How far is an extension of p-adic fields from having a normal integral basis?

Ilaria Del Corso
Università di PISA
(joint work with F. Ferri and D. Lombardo)

Hopf algebras and Galois module theory

Omaha, May 27, 2021

1. Notation and preliminaries

L/K finite Galois extension of p-adic fields;

$\mathcal{O}_L, \mathcal{O}_K$ ring of integers, $e_{L/K} f_{L/K} = [L:K]$ $e_L f_L = [L:\mathbb{Q}_p]$

If L/K is G-Galois $\xRightarrow{\text{N.B.Thm}}$ L is free of rank 1 as $K[G]$-mod.

We also have that $\mathcal{O}_L$ is an $\mathcal{O}_K[G]$-module

$\boxed{\text{Q: To determine the structure of } \mathcal{O}_L \text{ as } \mathcal{O}_K[G]\text{-module}}$

Theorem $\mathcal{O}_L$ is free (of rank 1) as an $\mathcal{O}_K[G]$-module

$\iff$ L/K is tamely ramified

2. The associated order

$$\mathcal{A}_{L/K} = \{ \lambda \in K[G] \mid \lambda \mathcal{O}_L \subseteq \mathcal{O}_L \}$$

- $\mathcal{A}_{L/K}$ is an $\mathcal{O}_K$-order in $K[G]$
- $\mathcal{A}_{L/K} = \mathcal{O}_K[G] \iff L/K$ is tame
- If Γ is an $\mathcal{O}_K$-order of $K[G]$, and $\mathcal{O}_L$ is free over $\Gamma \Rightarrow \Gamma = \mathcal{A}_{L/K}$
- When is $\mathcal{O}_L$ free over $\mathcal{A}_{L/K}$? This question is answered only in particular cases.
- $\mathcal{A}_{L/K}$ is mostly unknown

Freeness results

$\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ in the following cases

Leopoldt 59 + Lettl '98 : L absolutely abelian, $\forall K \subset L$

Bergé 72 : $K = \mathbb{Q}_p$, $L/\mathbb{Q}_p$ dihedral of order $2p$

Martinet '72 : $K = \mathbb{Q}_p$, $Gal(L/\mathbb{Q}_p) \cong Q_8$

Jaulent 81 $K = \mathbb{Q}_p$ $Gal(L/\mathbb{Q}_p)$ metacyclic of some special type.

Johnston '15 . L/K weakly ramified

3. A related question: the minimal index

$$m(L/K) = \min_{\alpha \in \mathcal{O}_L} [\mathcal{O}_L : \mathcal{O}_K[G]\alpha]$$

subgroup index

- $m(L/K) < +\infty$
- $m(L/K) = 1 \iff L/K$ is tame
- $m(L/K)$ is a measure of the failure of the freeness of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module

→ Why not consider $i(L/K) = \min_{\alpha \in \mathcal{O}_L} [\mathcal{O}_L : \mathcal{A}_{L/K}\alpha]$, instead?

- It is not too different, since

$$m(L/K) = [\mathcal{A}_{L/K} : \mathcal{O}_K[G]]\, i(L/K)$$

- If $\mathcal{A}_{L/K}$ is known → no difference, in practice
- If $\mathcal{A}_{L/K}$ is unknown → $m(L/K)$ gives information on

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]]$$

- $m(L/K)$ already appeared in the literature

Johnston 15: L/K wildly and weakly ramified

$$\boxed{m(L/K) = p^{f_L}}$$

→ $m(L/K)$ is effectively computable with the following

Algorithm

1. Compute an integral basis $\{\alpha_i\}$ (e.g. by using the Montes alg.)

2. Compute $w_0 \in \mathcal{O}_L$ such that $L = K[G]\, w_0$ (The NB Thm is effective)

3. Compute $[\mathcal{O}_L : \mathcal{O}_K[G]w_0] = \pi_K^R \mathcal{O}_K$ ← This is the determinant of a computable matrix.
$\mathcal{O}_K$

4. Compute $[\mathcal{O}_L : \mathcal{O}_K[G]w]$ for $w = \sum_{i=1}^{n} v_i \cdot \alpha_i$
and $v_i \in \left\{ \begin{array}{l} \text{representatives in } \mathcal{O}_K \text{ of} \\ \text{the classes of } \mathcal{O}_K / \pi^{R+1}\mathcal{O}_K \end{array} \right\}$ ← finite set

5. $m(L/K) = \min_{w \in X} [\mathcal{O}_L : \mathcal{O}_K[G]w]$
where $X = \{ w$ of point 4 $\}$.

4. A completely general bound

<u>Theorem 1</u> (Vale, Ferri, Lombardo)

Let L/K be a finite Galois extension of p-adic fields. Then

$$v_p(m(L/K)) \leq f_L\,(e_{L/K}-1) + \frac{1}{2}[L:\mathbb{Q}_p]\, v_p([L:K])$$

$$\leq [L:\mathbb{Q}_p]\left(1+\frac{1}{2}v_p[L:K]\right)$$

<u>Corollary</u> $v_p\left([\mathcal{A}_{L/K} : \mathcal{O}_K[G]]\right) \leq f_L\,(e_{L/K}-1) + \frac{1}{2}[L:\mathbb{Q}_p]\,v_p([L:K])$

5. The absolutely abelian case

$$\begin{array}{c} L \\ \Big| \ \text{tot ram} \\ L^{nr} \\ \big| \ \text{unram} \\ K \end{array}$$

Theorem 2 (Idc, Ferri, Lombardo)

L/K finite Galois extension of p-adic fields.

Assume $L/\mathbb{Q}_p$ abelian Then

$$m(L/K) = m(L/L^{nr})$$

If $p>2$ $\quad v_p(m(L/K)) = v_p(m(L/L^{nr}))$

$$= \frac{f_L}{2}\left(e_L\, v_p(e_{L/K}) - \sum_{d \mid e_{L/K}} \frac{\varphi(d)}{[L^{nr}(\zeta_d):L^{nr}]}\, v_{L^{nr}}\left(\operatorname{disc}\left(L^{nr}(\zeta_d)/L^{nr}\right)\right)\right)$$

For $p=2$ the formula is not the same.

Sketch of the proof.

$\boxed{\text{Step 1:}}$ $m(L/K) = m(L/L^{nr})$

We proved that this is true in a more general setting

Proposition

Assume that G_0 is abelian and $\mathcal{O}_L$ free over $A_{L/K}$

Then $\mathcal{O}_L$ is free over $A_{L/L^{nr}}$ and

$$\circledast \quad m(L/K) = [A_{L/K} : \mathcal{O}_K[G]] = m(L/L^{nr}) = [A_{L/L^{nr}} : \mathcal{O}_{L^{nr}}[G_0]]$$

Conversely, if G is abelian and $\mathcal{O}_L$ is free over $A_{L/L^{nr}}$, then $\mathcal{O}_L$ is free over $A_{L/K}$ and $\circledast$ holds

($\Rightarrow$)

- $\mathcal{O}_L$ free over $A_{L/K} \Rightarrow m(L/K) = [A_{L/K} : \mathcal{O}_K[G]]$

- Jacobinsky '63: $\mathcal{A}_{L/K} = \bigoplus_{s \in G/G_0} \left(\mathcal{A}_{L/L^{nr}} \cap K[G_0] \right) s$

$$\begin{tikzcd} L \arrow[d, dash] \arrow[d, dash, bend left=60, "G_0"] \arrow[dd, dash, bend right=60, "G"'] \\ L^{nr} \arrow[d, dash] \\ K \end{tikzcd}$$

so that

$$[\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = \Big[\bigoplus_{s \in G/G_0} (\mathcal{A}_{L/L^{nr}} \cap K[G_0]) s : \bigoplus_{s \in G/G_0} \mathcal{O}_K[G_0] s \Big] =$$

$$= [\mathcal{A}_{L/L^{nr}} \cap K[G_0] : \mathcal{O}_K[G_0]]^{[G:G_0]} = \left[\mathcal{O}_{L^{nr}} \otimes_{\mathcal{O}_K} (\mathcal{A}_{L/L^{nr}} \cap K[G_0]) : \mathcal{O}_{L^{nr}}[G_0] \right]$$

$\mathcal{O}_{L^{nr}}$ is free over $\mathcal{O}_K$ of rank $[G:G_0]$

- Bergé '78: If G is abelian (for simplicity we consider this case, but G_0 abelian is enough)

$$\mathcal{O}_{L^{nr}} \otimes \mathcal{A}_{L/L^{nr}} \cap K[G_0] \simeq \mathcal{A}_{L/L^{nr}}$$

$$\Rightarrow \quad m(L/K) = [\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = [\mathcal{A}_{L/L^{nr}} : \mathcal{O}_{L^{nr}}[G_0]]$$

- Using the properties of "clean orders" we can show $m(L/L^{nr})$

Step 2: Description of $\mathcal{A}_{L/K}$ for L/K TOT ram

1. L/K TOT ram + L absolutely abelian + p odd

$\Downarrow$ Lettl '98

$\mathcal{A}_{L/K}$ is the maximal order of $K[G]$

2. G is cyclic

In fact, local K-W $L \subset \mathbb{Q}_p(\zeta_n)$ and the inertia group of $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}$ is cyclic.

$$\Rightarrow \quad K[G] \cong \prod_{d \mid |G|} K(\zeta_d)^{\frac{\varphi(d)}{[K(\zeta_d):K]}}$$

$$\Rightarrow \quad \boxed{\mathcal{A}_{L/K} \cong \prod_{d \mid |G|} \mathcal{O}_{K(\zeta_d)}^{\frac{\varphi(d)}{[K(\zeta_d):K]}}}$$

Step 3: Computation of $m(L/K) = [\mathcal{A}_{L/K} : \mathcal{O}_K[G]]$

$$\operatorname{disc}_K \mathcal{O}_K[G] = [\mathcal{A}_{L/K} : \mathcal{O}_K[G]]^2_{\mathcal{O}_K} \operatorname{disc}_K \mathcal{A}_{L/K}$$

$$|G|^{|G|}\mathcal{O}_K \qquad\qquad \prod_{d \mid |G|} \operatorname{disc}(K(\zeta_d)/K)^{\frac{\varphi(d)}{[K(\zeta_d):K]}}$$

$\Rightarrow$ We have a formula for $[\mathcal{A}_{L/K} : \mathcal{O}_K[G]]_{\mathcal{O}_K}$

and $m(L/K) = [\mathcal{A}_{L/K} : \mathcal{O}_K[G]] = N_{K/\mathbb{Q}_p}\left([\mathcal{A}_{L/K} : \mathcal{O}_K[G]]_{\mathcal{O}_K}\right)$

Step 4: The case $p=2$

In general:
- $\mathcal{A}_{L/L^{nr}}$ is not maximal
- G_0 is not cyclic

One could, in principle, do similar computations, but we only considered some specific examples. □

Corollary

- L/K absolutely abelian, p odd
- $e_{L/K} = p^n d$, $(d,p)=1$
- $K/\mathbb{Q}_p$ unramified

$$\Longrightarrow \quad m(L/K) = p^{\frac{f_L d (p^n - 1)}{p-1}}$$

5. Extensions of degree p.

Theorem 3 (Del Corso, Ferri, Lombardo)

Let L/K be a ramified Galois extension, $[L:K]=p$

Let t be the ramification jump.

Then

- if $t \equiv 0 \ (p)$ $\quad v_p(m(L/K)) = \frac{1}{2}[L:\mathbb{Q}_p]$
- if $t \not\equiv 0 (p)$ $\quad v_p(m(L/K)) =$ explicit in terms of f_K, e_K, t

The method used to prove Theorem 3 also allows us to give a new proof of the following result originally due to Bertrandias and Ferton

Theorem 4 (BF 72)

Let L/K be a totally ramified cyclic extension of degree p of a p-adic field. Let t be the ramification jump, let $a \in \{0, \dots, p-1\}$ be such that $t \equiv a \ (p)$.

Then the following hold:

(1) if $a = 0$ or $a \mid p-1 \Rightarrow \mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$

(2) Suppose that $t < \frac{e_K p}{p-1} - 1$ holds. Then $\mathcal{O}_L$ free $\Rightarrow a \mid p-1$

Thank you!