# The ring of integers of degree *p* extensions of *p*-adic fields

## Daniel Gil Muñoz

Charles University & Università di Pisa

## Hopf Algebras & Galois Module Theory June 2025

University of Connecticut (online)







# Table of contents



- Problem and main result
- 3 Schema of proof

Let *p* be an odd prime number.

Let *p* be an odd prime number. By *p*-adic field we mean any finite extension of  $\mathbb{Q}_p$ . Let *p* be an odd prime number.

By *p*-adic field we mean any finite extension of  $\mathbb{Q}_p$ .

## Notation

Let F be a p-adic field.

- $\mathcal{O}_F$  is the ring of integers of F.
- $v_F$  is the valuation of F.
- $\pi_F$  is a uniformizer of F.
- $\mathfrak{p}_F$  is the prime ideal of  $\mathcal{O}_F$ .
- $\overline{F}$  is the residue field of F.

• 
$$\pi_{\mathcal{K}}\mathcal{O}_L = \mathfrak{p}_L^{e(L/\mathcal{K})}, e(L/\mathcal{K})$$
 is the ramification index.

• 
$$\pi_{\mathcal{K}}\mathcal{O}_{L} = \mathfrak{p}_{L}^{e(L/\mathcal{K})}$$
,  $e(L/\mathcal{K})$  is the ramification index.

**Fact:** e(L/K) | [L : K].

• 
$$\pi_{\mathcal{K}}\mathcal{O}_{L} = \mathfrak{p}_{L}^{e(L/\mathcal{K})}, e(L/\mathcal{K})$$
 is the ramification index.

**Fact:** e(L/K) | [L : K].

 L/K is ramified (resp. totally ramified) if e(L/K) > 1 (resp. e(L/K) = [L : K]).

• 
$$\pi_{\mathcal{K}}\mathcal{O}_{L} = \mathfrak{p}_{L}^{e(L/\mathcal{K})}, e(L/\mathcal{K})$$
 is the ramification index.

**Fact:** e(L/K) | [L : K].

 L/K is ramified (resp. totally ramified) if e(L/K) > 1 (resp. e(L/K) = [L : K]).

Assume that L/K is Galois with group G.

• 
$$\pi_{\mathcal{K}}\mathcal{O}_{L} = \mathfrak{p}_{L}^{e(L/\mathcal{K})}, e(L/\mathcal{K})$$
 is the ramification index.

**Fact:** e(L/K) | [L : K].

 L/K is ramified (resp. totally ramified) if e(L/K) > 1 (resp. e(L/K) = [L : K]).

Assume that L/K is Galois with group G.

• 
$$G_i := \{ \sigma \in G \mid v_L(\sigma(\alpha) - \alpha) \ge i + 1 \text{ for all } \alpha \in \mathcal{O}_L \}, i \ge 0.$$

*G<sub>i</sub> i*-th ramification group.

• 
$$\pi_{\mathcal{K}}\mathcal{O}_{L} = \mathfrak{p}_{L}^{e(L/\mathcal{K})}, e(L/\mathcal{K})$$
 is the ramification index.

**Fact:** e(L/K) | [L : K].

 L/K is ramified (resp. totally ramified) if e(L/K) > 1 (resp. e(L/K) = [L : K]).

Assume that L/K is Galois with group G.

• 
$$G_i := \{ \sigma \in G \mid v_L(\sigma(\alpha) - \alpha) \ge i + 1 \text{ for all } \alpha \in \mathcal{O}_L \}, i \ge 0.$$

*G<sub>i</sub> i*-th ramification group.

• Chain of ramification groups for L/K:  $G_{-1} := G \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq \{1\}.$ 

• 
$$\pi_{\mathcal{K}}\mathcal{O}_{L} = \mathfrak{p}_{L}^{e(L/\mathcal{K})}$$
,  $e(L/\mathcal{K})$  is the ramification index.

**Fact:** e(L/K) | [L : K].

 L/K is ramified (resp. totally ramified) if e(L/K) > 1 (resp. e(L/K) = [L : K]).

Assume that L/K is Galois with group G.

• 
$$G_i := \{ \sigma \in G \mid v_L(\sigma(\alpha) - \alpha) \ge i + 1 \text{ for all } \alpha \in \mathcal{O}_L \}, i \ge 0.$$

*G<sub>i</sub> i*-th ramification group.

• Chain of ramification groups for L/K:  $G_{-1} := G \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq \{1\}.$ 

• Ramification jump:  $t \in \mathbb{Z}_{\geq 1}, G_t \neq G_{t+1}$ .



- Problem and main result
- 3 Schema of proof

Let L/K be a degree *p* extension of *p*-adic fields, *p* odd prime. Let  $\tilde{L}$  be the normal closure of L/K and let  $G = \text{Gal}(\tilde{L}/K)$ . Let L/K be a degree *p* extension of *p*-adic fields, *p* odd prime. Let  $\tilde{L}$  be the normal closure of L/K and let  $G = \text{Gal}(\tilde{L}/K)$ . **1st remark:** L/K is Hopf-Galois. Let L/K be a degree p extension of p-adic fields, p odd prime. Let  $\tilde{L}$  be the normal closure of L/K and let  $G = \text{Gal}(\tilde{L}/K)$ . **1st remark:** L/K is Hopf-Galois.

 $\overline{K}$  finite  $\Longrightarrow$  *G* solvable  $\Longrightarrow$  *L*/*K* Hopf-Galois.

Let  $\widetilde{L}$  be the normal closure of L/K and let  $G = \operatorname{Gal}(\widetilde{L}/K)$ .

**1st remark:** L/K is Hopf-Galois.

 $\overline{K}$  finite  $\Longrightarrow$  *G* solvable  $\Longrightarrow$  *L*/*K* Hopf-Galois.

**2nd remark:** *L*/*K* admits a unique Hopf-Galois structure *H*.

Let  $\widetilde{L}$  be the normal closure of L/K and let  $G = \operatorname{Gal}(\widetilde{L}/K)$ .

**1st remark:** L/K is Hopf-Galois.

 $\overline{K}$  finite  $\Longrightarrow$  *G* solvable  $\Longrightarrow$  *L*/*K* Hopf-Galois.

**2nd remark:** L/K admits a unique Hopf-Galois structure H.

It follows from Byott's uniqueness theorem (*p* is Burnside).

Let  $\widetilde{L}$  be the normal closure of L/K and let  $G = \operatorname{Gal}(\widetilde{L}/K)$ .

**1st remark:** L/K is Hopf-Galois.

 $\overline{K}$  finite  $\Longrightarrow$  *G* solvable  $\Longrightarrow$  *L*/*K* Hopf-Galois.

**2nd remark:** L/K admits a unique Hopf-Galois structure H.

It follows from Byott's uniqueness theorem (*p* is Burnside).

#### Problem

Let L/K be a degree p extension of p-adic fields and write  $\mathfrak{A}_{L/K}$  for the associated order in H. Find a necessary and sufficient condition for  $\mathcal{O}_L$  being  $\mathfrak{A}_{L/K}$ -free.

Let  $\widetilde{L}$  be the normal closure of L/K and let  $G = \operatorname{Gal}(\widetilde{L}/K)$ .

**1st remark:** L/K is Hopf-Galois.

 $\overline{K}$  finite  $\Longrightarrow$  *G* solvable  $\Longrightarrow$  *L*/*K* Hopf-Galois.

**2nd remark:** L/K admits a unique Hopf-Galois structure *H*.

It follows from Byott's uniqueness theorem (*p* is Burnside).

#### Problem

Let L/K be a degree p extension of p-adic fields and write  $\mathfrak{A}_{L/K}$  for the associated order in H. Find a necessary and sufficient condition for  $\mathcal{O}_L$  being  $\mathfrak{A}_{L/K}$ -free.

Recall that

$$\mathfrak{A}_{L/K} = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}.$$

Let 
$$r = [\widetilde{L} : L]$$
. Then  $G \cong C_p \rtimes C_r$  and  $r \mid p - 1$ .

Standard result: If L/K is unramified, then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. This only might happen when L/K is Galois.

Standard result: If L/K is unramified, then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. This only might happen when L/K is Galois.

Assume that L/K is (totally) ramified. Then  $G_1 \cong C_p$ .

Standard result: If L/K is unramified, then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. This only might happen when L/K is Galois.

Assume that L/K is (totally) ramified. Then  $G_1 \cong C_p$ .

The chain of ramification groups of  $\tilde{L}/K$  is

$$G_{-1} \coloneqq G \supseteq G_0 \supseteq G_1 = \cdots = G_t \supseteq \{1\}$$

Standard result: If L/K is unramified, then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. This only might happen when L/K is Galois.

Assume that L/K is (totally) ramified. Then  $G_1 \cong C_p$ .

The chain of ramification groups of  $\tilde{L}/K$  is

$$G_{-1} := G \supseteq G_0 \supseteq G_1 = \cdots = G_t \supseteq \{1\}$$

We see that there is a unique ramification jump *t*, which satisfies

$$1 \leq t \leq \frac{r\rho e}{p-1},$$

where  $e := e(K/\mathbb{Q}_p)$ .

Standard result: If L/K is unramified, then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. This only might happen when L/K is Galois.

Assume that L/K is (totally) ramified. Then  $G_1 \cong C_p$ .

The chain of ramification groups of  $\tilde{L}/K$  is

$$G_{-1} \coloneqq G \supseteq G_0 \supseteq G_1 = \cdots = G_t \supsetneq \{1\}$$

We see that there is a unique ramification jump *t*, which satisfies

$$1 \leq t \leq \frac{r\rho e}{p-1},$$

where  $e := e(K/\mathbb{Q}_p)$ .

It is known that  $p \mid t$  if and only if  $t = \frac{rpe}{p-1}$ .

# **F.** Bertrandias, J. P. Bertrandias, M. J. Ferton (1972): Complete characterization when L/K is Galois.

# **F.** Bertrandias, J. P. Bertrandias, M. J. Ferton (1972): Complete characterization when L/K is Galois.

#### Theorem

Let L/K be a totally ramified Galois degree p extension of p-adic fields. Let t be the ramification jump of L/K and a = rem(t, p).

• If 
$$a = 0$$
,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

2 If  $a \mid p - 1$ ,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. Moreover, if  $t < \frac{pe}{p-1} - 1$ , the converse holds.

If  $t \ge \frac{pe}{p-1} - 1$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if the length of the continued fraction expansion of  $\frac{t}{p}$  is at most 4.

Continued fraction expansion of  $\frac{t}{p}$ :

$$\frac{t}{p} = [a_0; a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_n}}}.$$

Continued fraction expansion of  $\frac{t}{D}$ :

$$\frac{t}{p} = [a_0; a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_n}}}.$$

The number *n* is called the **length** of the continued fraction expansion.

Continued fraction expansion of  $\frac{t}{D}$ :

$$\frac{t}{p} = [a_0; a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_n}}}.$$

The number *n* is called the **length** of the continued fraction expansion.

Every rational number has a continued fraction expansion with finite length.

## • F. Bertrandias, M. J. Ferton (1972).

Sketch of proof of the first two statements.

#### • F. Bertrandias, J. P. Bertrandias, M. J. Ferton (1972).

Sketch of proof of the third statement.

# • F. Bertrandias, M. J. Ferton (1972).

Sketch of proof of the first two statements.

# • F. Bertrandias, J. P. Bertrandias, M. J. Ferton (1972).

Sketch of proof of the third statement.

# • M. J. Ferton PhD dissertation (1972).

Detailed proof of the three statements.
### • F. Bertrandias, M. J. Ferton (1972).

Sketch of proof of the first two statements.

• F. Bertrandias, J. P. Bertrandias, M. J. Ferton (1972). Sketch of proof of the third statement.

# • M. J. Ferton PhD dissertation (1972).

Detailed proof of the three statements.

# • N. P. Byott, L. Childs, G. Elder (2018).

Proof of the second statement (weaker version) using scaffolds.

### • F. Bertrandias, M. J. Ferton (1972).

Sketch of proof of the first two statements.

• F. Bertrandias, J. P. Bertrandias, M. J. Ferton (1972). Sketch of proof of the third statement.

# • M. J. Ferton PhD dissertation (1972).

Detailed proof of the three statements.

# • N. P. Byott, L. Childs, G. Elder (2018).

Proof of the second statement (weaker version) using scaffolds.

# • I. Del Corso, F. Ferri, D. Lombardo (2022).

Proof of the first two statements using the notion of minimal index.

**G.** (2023): Complete characterization when L/K has normal closure  $\tilde{L}$  dihedral of degree 2*p*.

**G.** (2023): Complete characterization when L/K has normal closure  $\tilde{L}$  dihedral of degree 2*p*.

If  $e(\tilde{L}/K) = p$ , the criteria are the same as in the Galois case. Otherwise,  $\tilde{L}/K$  is totally ramified. **G. (2023)**: Complete characterization when L/K has normal closure  $\tilde{L}$  dihedral of degree 2*p*.

If  $e(\tilde{L}/K) = p$ , the criteria are the same as in the Galois case. Otherwise,  $\tilde{L}/K$  is totally ramified.

#### Theorem

Let L/K be a degree p extension of p-adic fields with totally ramified dihedral degree 2p normal closure  $\tilde{L}$ . Let t be the ramification jump of  $\tilde{L}/K$  and let  $a = \text{rem}(\ell := \frac{t+p}{2}, p)$ .

**1** If 
$$a = 0$$
,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

- ② If a | p 1,  $O_L$  is  $\mathfrak{A}_{L/K}$ -free. Moreover, if  $t < \frac{2pe}{p-1} 2$ , the converse holds.
- If  $t \ge \frac{2pe}{p-1} 2$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if the length of the continued fraction expansion of  $\frac{\ell}{p}$  is at most 4.

#### Theorem

Let L/K be a degree p extension of p-adic fields with totally ramified normal closure  $\tilde{L}$ . Let  $r = [\tilde{L} : L]$ , t be the ramification jump of  $\tilde{L}/K$ , let c = rem(t, r) and let  $a = \text{rem}(\ell := \frac{t+pc(r-1)}{r}, p)$ .

**1** If 
$$a = 0$$
,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

- 2 If  $a \mid p 1$ ,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. Moreover, if  $t < \frac{rpe}{p-1} r$ , the converse holds.
- If  $t \ge \frac{rpe}{p-1} r$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if the length of the continued fraction expansion of  $\frac{\ell}{p}$  is at most 4.

#### Theorem

Let L/K be a degree p extension of p-adic fields with totally ramified normal closure  $\tilde{L}$ . Let  $r = [\tilde{L} : L]$ , t be the ramification jump of  $\tilde{L}/K$ , let c = rem(t, r) and let  $a = \text{rem}(\ell := \frac{t+pc(r-1)}{r}, p)$ .

**1** If 
$$a = 0$$
,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

- 2 If  $a \mid p 1$ ,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. Moreover, if  $t < \frac{rpe}{p-1} r$ , the converse holds.
- If  $t \ge \frac{rpe}{p-1} r$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if the length of the continued fraction expansion of  $\frac{\ell}{p}$  is at most 4.

• Why  $\ell \in \mathbb{Z}$ ?

#### Theorem

Let L/K be a degree p extension of p-adic fields with totally ramified normal closure  $\tilde{L}$ . Let  $r = [\tilde{L} : L]$ , t be the ramification jump of  $\tilde{L}/K$ , let c = rem(t, r) and let  $a = \text{rem}(\ell := \frac{t+pc(r-1)}{r}, p)$ .

**1** If 
$$a = 0$$
,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

- 2 If  $a \mid p 1$ ,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. Moreover, if  $t < \frac{rpe}{p-1} r$ , the converse holds.
- If  $t \ge \frac{rpe}{p-1} r$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if the length of the continued fraction expansion of  $\frac{\ell}{p}$  is at most 4.
  - Why  $\ell \in \mathbb{Z}$ ?
  - What if  $\tilde{L}/K$  is not totally ramified?



#### • Why $\ell \in \mathbb{Z}$ ?

Since  $c = \operatorname{rem}(t, r)$ ,  $t \equiv c \pmod{r}$ .

#### • Why $\ell \in \mathbb{Z}$ ?

Since  $c = \operatorname{rem}(t, r)$ ,  $t \equiv c \pmod{r}$ . In addition,  $r \mid p - 1 \Longrightarrow p \equiv 1 \pmod{r}$ .

• Why 
$$\ell \in \mathbb{Z}$$
?

Since  $c = \operatorname{rem}(t, r)$ ,  $t \equiv c \pmod{r}$ . In addition,  $r \mid p - 1 \Longrightarrow p \equiv 1 \pmod{r}$ . Thus,

$$t + pc(r-1) \equiv c - c = 0 \pmod{r}.$$

• Why 
$$\ell \in \mathbb{Z}$$
?

Since  $c = \operatorname{rem}(t, r)$ ,  $t \equiv c \pmod{r}$ . In addition,  $r \mid p - 1 \Longrightarrow p \equiv 1 \pmod{r}$ . Thus,

$$t + pc(r-1) \equiv c - c = 0 \pmod{r}.$$

Hence,  $\ell \in \mathbb{Z}$ .

```
What if L̃/K is not totally ramified?
L̃
H
K
```

Н

Κ

Let *L'* (resp. *K'*) be the inertia field of  $\tilde{L}/L$  (resp.  $\tilde{L}/K$ ) and let  $H' = K' \otimes_K H$ .



Let L' (resp. K') be the inertia field of  $\tilde{L}/L$  (resp.  $\tilde{L}/K$ ) and let  $H' = K' \otimes_K H$ .



Let L' (resp. K') be the inertia field of  $\tilde{L}/L$  (resp.  $\tilde{L}/K$ ) and let  $H' = K' \otimes_K H$ .

#### Proposition

L'/K' is a degree p extension of p-adic fields with totally ramified normal closure and  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if  $\mathcal{O}_{L'}$  is  $\mathfrak{A}_{L'/K'}$ -free.



Then, we may assume without loss of generality that L/K is totally ramified.



- Problem and main result
- 3 Schema of proof

We recall the main result.

We recall the main result.

#### Theorem

Let L/K be a degree p extension of p-adic fields with totally ramified normal closure  $\tilde{L}$ . Let  $r = [\tilde{L} : L]$ , t be the ramification jump of  $\tilde{L}/K$ , let  $c = \operatorname{rem}(t, r)$  and let  $a = \operatorname{rem}(\ell := \frac{t + pc(r-1)}{r}, p)$ .

**1** If 
$$a = 0$$
,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

- 2 If  $a \mid p 1$ ,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free. Moreover, if  $t < \frac{rpe}{p-1} r$ , the converse holds.
- If  $t \ge \frac{rpe}{p-1} r$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if the length of the continued fraction expansion of  $\frac{\ell}{p}$  is at most 4.

• This is the condition that  $p \mid \ell = \frac{t + pc(r-1)}{r}$ , so  $p \mid t$  and  $t = \frac{rpe}{p-1}$ .

- 1. If a = 0,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.
- This is the condition that  $p \mid \ell = \frac{t + pc(r-1)}{r}$ , so  $p \mid t$  and  $t = \frac{rpe}{p-1}$ .
- Let *M* be such that *LM* = *L*. By the Galois case, *L* = *M*(γ) for some γ ∈ O<sub>*i*</sub> which is a *p*-th root of a uniformizer of *M*.

- This is the condition that  $p \mid \ell = \frac{t + pc(r-1)}{r}$ , so  $p \mid t$  and  $t = \frac{rpe}{p-1}$ .
- Let *M* be such that *LM* = *L*. By the Galois case, *L* = *M*(γ) for some γ ∈ O<sub>*i*</sub> which is a *p*-th root of a uniformizer of *M*.
- Now, L = K(α) for α = N<sub>L/L</sub>(γ), and this is a p-th root of a uniformizer of K.

- This is the condition that  $p \mid \ell = \frac{t + pc(r-1)}{r}$ , so  $p \mid t$  and  $t = \frac{rpe}{p-1}$ .
- Let *M* be such that *LM* = *L*. By the Galois case, *L* = *M*(γ) for some γ ∈ O<sub>1</sub> which is a *p*-th root of a uniformizer of *M*.
- Now, L = K(α) for α = N<sub>L/L</sub>(γ), and this is a p-th root of a uniformizer of K.
- We prove that α is an eigenvector of the action of H, which allows us to obtain an O<sub>K</sub>-basis of 𝔅<sub>H</sub> of primitive pairwise orthogonal idempotents.

- This is the condition that  $p \mid \ell = \frac{t + pc(r-1)}{r}$ , so  $p \mid t$  and  $t = \frac{rpe}{p-1}$ .
- Let *M* be such that *LM* = *L*. By the Galois case, *L* = *M*(γ) for some γ ∈ O<sub>1</sub> which is a *p*-th root of a uniformizer of *M*.
- Now, L = K(α) for α = N<sub>L/L</sub>(γ), and this is a p-th root of a uniformizer of K.
- We prove that α is an eigenvector of the action of H, which allows us to obtain an O<sub>K</sub>-basis of 𝔅<sub>H</sub> of primitive pairwise orthogonal idempotents.
- We use this basis to establish an isomorphism  $\varphi: H \longrightarrow K^p$  of K-algebras such that  $\varphi(\mathfrak{A}_{L/K}) = \mathcal{O}_K^p$ .

- This is the condition that  $p \mid \ell = \frac{t + pc(r-1)}{r}$ , so  $p \mid t$  and  $t = \frac{rpe}{p-1}$ .
- Let *M* be such that *LM* = *L*. By the Galois case, *L* = *M*(γ) for some γ ∈ O<sub>*i*</sub> which is a *p*-th root of a uniformizer of *M*.
- Now, L = K(α) for α = N<sub>L/L</sub>(γ), and this is a p-th root of a uniformizer of K.
- We prove that α is an eigenvector of the action of H, which allows us to obtain an O<sub>K</sub>-basis of 𝔄<sub>H</sub> of primitive pairwise orthogonal idempotents.
- We use this basis to establish an isomorphism
   φ: H → K<sup>p</sup> of K-algebras such that φ(𝔄<sub>L/K</sub>) = O<sup>p</sup><sub>K</sub>.

Therefore,  $\mathfrak{A}_{L/K}$  is the maximal  $\mathcal{O}_{K}$ -order in  $H \Longrightarrow \mathcal{O}_{L}$  is  $\mathfrak{A}_{L/K}$ -free.

G. Elder; *Ramified extensions of degree p and their Hopf-Galois module structure* J. Théor. Nr. Bordx. 1 (2018), 19-40.

G. Elder; *Ramified extensions of degree p and their Hopf-Galois module structure* J. Théor. Nr. Bordx. 1 (2018), 19-40.

**Typical extensions:** Separable totally ramified degree *p* extensions of local fields that are not generated by a root of a prime element.

G. Elder; *Ramified extensions of degree p and their Hopf-Galois module structure* J. Théor. Nr. Bordx. 1 (2018), 19-40.

**Typical extensions:** Separable totally ramified degree *p* extensions of local fields that are not generated by a root of a prime element.

**Main theorem (particular case):** The typical degree *p* extensions of *p*-adic fields with totally ramified normal closure are the ones defined by an equation

$$x^{p} - \alpha^{\frac{p-1}{r}} x - \beta = \mathbf{0},$$

with  $v_{\mathcal{K}}(\alpha) = c$ ,  $v_{\mathcal{K}}(\beta) = -b$ , where  $b, c \in \mathbb{Z}$  are such that  $0 \le c < r$ , gcd(c, r) = 1 and  $1 \le bc + pr \le \frac{rpe}{p-1}$ .

G. Elder; *Ramified extensions of degree p and their Hopf-Galois module structure* J. Théor. Nr. Bordx. 1 (2018), 19-40.

**Typical extensions:** Separable totally ramified degree p extensions of local fields that are not generated by a root of a prime element.

**Main theorem (particular case):** The typical degree *p* extensions of *p*-adic fields with totally ramified normal closure are the ones defined by an equation

$$x^{p} - \alpha^{\frac{p-1}{r}} x - \beta = \mathbf{0},$$

with  $v_{\mathcal{K}}(\alpha) = c$ ,  $v_{\mathcal{K}}(\beta) = -b$ , where  $b, c \in \mathbb{Z}$  are such that  $0 \le c < r$ , gcd(c, r) = 1 and  $1 \le bc + pr \le \frac{rpe}{p-1}$ .

Moreover, the ramification jump of  $\tilde{L}/K$  is t = br + pc.

Since  $p \nmid t$ , L/K is typical. Let  $x^p - \alpha^{\frac{p-1}{r}}x - \beta = 0$  be its defining equation.
We can give a description of the underlying Hopf algebra of H.

We can give a description of the underlying Hopf algebra of H.

## Theorem

Let L/K be a typical degree p extension of p-adic fields. The only Hopf-Galois structure on L/K is H = K[w], where

$$w = y^{r-1} \Big( \sum_{m=1}^{p-1} \chi(m)^{-1} \sigma^m \Big).$$

Moreover,  $w^p = \varepsilon p y^{(p-1)(r-1)} w$ ,  $\varepsilon \in \mathcal{O}_K^*$ .

We can give a description of the underlying Hopf algebra of H.

## Theorem

Let L/K be a typical degree p extension of p-adic fields. The only Hopf-Galois structure on L/K is H = K[w], where

$$w = y^{r-1} \Big( \sum_{m=1}^{p-1} \chi(m)^{-1} \sigma^m \Big).$$

Moreover,  $w^{p} = \varepsilon p y^{(p-1)(r-1)} w$ ,  $\varepsilon \in \mathcal{O}_{K}^{*}$ .

• 
$$\widetilde{L} = L(y)$$
 with  $y^r = \alpha$  (by Elder's result).

We can give a description of the underlying Hopf algebra of H.

# Theorem

Let L/K be a typical degree p extension of p-adic fields. The only Hopf-Galois structure on L/K is H = K[w], where

$$w = y^{r-1} \Big( \sum_{m=1}^{p-1} \chi(m)^{-1} \sigma^m \Big).$$

Moreover,  $w^{p} = \varepsilon p y^{(p-1)(r-1)} w$ ,  $\varepsilon \in \mathcal{O}_{K}^{*}$ .

• 
$$\widetilde{L} = L(y)$$
 with  $y^r = \alpha$  (by Elder's result).

•  $\sigma$  is an order p generator of  $G \cong C_p \rtimes C_r$ .

We can give a description of the underlying Hopf algebra of H.

# Theorem

Let L/K be a typical degree p extension of p-adic fields. The only Hopf-Galois structure on L/K is H = K[w], where

$$w = y^{r-1} \Big( \sum_{m=1}^{p-1} \chi(m)^{-1} \sigma^m \Big).$$

Moreover,  $w^{p} = \varepsilon p y^{(p-1)(r-1)} w$ ,  $\varepsilon \in \mathcal{O}_{K}^{*}$ .

- $\widetilde{L} = L(y)$  with  $y^r = \alpha$  (by Elder's result).
- $\sigma$  is an order p generator of  $G \cong C_p \rtimes C_r$ .
- $\chi: \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}_p$  is the *p*-adic Teichmuller character.

The knowledge of w and the degree p polynomial it satisfies allows us to have a good control on the action of H on L and, especially, their valuations.

The knowledge of w and the degree p polynomial it satisfies allows us to have a good control on the action of H on L and, especially, their valuations.

# Proposition

Let L/K be a typical degree p extension of p-adic fields and let H = K[w] be its only Hopf-Galois structure. Call  $\ell = \frac{pc(r-1)+t}{r}$ . Given  $x \in L$ ,  $v_l(w \cdot x) > \ell + v_l(x)$ ,

with equality if and only if  $p \nmid v_L(x)$ .

The knowledge of w and the degree p polynomial it satisfies allows us to have a good control on the action of H on L and, especially, their valuations.

## Proposition

Let L/K be a typical degree p extension of p-adic fields and let H = K[w] be its only Hopf-Galois structure. Call  $\ell = \frac{pc(r-1)+t}{r}$ . Given  $x \in L$ ,  $v_l(w \cdot x) > \ell + v_l(x)$ ,

with equality if and only if  $p \nmid v_L(x)$ .

In other words, *w* raises the valuations of elements at least  $\ell$ , and exactly  $\ell$  if and only if such a valuation is not divisible by *p*.

$$\mathfrak{A}_{\theta} = \{ h \in H \, | \, h \cdot \theta \in \mathcal{O}_L \}.$$

$$\mathfrak{A}_{\theta} = \{ h \in H \, | \, h \cdot \theta \in \mathcal{O}_L \}.$$

 $\mathfrak{A}_{L/K} \subseteq \mathfrak{A}_{\theta}$  and  $\mathfrak{A}_{\theta}$  is an  $\mathfrak{A}_{L/K}$ -fractional ideal.

$$\mathfrak{A}_{\theta} = \{h \in H \,|\, h \cdot \theta \in \mathcal{O}_L\}.$$

 $\mathfrak{A}_{L/K} \subseteq \mathfrak{A}_{\theta}$  and  $\mathfrak{A}_{\theta}$  is an  $\mathfrak{A}_{L/K}$ -fractional ideal.

# Proposition

The following statements are equivalent:

•  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

• 
$$\mathfrak{A}_{L/K} = \mathfrak{A}_{ heta}$$
 for some  $heta \in \mathcal{O}_L$ .

•  $\mathfrak{A}_{\theta}$  is a principal  $\mathfrak{A}_{L/K}$ -fractional ideal for some (any)  $\theta \in \mathcal{O}_L$ .

$$\mathfrak{A}_{\theta} = \{h \in H \,|\, h \cdot \theta \in \mathcal{O}_L\}.$$

 $\mathfrak{A}_{L/K} \subseteq \mathfrak{A}_{\theta}$  and  $\mathfrak{A}_{\theta}$  is an  $\mathfrak{A}_{L/K}$ -fractional ideal.

# Proposition

The following statements are equivalent:

• 
$$\mathcal{O}_L$$
 is  $\mathfrak{A}_{L/K}$ -free.

• 
$$\mathfrak{A}_{L/K} = \mathfrak{A}_{ heta}$$
 for some  $heta \in \mathcal{O}_L$ .

•  $\mathfrak{A}_{\theta}$  is a principal  $\mathfrak{A}_{L/K}$ -fractional ideal for some (any)  $\theta \in \mathcal{O}_L$ .

Thanks to *w*, we can find  $\mathcal{O}_{\mathcal{K}}$ -bases of  $\mathfrak{A}_{L/\mathcal{K}}$  and  $\mathfrak{A}_{\theta}$  with  $\theta = \pi_{L}^{a}$ .

This is the scaffolds part.

This is the *scaffolds* part.

Roughly speaking, a scaffold on L/K consists in families of elements  $\Psi_i \in H$  and  $\lambda_j \in L$  such that the elements  $\Psi_i \cdot \lambda_j$  have a prescribed valuation depending on *i* and *j* up to a certain precision c.

This is the *scaffolds* part.

Roughly speaking, a scaffold on L/K consists in families of elements  $\Psi_i \in H$  and  $\lambda_j \in L$  such that the elements  $\Psi_i \cdot \lambda_j$  have a prescribed valuation depending on *i* and *j* up to a certain precision  $\mathfrak{c}$ .

If the precision is high enough, we obtain conditions for freeness.

This is the *scaffolds* part.

Roughly speaking, a scaffold on L/K consists in families of elements  $\Psi_i \in H$  and  $\lambda_j \in L$  such that the elements  $\Psi_i \cdot \lambda_j$  have a prescribed valuation depending on *i* and *j* up to a certain precision c.

If the precision is high enough, we obtain conditions for freeness.

- Weak requirement ~> Sufficient condition for freeness.
- Strong requirement → Necessary and sufficient condition for freeness.

$$\mathfrak{c}=\frac{p-1}{r}\Big(\frac{rpe}{p-1}-t\Big).$$

$$\mathfrak{c}=\frac{p-1}{r}\Big(\frac{rpe}{p-1}-t\Big).$$

- Weak requirement:  $\mathfrak{c} \geq a$ .
- Strong requirement: c > a.
- Condition:  $\mathfrak{A}_{L/K} = \mathfrak{A}_{\theta}, \ \theta = \pi_L^a \iff a \mid p-1$ ).

$$\mathfrak{c}=\frac{p-1}{r}\Big(\frac{rpe}{p-1}-t\Big).$$

- Weak requirement:  $c \ge a$ .
- Strong requirement: c > a.
- Condition:  $\mathfrak{A}_{L/K} = \mathfrak{A}_{\theta}, \ \theta = \pi_L^a \iff a \mid p-1$ ).

Let  $a_0$  be the integer part of  $\frac{\ell}{p}$  and denote

$$\nu_{p-1}=a+(p-1)a_0.$$

$$\mathfrak{c}=\frac{p-1}{r}\Big(\frac{rpe}{p-1}-t\Big).$$

- Weak requirement:  $c \ge a$ .
- Strong requirement: c > a.
- Condition:  $\mathfrak{A}_{L/K} = \mathfrak{A}_{\theta}, \ \theta = \pi_L^a \iff a \mid p-1$ ).

Let  $a_0$  be the integer part of  $\frac{\ell}{p}$  and denote

$$\nu_{p-1}=a+(p-1)a_0.$$

We can rewrite

$$\mathfrak{c} = p\left(e + \frac{p-1}{r}(r-1)c - \nu_{p-1}\right) + a.$$

$$\mathfrak{c} = p\Big(e + \frac{p-1}{r}(r-1)c - \nu_{p-1}\Big) + a.$$

$$\mathfrak{c} = p\Big(e + rac{p-1}{r}(r-1)c - 
u_{p-1}\Big) + a.$$

Then the weak requirement  $c \ge a$  is always met, so  $a \mid p - 1 \Longrightarrow \mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

$$\mathfrak{c} = p\Big(e + rac{p-1}{r}(r-1)c - 
u_{p-1}\Big) + a.$$

Then the weak requirement  $c \ge a$  is always met, so  $a \mid p - 1 \Longrightarrow \mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

On the other hand, c > a holds if and only if  $e + \frac{p-1}{r}(r-1)c - \nu_{p-1} > 0$ .

$$\mathfrak{c} = p\Big(e + rac{p-1}{r}(r-1)c - 
u_{p-1}\Big) + a.$$

Then the weak requirement  $c \ge a$  is always met, so  $a \mid p-1 \Longrightarrow \mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

On the other hand, c > a holds if and only if  $e + \frac{p-1}{r}(r-1)c - \nu_{p-1} > 0.$ 

This is equivalent to  $t < \frac{rpe}{p-1} - r$ .

$$\mathfrak{c} = p\Big(e + rac{p-1}{r}(r-1)c - 
u_{p-1}\Big) + a.$$

Then the weak requirement  $c \ge a$  is always met, so  $a \mid p - 1 \Longrightarrow \mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

On the other hand, c > a holds if and only if  $e + \frac{p-1}{r}(r-1)c - \nu_{p-1} > 0.$ 

This is equivalent to  $t < \frac{rpe}{p-1} - r$ .

Therefore, when  $t < \frac{rpe}{p-1} - r$ ,  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free if and only if  $a \mid p-1$ .

This is the *continued fractions* part.

This is the continued fractions part.

For each  $\alpha \in \mathfrak{A}_{\theta}$  consider the map

$$\begin{array}{cccc} \psi_{\alpha} \colon & \mathfrak{A}_{L/K} & \longrightarrow & \mathfrak{A}_{\theta} \\ & \lambda & \longmapsto & \lambda \alpha \end{array}$$

This is the continued fractions part.

For each  $\alpha \in \mathfrak{A}_{\theta}$  consider the map

$$\begin{array}{cccc} \psi_{\alpha} \colon & \mathfrak{A}_{L/K} & \longrightarrow & \mathfrak{A}_{\theta} \\ & \lambda & \longmapsto & \lambda \alpha \end{array}$$

Let  $M(\alpha)$  be the matrix of  $\psi_{\alpha}$  with respect to the known bases of  $\mathfrak{A}_{L/K}$  and  $\mathfrak{A}_{\theta}$ .

This is the continued fractions part.

For each  $\alpha \in \mathfrak{A}_{\theta}$  consider the map

$$\psi_{lpha} \colon \mathfrak{A}_{L/K} \longrightarrow \mathfrak{A}_{ heta}$$
  
 $\lambda \longmapsto \lambda lpha$ 

Let  $M(\alpha)$  be the matrix of  $\psi_{\alpha}$  with respect to the known bases of  $\mathfrak{A}_{L/K}$  and  $\mathfrak{A}_{\theta}$ .

Then  $\mathfrak{A}_{\theta}$  is  $\mathfrak{A}_{L/K}$ -principal if and only if  $\det(M(\alpha)) \not\equiv 0 \pmod{\mathfrak{p}_K}$  for some  $\alpha \in \mathfrak{A}_{\theta}$ .

$$E = \Big\{ h \in \mathbb{Z} \mid 1 \le h < p, \ 1 \le h' < h \Longrightarrow \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \Big\},\$$

which is parametrized in terms of the continued fraction expansion of  $\frac{\ell}{\rho}$ .

$$E = \Big\{ h \in \mathbb{Z} \mid 1 \le h < p, \ 1 \le h' < h \implies \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \Big\},\$$

which is parametrized in terms of the continued fraction expansion of  $\frac{\ell}{\rho}$ .

Let *n* be the length of the continued fraction expansion of  $\frac{\ell}{\rho}$ .

$$E = \Big\{ h \in \mathbb{Z} \mid 1 \le h < p, \ 1 \le h' < h \implies \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \Big\},\$$

which is parametrized in terms of the continued fraction expansion of  $\frac{\ell}{\rho}$ .

Let *n* be the length of the continued fraction expansion of  $\frac{\ell}{p}$ .

• If  $n \leq 2$ , then  $a \mid p - 1$  and we already know that  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

$$E = \Big\{ h \in \mathbb{Z} \mid 1 \le h < p, \ 1 \le h' < h \implies \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \Big\},\$$

which is parametrized in terms of the continued fraction expansion of  $\frac{\ell}{\rho}$ .

Let *n* be the length of the continued fraction expansion of  $\frac{\ell}{p}$ .

- If  $n \leq 2$ , then  $a \mid p 1$  and we already know that  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.
- If n ∈ {3,4}, we construct an α for which det(M(α)) ≠ 0 (mod p<sub>K</sub>), so O<sub>L</sub> is 𝔄<sub>L/K</sub>-free.

$$E = \Big\{ h \in \mathbb{Z} \mid 1 \le h < p, \ 1 \le h' < h \implies \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \Big\},\$$

which is parametrized in terms of the continued fraction expansion of  $\frac{\ell}{\rho}$ .

Let *n* be the length of the continued fraction expansion of  $\frac{\ell}{p}$ .

- If  $n \leq 2$ , then  $a \mid p 1$  and we already know that  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.
- If n ∈ {3,4}, we construct an α for which det(M(α)) ≠ 0 (mod p<sub>K</sub>), so O<sub>L</sub> is 𝔄<sub>L/K</sub>-free.
- If  $n \ge 5$ , we prove that  $det(M(\alpha)) \equiv 0 \pmod{\mathfrak{p}_K}$  for all  $\alpha \in \mathfrak{A}_{\theta}$ , so  $\mathcal{O}_L$  is not  $\mathfrak{A}_{L/K}$ -free.
#### Proposition

If  $G \cong C_p$  or  $D_p$  and e = 1, then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

This does not necessarily hold in the general case.

### Proposition

If 
$$G \cong C_p$$
 or  $D_p$  and  $e = 1$ , then  $\mathcal{O}_L$  is  $\mathfrak{A}_{L/K}$ -free.

This does not necessarily hold in the general case.

### Example

Let L/K be a typical degree p extension with p = 13, e = 1, r = 12 and t = 5. Then c = 5 and  $\ell = 60$ . Now,

$$\frac{\ell}{\rho} = \frac{60}{13} = [4; 1, 1, 1, 1, 2].$$

Then n = 5 and  $\mathcal{O}_L$  is not  $\mathfrak{A}_{L/K}$ -free.

## Bibliography

- F. Bertrandias, M. J. Ferton; Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local (I), C.R. Acad. Sc. 18 Vol. 274 (1972), 1388-1391.
- F. Bertrandias, J. P. Bertrandias, M. J. Ferton; Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local (II), C.R. Acad. Sc. 18 Vol. 274 (1972), 1388-1391.
- N. Byott, L. Childs, G. Elder; Scaffolds and generalized integral Galois module structure, Ann. Inst. Fourier 68 Vol. 3 (2018), 965-1010.
- L.N. Childs; Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, Mathematical Surveys and Monographs 80, American Mathematical Society, 2000.

- I. Del Corso, F. Ferri, D. Lombardo; How far is an extension of p-adic fields from having a normal integral basis?, Journal of Number Theory, Vol. 233 (2022), 158-197.
- G. Elder; *Ramified extensions of degree p and their Hopf-Galois module structure* J. Théor. Nr. Bordx. 1 (2018), 19-40.
- M. J. Ferton; Sur l'anneau des entiers d'extensions cycliques de degré p et d'extensions diédrales de degré 2p d'un corps local, PhD thesis, University of Grenoble, 1972.
- D. Gil-Muñoz; The ring of integers of Hopf-Galois degree p extensions of p-adic fields with dihedral normal closure, J. Number Theory 245 (2023), 65-118.
- D. Gil-Muñoz; *Hopf-Galois module structure of degree p extensions of p-adic fields,* Preprint (2024).

# Thank you for your attention