak{A}(\mathcal{M}_L^h)$ if and only if $e \cdot \mathcal{M}_L^h$ is free over $e\mathfrak{A}(\mathcal{M}_L^h)$ for each $e \in \mathcal{E}_h$.

When are the Factors Free?

Theorem

Let $e \in \mathcal{E}_h$ and let $\{\alpha_1, \ldots, \alpha_r\}$ be an $\mathcal{O}_K$-basis for $e \cdot \mathcal{M}_L^h$. Then $e \cdot \mathcal{M}_L^h$ is free over $e\mathfrak{A}(\mathcal{M}_L^h)$ if and only if $e\mathfrak{A}(\mathcal{M}_L^h) \cdot \alpha_i = e \cdot \mathcal{M}_L^h$ for some $1 \leq i \leq r$.

Proof: See the proof of Theorem 2.1 in [By97].

This leads to an efficient method for determining whether $\mathcal{M}_L^h$ is free over $\mathfrak{A}(\mathcal{M}_L^h)$ in the case where G is abelian.

Abelian examples

```
> Q3:=pAdicField(3,20);
> Q3x<x>:=PolynomialRing(Q3);
> f:=x^9 + 9*x^7 + 6*x^6 + 18*x^5 + 75;
> KG,G,phi,L<piL>:=GroupRing(f);

> time AbelianGenerator(KG,phi,2);
piL^2 + O(piL^144)
Time: 0.220

> time AbelianGenerator(KG,phi,1);
0
Time: 0.360
```

The Bondarko map

There is an L-linear map $\phi : L \otimes_K L \to L[G]$ defined by

$$\phi(a \otimes b) = \sum_{\sigma \in G} a\sigma(b)\sigma.$$

For $a, b, c \in L$ we get

$$\phi(a \otimes b)(c) = \sum_{\sigma \in G} a\sigma(bc) = a\mathrm{Tr}_{L/K}(bc).$$

Proposition

ϕ is an isomorphism of vector spaces over L.

Diagrams

The set $\mathcal{F} = \{(i,j) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq j < n\}$ has a partial order defined by $(i,j) \leq (i',j')$ if and only if $i \leq i'$ and $j \leq j'$.

Let $\beta \in L \otimes_K L$. Then there are unique $b_j \in L$ such that $\beta = \sum_{j=0}^{n-1} b_j \otimes \pi_L^j$. Let

$$R(\beta) = \{(v_L(b_j), j) : 0 \leq j < n,\ b_j \neq 0\}.$$

Then $R(\beta) \subset \mathcal{F}$.

Definition

Define the diagram of $\beta \in L \otimes_K L$ to be

$$D(\beta) = \{(x,y) \in \mathcal{F} : (i,j) \leq (x,y) \text{ for some } (i,j) \in R(\beta)\}.$$

Minimal elements and the diagonal

Let $G(\beta)$ denote the set of minimal elements of $D(\beta)$. Then $G(\beta)$ is also the set of minimal elements of $R(\beta)$. Furthermore, we have

$$D(\beta) = \{(x, y) \in \mathcal{F} : (i, j) \leq (x, y) \text{ for some } (i, j) \in G(\beta)\}.$$

For $\beta \in L \otimes_K L$ with $\beta \neq 0$ define

$$d(\beta) = \min\{i + j : (i, j) \in D(\beta)\}.$$

Define the diagonal of β to be

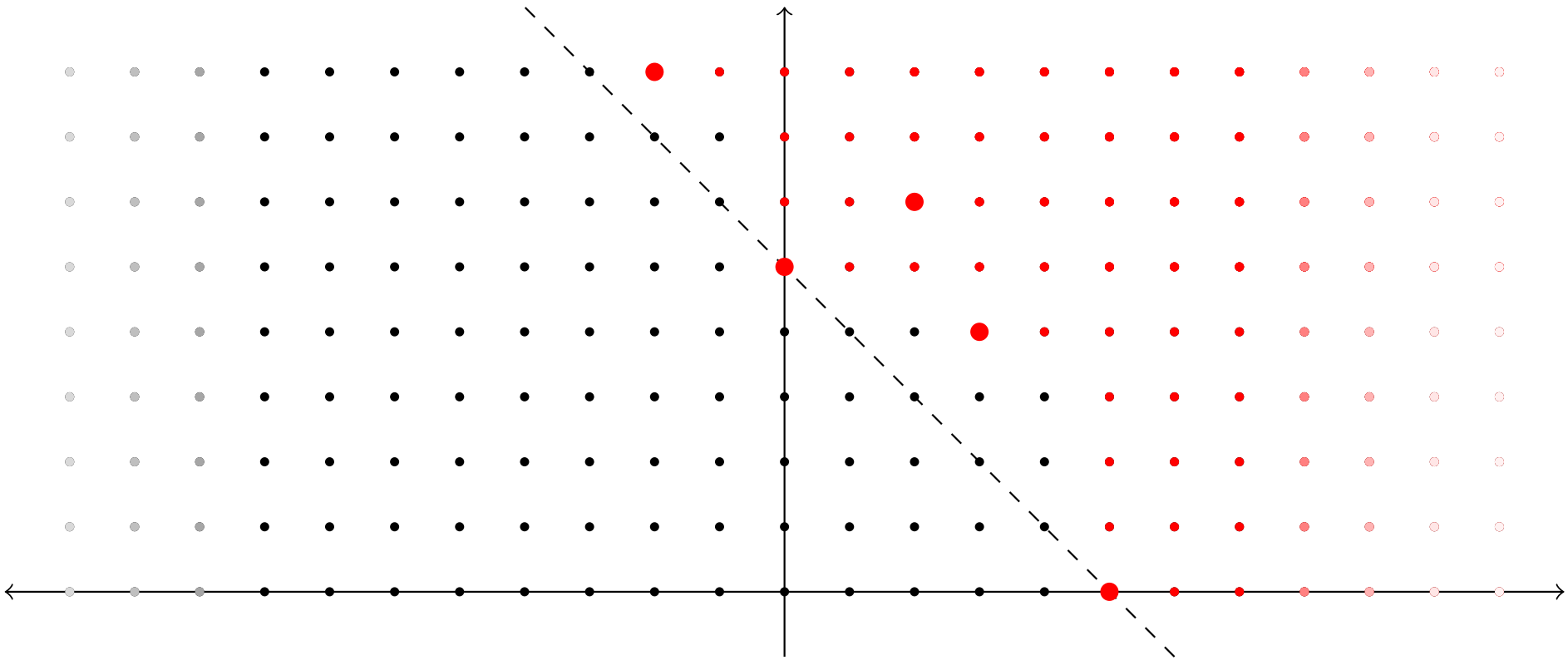
$$N(\beta) = \{(i, j) \in D(\beta) : i + j = d(\beta)\}.$$

Then $N(\beta) \subset G(\beta)$.

A Diagram

$$n = 3^2, \quad \beta = \pi_L^5 \otimes 1 + \pi_L^3 \otimes \pi_L^4 + 1 \otimes \pi_L^5 + \pi_L^2 \otimes \pi_L^6 + \pi_L^{-2} \otimes \pi_L^8$$

$$R(\beta) = \{(5,0),(3,4),(0,5),(2,6),(-2,8)\}$$
$$G(\beta) = \{(5,0),(3,4),(0,5),(-2,8)\}$$
$$N(\beta) = \{(5,0),(0,5)\}$$



Semistable extensions

Definition

Let L/K be a totally ramified Galois extension of degree $n = p^d$. Say that L/K is semistable if there is nonzero $\beta \in L \otimes_K L$ such that

- $\phi(\beta) \in K[G]$,
- $|N(\beta)| = 2$,
- $p \nmid d(\beta)$.

Let $\delta_{L/K}$ be the different of L/K. Then the zeroth index of inseparability of L/K is $i_0 = v_L(\delta_{L/K}) - n + 1$.

Theorem ([Bon02])

Let L/K be a semistable extension. Then $\mathcal{M}_L^{-i_0}$ is a free $\mathfrak{A}(\mathcal{M}_L^{-i_0})$-module of rank 1.

Inverting the Bondarko map

The Bondarko map $\phi : L \otimes_K L \to L[G]$ is L-linear. Using the basis $\{1 \otimes \pi_L^{i-1} : 1 \leq i \leq n\}$ for $L \otimes_K L$ and the basis $G = \{\sigma_i : 1 \leq i \leq n\}$ for $L[G]$, we can represent ϕ by a matrix $A \in M_{n,n}(L)$.

The (i, j) entry of A is $\sigma_i(\pi_L)^{j-1}$, so A is a Vandermonde matrix. There is an easy formula for computing A^{-1}, and hence ϕ^{-1}.

Lemma ([Bon02])

Let L/K be a semistable extension and let $0 \leq t < n$ be such that $t \equiv i_0 \pmod{n}$. Then $p \nmid t$ and there is $\beta \in L \otimes_K L$ such that $\phi(\beta) \in K[G]$ and $N(\beta) = \{(t, 0), (0, t)\}$.

It follows that L/K is semistable if and only if there is $\beta \in L \otimes_K L$ such that $N(\beta) = \{(t, 0), (0, t)\}$ and β is in the K-span of $\{\phi^{-1}(\sigma_i) : \sigma_i \in G\}$.

How to tell whether L/K is semistable

Let $\Lambda_t \subset L \otimes_K L$ denote the $\mathcal{O}_K$-span of the set

$$S_t = \{\pi_L^{t+i-j} \otimes \pi_L^j : 0 \leq i, j < n\}.$$

Then Λ_t is an $\mathcal{O}_K$-lattice in $L \otimes_K L$ with basis S_t.

We use row reduction to find an $\mathcal{O}_K$-basis for $\phi^{-1}(K[G]) \cap \Lambda_t$.

Then we search for $\beta \in \phi^{-1}(K[G]) \cap \Lambda_t$ such that $N(\beta) = \{(t, 0), (0, t)\}$. This can be done by row reducing an $n \times n$ matrix with entries in $\overline{K}$.

L/K is semistable if and only if such β exists.

Example

```
> Q3:=pAdicField(3,20);
> Q3x<x>:=PolynomialRing(Q3);
> f:=(x+1)^6+(x+1)^3+1;
> K<piK>:=ext<Q3|f>;

> Ky<y>:=PolynomialRing(K);
> g:=(y+1)^9-1-piK;
> KG,G,phi,L:=GroupRing(g);
> beta:=Semistab(KG,phi);
```

Example ...

```
> beta;
((-2*piK - 2)*piL - 2*piK - 2 +O(piL^774))*pi2^8
+((-16*piK - 16)*piL - 16*piK - 16 +O(piL^774))*pi2^7
+((-56*piK - 56)*piL - 56*piK - 56 +O(piL^774))*pi2^6
+((-112*piK - 112)*piL - 112*piK - 112 +O(piL^777))*pi2^5
+(4782969*piK^2*piL^2 + (-140*piK - 140)*piL - 140*piK
    - 140 +O(piL^777))*pi2^4
+((-112*piK - 112)*piL - 112*piK - 112 +O(piL^777))*pi2^3
+(-4782969*piK^2*piL^5 - 4782969*piK^2*piL^4
    + (-56*piK - 56)*piL - 56*piK - 56 +O(piL^780))*pi2^2
+((-16*piK - 16)*piL - 16*piK - 16 +O(piL^780))*pi2
+(-2*piK - 2)*piL +O(piL^780)
```

In the above, pi2 represents $1 \otimes \pi_L$. Note that since $i_0 = 100$, we have $-i_0 \equiv 8 \pmod 9$.

```
> AbelianGenerator(KG,phi,8);
piL^8 + O(piL^891)
```

Other things to do

- Collect data about which ideals in L are free over their associated orders in the cases where L/K is a C_p-extension which is maximally ramified, or nearly so.
- Extend this work to compute Galois module structure for local fields of characteristic p.
- Compute Hopf-Galois module structure for local fields.
- Write programs to construct Galois scaffolds.

The Magma programs used here will be made available at:

`https://github.com/kpkeating/galmod`

References

[Mag] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., **24** (1997), 235–265.

[Bo00] Bondarko, M. V., Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields, Doc. Math. **5** (2000), 657–693.

[Bo02] Bondarko, M. V., Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields, Algebraic number theory and algebraic geometry, 27–57, Contemp. Math. 300, Amer. Math. Soc., Providence, RI, 2002.

[By97] Byott, N. P., Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications. J. Thèor. Nombres Bordeaux **9** (1997), 201–219.