# Hopf-Galois module structure of degree $p$ extensions of $p$-adic fields

Daniel Gil Muñoz

Charles University in Prague
Department of Algebra

Omaha, May 2022

# Table of contents

# Table of contents

# Preliminaries

Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.

# Preliminaries

Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ \Big| \, G & & \Big| \, \mathcal{O}_K[G] \\ K & \text{———} & \mathcal{O}_K \end{array}$$

# Preliminaries

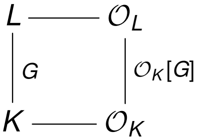
Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ \Big| G & & \Big| \mathcal{O}_K[G] \\ K & \text{———} & \mathcal{O}_K \end{array}$$

**Noether's theorem**: $\mathcal{O}_L$ $\mathcal{O}_K[G]$-free if and only if $L/K$ is tamely ramified.

# Preliminaries

Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.

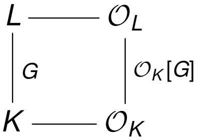



**Noether's theorem**: $\mathcal{O}_L$ $\mathcal{O}_K[G]$-free if and only if $L/K$ is tamely ramified.

In affirmative case, $L/K$ posseses a normal integral basis.

# Preliminaries

Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.




**Noether's theorem**: $\mathcal{O}_L$ $\mathcal{O}_K[G]$-free if and only if $L/K$ is tamely ramified.

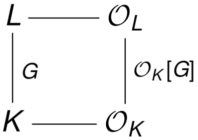
In affirmative case, $L/K$ posseses a normal integral basis.

More generally, if $L/K$ is $H$-Galois, one can ask for the freeness of $\mathcal{O}_L$ over its **associated order** in $H$

$$\mathfrak{A}_H = \{\lambda \in H \,|\, \lambda \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

# Preliminaries

Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.




**Noether's theorem**: $\mathcal{O}_L$ $\mathcal{O}_K[G]$-free if and only if $L/K$ is tamely ramified.

In affirmative case, $L/K$ posseses a normal integral basis.

More generally, if $L/K$ is $H$-Galois, one can ask for the freeness of $\mathcal{O}_L$ over its **associated order** in $H$

$$\mathfrak{A}_H = \{\lambda \in H \,|\, \lambda\mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

There is not a general answer.

# Preliminaries

Let $L/K$ be a Galois extension of $p$-adic fields, $G := \mathrm{Gal}(L/K)$.

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ \Big| G & & \Big| \mathcal{O}_K[G] \\ K & \text{———} & \mathcal{O}_K \end{array}$$

**Noether's theorem**: $\mathcal{O}_L$ $\mathcal{O}_K[G]$-free if and only if $L/K$ is tamely ramified.

In affirmative case, $L/K$ posseses a normal integral basis.

More generally, if $L/K$ is $H$-Galois, one can ask for the freeness of $\mathcal{O}_L$ over its **associated order** in $H$

$$\mathfrak{A}_H = \{\lambda \in H \,|\, \lambda\mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

There is not a general answer.

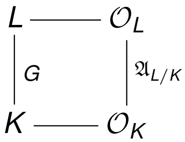
The study of this question is closely related with the **ramification** of $L/K$.

Let $L/K$ be a cyclic degree $p$ extension of $p$-adic fields.

Let $L/K$ be a cyclic degree $p$ extension of $p$-adic fields.

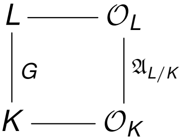
$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ \Big| {\scriptstyle G} & & \Big| {\scriptstyle \mathfrak{A}_{L/K}} \\ K & \text{———} & \mathcal{O}_K \end{array}$$

Let $L/K$ be a cyclic degree $p$ extension of $p$-adic fields.




Its unique Hopf-Galois structure is $K[G]$, where $G := \mathrm{Gal}(L/K) = \langle\sigma\rangle$.

Let $L/K$ be a cyclic degree $p$ extension of $p$-adic fields.




Its unique Hopf-Galois structure is $K[G]$, where $G := \mathrm{Gal}(L/K) = \langle \sigma \rangle$.

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

Let $L/K$ be a cyclic degree $p$ extension of $p$-adic fields.

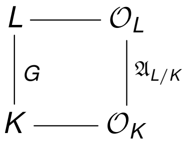
$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ \Big| \, G & & \Big| \, \mathfrak{A}_{L/K} \\ K & \text{———} & \mathcal{O}_K \end{array}$$

Its unique Hopf-Galois structure is $K[G]$, where $G := \mathrm{Gal}(L/K) = \langle \sigma \rangle$.

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

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

Let $L/K$ be a cyclic degree $p$ extension of $p$-adic fields.




Its unique Hopf-Galois structure is $K[G]$, where $G := \mathrm{Gal}(L/K) = \langle \sigma \rangle$.

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

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

Let $t$ be the ramification jump of $L/K$ and $e = e(K/\mathbb{Q}_p)$. Then

$$1 \leq t \leq \frac{pe}{p-1}.$$

**F. Bertrandias, J.P. Bertrandias, M.J. Ferton (1972)**:
Complete answer on the freeness of $\mathcal{O}_L$.

$$t = pa_0 + a, \quad 0 \leq a \leq p-1$$

**F. Bertrandias, J.P. Bertrandias, M.J. Ferton (1972)**:
Complete answer on the freeness of $\mathcal{O}_L$.

$$t = pa_0 + a, \quad 0 \leq a \leq p-1$$

- If $a = 0$, then $t = \frac{pe}{p-1}$ ($L/K$ is maximally ramified) and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

**F. Bertrandias, J.P. Bertrandias, M.J. Ferton (1972)**:
Complete answer on the freeness of $\mathcal{O}_L$.

$$t = pa_0 + a, \quad 0 \leq a \leq p-1$$

- If $a = 0$, then $t = \frac{pe}{p-1}$ ($L/K$ is maximally ramified) and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.
- If $a$ divides $p-1$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free. If in addition $t < \frac{pe}{p-1} - 1$, the converse holds.

**F. Bertrandias, J.P. Bertrandias, M.J. Ferton (1972)**:
Complete answer on the freeness of $\mathcal{O}_L$.

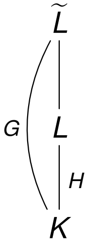
$$t = pa_0 + a, \quad 0 \leq a \leq p-1$$

- If $a = 0$, then $t = \frac{pe}{p-1}$ ($L/K$ is maximally ramified) and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.
- If $a$ divides $p-1$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free. If in addition $t < \frac{pe}{p-1} - 1$, the converse holds.
- If $t \geq \frac{pe}{p-1} - 1$ ($L/K$ is almost maximally ramified), $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $n \leq 4$, where

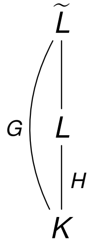
$$\frac{t}{p} = [a_0; a_1, \dots, a_n].$$

Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.

Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.

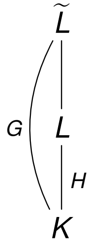


Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.




$$G = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1,\ \sigma\tau\sigma = \tau \rangle \cong D_p.$$

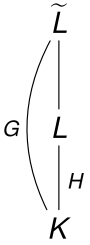
Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.




$$G = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1, \ \sigma\tau\sigma = \tau \rangle \cong D_p.$$

$$G = J \rtimes G', \ J = \langle \sigma \rangle, \ G' = \langle \tau \rangle.$$

Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.



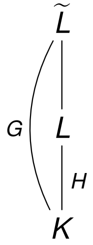

$$G = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1,\ \sigma\tau\sigma = \tau \rangle \cong D_p.$$

$$G = J \rtimes G',\ J = \langle \sigma \rangle,\ G' = \langle \tau \rangle.$$

By Byott uniqueness theorem, $L/K$ has a unique Hopf-Galois structure

$$H = \widetilde{L}[J]^G.$$

Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.




$$G = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1,\ \sigma\tau\sigma = \tau \rangle \cong D_p.$$

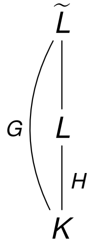
$$G = J \rtimes G',\ J = \langle \sigma \rangle,\ G' = \langle \tau \rangle.$$

By Byott uniqueness theorem, $L/K$ has a unique Hopf-Galois structure

$$H = \widetilde{L}[J]^G.$$

Associated order: $\mathfrak{A}_{L/K} = \{\lambda \in H \mid \lambda \mathcal{O}_L \subseteq \mathcal{O}_L\}$.

Let $L/K$ be a degree $p$ extension of $p$-adic fields with dihedral normal closure.




$$G = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1,\ \sigma\tau\sigma = \tau \rangle \cong D_p.$$

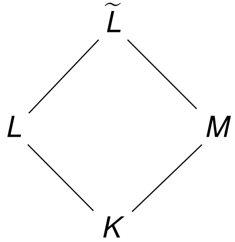
$$G = J \rtimes G',\ J = \langle \sigma \rangle,\ G' = \langle \tau \rangle.$$

By Byott uniqueness theorem, $L/K$ has a unique Hopf-Galois structure

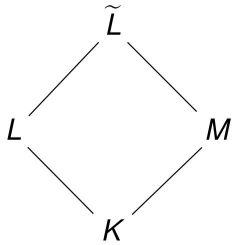
$$H = \widetilde{L}[J]^G.$$

Associated order: $\mathfrak{A}_{L/K} = \{\lambda \in H \mid \lambda \mathcal{O}_L \subseteq \mathcal{O}_L\}$.

We shall characterize the $\mathfrak{A}_{L/K}$-freeness of $\mathcal{O}_L$.

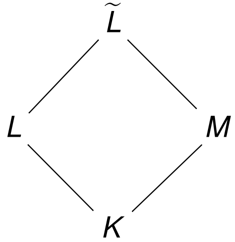



$\widetilde{L}/K$ has a unique quadratic subextension $M/K$. The extension $\widetilde{L}/M$ **is cyclic of degree** $p$.




$\widetilde{L}/K$ has a unique quadratic subextension $M/K$. The extension $\widetilde{L}/M$ **is cyclic of degree** $p$.

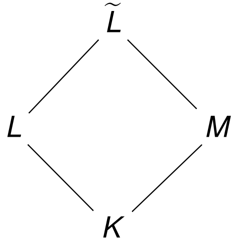
The extension $L/K$ is always totally ramified. Equivalently, $\widetilde{L}/K$ is totally ramified if and only if so is $M/K$.




$\widetilde{L}/K$ has a unique quadratic subextension $M/K$. The extension $\widetilde{L}/M$ **is cyclic of degree** $p$.

The extension $L/K$ is always totally ramified. Equivalently, $\widetilde{L}/K$ is totally ramified if and only if so is $M/K$.

If $M/K$ is unramified, $L/K$ and $M/K$ are **arithmetically disjoint**.




$\widetilde{L}/K$ has a unique quadratic subextension $M/K$. The extension $\widetilde{L}/M$ **is cyclic of degree $p$**.

The extension $L/K$ is always totally ramified. Equivalently, $\widetilde{L}/K$ is totally ramified if and only if so is $M/K$.

If $M/K$ is unramified, $L/K$ and $M/K$ are **arithmetically disjoint**.

### Corollary

*If $\widetilde{L}/K$ is not totally ramified, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $\mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free.*

Let $t$ be the ramification jump of $\widetilde{L}/K$. Then

$$1 \leq t \leq \frac{2pe}{p-1}.$$

Let $t$ be the ramification jump of $\widetilde{L}/K$. Then

$$1 \leq t \leq \frac{2pe}{p-1}.$$

In this situation, $t$ is an odd number. Call $\ell := \frac{p+t}{2}$ and write

$$\ell = pa_0 + a, \quad 0 \leq a \leq p-1.$$

Let $t$ be the ramification jump of $\widetilde{L}/K$. Then

$$1 \leq t \leq \frac{2pe}{p-1}.$$

In this situation, $t$ is an odd number. Call $\ell := \frac{p+t}{2}$ and write

$$\ell = pa_0 + a, \quad 0 \leq a \leq p-1.$$

We claim:

- If $a = 0$, then $t = \frac{2pe}{p-1}$ and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.
- If $a$ divides $p-1$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free. Moreover, if $t < \frac{2pe}{p-1} - 2$, the converse holds.
- If $t \geq \frac{2pe}{p-1} - 2$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $n \leq 4$, where

$$\frac{\ell}{p} = [a_0; a_1, \ldots, a_n].$$

Why $\ell = \frac{p+t}{2}$?

## Why $\ell = \frac{p+t}{2}$?

$$\begin{array}{c} L \\ \Big| \, G \\ K \\ \Big| \\ \mathbb{Q}_p \end{array}$$

**Cyclic case:** $G = \mathrm{Gal}(L/K) \cong C_p$

## Why $\ell = \frac{p+t}{2}$?

$$\begin{array}{c} L \\ \Big| G \\ K \\ \Big| \\ \mathbb{Q}_p \end{array}$$

**Cyclic case:** $G = \mathrm{Gal}(L/K) \cong C_p$

$G = \langle \sigma \rangle \Longrightarrow K[G] = K[f]$, $f = \sigma - 1$

Why $\ell = \frac{p+t}{2}$?


**Cyclic case:** $G = \mathrm{Gal}(L/K) \cong C_p$

$G = \langle \sigma \rangle \Longrightarrow K[G] = K[f]$, $f = \sigma - 1$

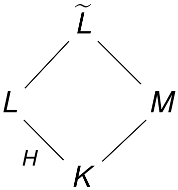
**Proposition:** $v_L(f \cdot x) \geq t + v_L(x)\ \forall x \in \mathcal{O}_L$, with equality $\iff p \nmid t$.

Why $\ell = \frac{p+t}{2}$?


**Cyclic case:** $G = \mathrm{Gal}(L/K) \cong C_p$

$G = \langle \sigma \rangle \Longrightarrow K[G] = K[f]$, $f = \sigma - 1$

**Proposition:** $v_L(f \cdot x) \geq t + v_L(x)\ \forall x \in \mathcal{O}_L$, with equality $\Longleftrightarrow p \nmid t$.



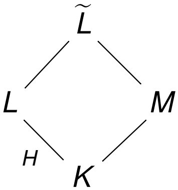

**Hopf-Galois case:** $G = \mathrm{Gal}(\widetilde{L}/K) \cong D_p$

Why $\ell = \frac{p+t}{2}$?


**Cyclic case:** $G = \mathrm{Gal}(L/K) \cong C_p$

$G = \langle \sigma \rangle \implies K[G] = K[f]$, $f = \sigma - 1$

**Proposition:** $v_L(f \cdot x) \geq t + v_L(x)\ \forall x \in \mathcal{O}_L$, with equality $\iff p \nmid t$.




**Hopf-Galois case:** $G = \mathrm{Gal}(\widetilde{L}/K) \cong D_p$

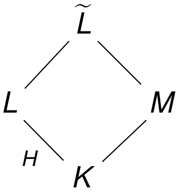
$\mathcal{O}_M = \mathcal{O}_K[z] \implies$
$H = K[w]$, $w = z(\sigma - \sigma^{-1})$

Why $\ell = \frac{p+t}{2}$?


**Cyclic case:** $G = \mathrm{Gal}(L/K) \cong C_p$

$G = \langle \sigma \rangle \Longrightarrow K[G] = K[f]$, $f = \sigma - 1$

**Proposition:** $v_L(f \cdot x) \geq t + v_L(x)\ \forall x \in \mathcal{O}_L$, with equality $\Longleftrightarrow p \nmid t$.




**Hopf-Galois case:** $G = \mathrm{Gal}(\widetilde{L}/K) \cong D_p$

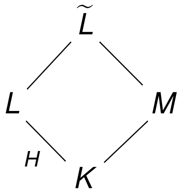
$\mathcal{O}_M = \mathcal{O}_K[z] \Longrightarrow$
$H = K[w]$, $w = z(\sigma - \sigma^{-1})$

**Proposition:** $v_L(w \cdot x) \geq \ell + v_L(x)\ \forall x \in \mathcal{O}_L$, with equality $\Longleftrightarrow p \nmid t$.

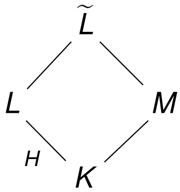
# Table of contents

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

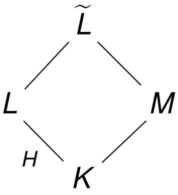


$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.




We assume that $a = 0$, so $t = \frac{2pe}{p-1}$.

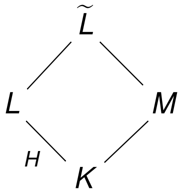
$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.




We assume that $a = 0$, so $t = \frac{2pe}{p-1}$.

- $M$ contains a primitive $p$-th root of unity $\xi$.
- There is $\gamma \in \widetilde{L}$ with $v_{\widetilde{L}}(\gamma) = 1$ such that $\gamma^p \in \mathcal{O}_M$.
- $\sigma(\gamma^j) = \xi^j \gamma^j$ for every $0 \leq j \leq p-1$.

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

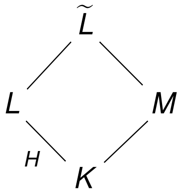



We assume that $a = 0$, so $t = \frac{2pe}{p-1}$.

- $M$ contains a primitive $p$-th root of unity $\xi$.
- There is $\gamma \in \widetilde{L}$ with $v_{\widetilde{L}}(\gamma) = 1$ such that $\gamma^p \in \mathcal{O}_M$.
- $\sigma(\gamma^j) = \xi^j \gamma^j$ for every $0 \leq j \leq p - 1$.

Let us define $\alpha = \gamma\tau(\gamma)$.

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.




We assume that $a = 0$, so $t = \frac{2pe}{p-1}$.

- $M$ contains a primitive $p$-th root of unity $\xi$.
- There is $\gamma \in \widetilde{L}$ with $v_{\widetilde{L}}(\gamma) = 1$ such that $\gamma^p \in \mathcal{O}_M$.
- $\sigma(\gamma^j) = \xi^j \gamma^j$ for every $0 \leq j \leq p-1$.

Let us define $\alpha = \gamma\tau(\gamma)$. Then:

- $v_L(\alpha) = 1$ and $\alpha^p \in \mathcal{O}_K$.
- $w \cdot \alpha^j = \lambda_j \alpha^j$ for every $0 \leq j \leq p-1$.
- $\lambda_j \in K$ for every $0 \leq j \leq p-1$.

- $v_L(\alpha) = 1$ and $\alpha^p \in \mathcal{O}_K$.
- $w \cdot \alpha^j = \lambda_j \alpha^j$ for every $0 \leq j \leq p-1$.
- $\lambda_j \in K$ for every $0 \leq j \leq p-1$.

- $v_L(\alpha) = 1$ and $\alpha^p \in \mathcal{O}_K$.
- $w \cdot \alpha^j = \lambda_j \alpha^j$ for every $0 \leq j \leq p-1$.
- $\lambda_j \in K$ for every $0 \leq j \leq p-1$.

We find $\{v_i\}_{i=0}^{p-1}$ $\mathcal{O}_K$-basis of $\mathfrak{A}_{L/K}$ such that

$$v_i \cdot \alpha^j = \delta_{ij} \alpha^j.$$

- $v_L(\alpha) = 1$ and $\alpha^p \in \mathcal{O}_K$.
- $w \cdot \alpha^j = \lambda_j \alpha^j$ for every $0 \leq j \leq p-1$.
- $\lambda_j \in K$ for every $0 \leq j \leq p-1$.

We find $\{v_i\}_{i=0}^{p-1}$ $\mathcal{O}_K$-basis of $\mathfrak{A}_{L/K}$ such that

$$v_i \cdot \alpha^j = \delta_{ij} \alpha^j.$$

Hence they are primitive pairwise orthogonal idempotents of $H$.

- $v_L(\alpha) = 1$ and $\alpha^p \in \mathcal{O}_K$.
- $w \cdot \alpha^j = \lambda_j \alpha^j$ for every $0 \leq j \leq p-1$.
- $\lambda_j \in K$ for every $0 \leq j \leq p-1$.

We find $\{v_i\}_{i=0}^{p-1}$ $\mathcal{O}_K$-basis of $\mathfrak{A}_{L/K}$ such that

$$v_i \cdot \alpha^j = \delta_{ij} \alpha^j.$$

Hence they are primitive pairwise orthogonal idempotents of $H$.

$$\begin{array}{rccl} \varphi\colon & H & \longrightarrow & K^p, \\ & v_i & \longmapsto & e_i := (\delta_{ij})_{j=0}^{p-1}. \end{array}$$

is an isomorphism of $K$-algebras.

- $v_L(\alpha) = 1$ and $\alpha^p \in \mathcal{O}_K$.
- $w \cdot \alpha^j = \lambda_j \alpha^j$ for every $0 \leq j \leq p-1$.
- $\lambda_j \in K$ for every $0 \leq j \leq p-1$.

We find $\{v_i\}_{i=0}^{p-1}$ $\mathcal{O}_K$-basis of $\mathfrak{A}_{L/K}$ such that

$$v_i \cdot \alpha^j = \delta_{ij} \alpha^j.$$

Hence they are primitive pairwise orthogonal idempotents of $H$.

$$\begin{array}{rccc} \varphi\colon & H & \longrightarrow & K^p, \\ & v_i & \longmapsto & e_i := (\delta_{ij})_{j=0}^{p-1}. \end{array}$$

is an isomorphism of $K$-algebras.

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

# The lattice $\mathfrak{A}_\theta$

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

# The lattice $\mathfrak{A}_\theta$

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

$$1 \leq t < \frac{2pe}{p-1}.$$

# The lattice $\mathfrak{A}_\theta$

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

$$1 \leq t < \frac{2pe}{p-1}.$$

If $L = H \cdot \theta$, we define

$$\mathfrak{A}_\theta := \{\lambda \in H \mid \lambda \cdot \theta \in \mathcal{O}_L\}.$$

# The lattice $\mathfrak{A}_\theta$

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

$$1 \leq t < \frac{2pe}{p-1}.$$

If $L = H \cdot \theta$, we define

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

- $\mathfrak{A}_\theta$ is an $\mathcal{O}_K$-lattice but not a ring in general.
- $\mathfrak{A}_{L/K} \subseteq \mathfrak{A}_\theta$ and $\mathfrak{A}_\theta$ is a fractional $\mathfrak{A}_{L/K}$-ideal.

# The lattice $\mathfrak{A}_\theta$

$L/K$ degree $p$ extension of $p$-adic fields with dihedral $\widetilde{L}$.

$$1 \leq t < \frac{2pe}{p-1}.$$

If $L = H \cdot \theta$, we define

$$\mathfrak{A}_\theta := \{\lambda \in H \mid \lambda \cdot \theta \in \mathcal{O}_L\}.$$

- $\mathfrak{A}_\theta$ is an $\mathcal{O}_K$-lattice but not a ring in general.
- $\mathfrak{A}_{L/K} \subseteq \mathfrak{A}_\theta$ and $\mathfrak{A}_\theta$ is a fractional $\mathfrak{A}_{L/K}$-ideal.

Write $\ell = pa_0 + a$ and denote $\theta := \pi_L^a$.

# Basis of $\mathfrak{A}_\theta$

## Proposition

*The lattice $\mathfrak{A}_\theta$ has $\mathcal{O}_K$-basis*

$$\{\pi_K^{-\nu_i} w^i\}_{i=0}^{p-1},$$

*where for each $0 \leq i \leq p-1$,*

$$\nu_i = \left\lfloor \frac{a + i\ell}{p} \right\rfloor = ia_0 + \left\lfloor (i+1)\frac{a}{p} \right\rfloor.$$

# Basis of $\mathfrak{A}_\theta$

## Proposition

*The lattice $\mathfrak{A}_\theta$ has $\mathcal{O}_K$-basis*

$$\{\pi_K^{-\nu_i} w^i\}_{i=0}^{p-1},$$

*where for each $0 \leq i \leq p-1$,*

$$\nu_i = \left\lfloor \frac{a + i\ell}{p} \right\rfloor = ia_0 + \left\lfloor (i+1)\frac{a}{p} \right\rfloor.$$

This is a direct consequence from the fact that

$$v_L(w^i \cdot \theta) = a + i\ell, \quad 0 \leq i \leq p-1.$$

# Basis for the associated order

## Theorem

*$\mathfrak{A}_{L/K}$ has $\mathcal{O}_K$-basis*

$$\{\pi_K^{-n_i} w^i\}_{i=0}^{p-1},$$

*where for each $0 \leq i \leq p-1$,*

$$n_i = \min_{0 \leq j \leq p-1-i}(\nu_{i+j} - \nu_j).$$

# Basis for the associated order

**Theorem**

*$\mathfrak{A}_{L/K}$ has $\mathcal{O}_K$-basis*

$$\{\pi_K^{-n_i} w^i\}_{i=0}^{p-1},$$

*where for each $0 \leq i \leq p-1$,*

$$n_i = \min_{0 \leq j \leq p-1-i}(\nu_{i+j} - \nu_j).$$

Note that $n_i \leq \nu_i$ for every $0 \leq i \leq p-1$. The equalities hold if and only if $\mathfrak{A}_\theta = \mathfrak{A}_{L/K}$.

# The sequence $\{\nu_i\}_{0 \leq i \leq p-1}$

Some properties of the numbers $\nu_i$:

# The sequence $\{\nu_i\}_{0 \leq i \leq p-1}$

Some properties of the numbers $\nu_i$:

- $\nu_{p-1} \leq e + \frac{p-1}{2}$.
- $\nu_{p-1} = e + \frac{p-1}{2}$ if and only if $t \geq \frac{2pe}{p-1} - 2$.
- $\nu_{k+2} - \nu_k \geq 1$ for every $0 \leq k \leq p-3$.

# The sequence $\{\nu_i\}_{0 \leq i \leq p-1}$

Some properties of the numbers $\nu_i$:

- $\nu_{p-1} \leq e + \frac{p-1}{2}$.
- $\nu_{p-1} = e + \frac{p-1}{2}$ if and only if $t \geq \frac{2pe}{p-1} - 2$.
- $\nu_{k+2} - \nu_k \geq 1$ for every $0 \leq k \leq p-3$.

Proof of the third one:

# The sequence $\{\nu_i\}_{0 \leq i \leq p-1}$

Some properties of the numbers $\nu_i$:

- $\nu_{p-1} \leq e + \frac{p-1}{2}$.
- $\nu_{p-1} = e + \frac{p-1}{2}$ if and only if $t \geq \frac{2pe}{p-1} - 2$.
- $\nu_{k+2} - \nu_k \geq 1$ for every $0 \leq k \leq p-3$.

Proof of the third one:

If $a_0 > 0$, it is trivial. If $a_0 = 0$,

$$a = \frac{p+t}{2} \geq \frac{p+1}{2} \implies 2a \geq p+1.$$

# The sequence $\{\nu_i\}_{0 \leq i \leq p-1}$

Some properties of the numbers $\nu_i$:

- $\nu_{p-1} \leq e + \frac{p-1}{2}$.
- $\nu_{p-1} = e + \frac{p-1}{2}$ if and only if $t \geq \frac{2pe}{p-1} - 2$.
- $\nu_{k+2} - \nu_k \geq 1$ for every $0 \leq k \leq p-3$.

Proof of the third one:

If $a_0 > 0$, it is trivial. If $a_0 = 0$,

$$a = \frac{p+t}{2} \geq \frac{p+1}{2} \implies 2a \geq p+1.$$

Then,

$$(k+3)\frac{a}{p} - (k+1)\frac{a}{p} = \frac{2a}{p} > 1 \implies \nu_{k+2} - \nu_k \geq 1$$

# Sufficient condition for freeness

Since $a \neq 0$, $L/K$ is typical in the language of Elder's 2018 paper.

# Sufficient condition for freeness

Since $a \neq 0$, $L/K$ is typical in the language of Elder's 2018 paper. Therefore it posseses a scaffold of precision

$$\mathfrak{c} = pe - \frac{p-1}{2}t = \frac{p-1}{2}\left(\frac{2pe}{p-1} - t\right) = p\left(e + \frac{p-1}{2} - \nu_{p-1}\right) + a.$$

# Sufficient condition for freeness

Since $a \neq 0$, $L/K$ is typical in the language of Elder's 2018 paper. Therefore it posseses a scaffold of precision

$$\mathfrak{c} = pe - \frac{p-1}{2}t = \frac{p-1}{2}\left(\frac{2pe}{p-1} - t\right)$$
$$= p\left(e + \frac{p-1}{2} - \nu_{p-1}\right) + a.$$

Weak condition: $\mathfrak{c} \geq a$.
Strong condition: $\mathfrak{c} > a$.

# Sufficient condition for freeness

Since $a \neq 0$, $L/K$ is typical in the language of Elder's 2018 paper. Therefore it posseses a scaffold of precision

$$\mathfrak{c} = pe - \frac{p-1}{2}t = \frac{p-1}{2}\left(\frac{2pe}{p-1} - t\right) = p\left(e + \frac{p-1}{2} - \nu_{p-1}\right) + a.$$

Weak condition: $\mathfrak{c} \geq a$.
Strong condition: $\mathfrak{c} > a$.

**Corollary**

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

Finally, we consider the cases in which

$$\frac{2pe}{p-1} - 2 \leq t \leq \frac{2pe}{p-1}.$$

Finally, we consider the cases in which

$$\frac{2pe}{p-1} - 2 \leq t \leq \frac{2pe}{p-1}.$$

Continued fraction expansion: $\frac{\ell}{p} = [a_0; a_1, \dots, a_n]$.

Finally, we consider the cases in which

$$\frac{2pe}{p-1} - 2 \leq t \leq \frac{2pe}{p-1}.$$

Continued fraction expansion: $\frac{\ell}{p} = [a_0; a_1, \dots, a_n]$.

For $0 \leq i \leq n$, the $i$-th convergent is $\frac{p_i}{q_i} = [a_0, \dots, a_i]$.

Finally, we consider the cases in which

$$\frac{2pe}{p-1} - 2 \leq t \leq \frac{2pe}{p-1}.$$

Continued fraction expansion: $\frac{\ell}{p} = [a_0; a_1, \dots, a_n]$.

For $0 \leq i \leq n$, the $i$-th convergent is $\frac{p_i}{q_i} = [a_0, \dots, a_i]$.

$q_0 = 1$, $q_1 = a_1$, $q_{i+2} = a_{i+2}q_{i+1} + q_i$.

Finally, we consider the cases in which

$$\frac{2pe}{p-1} - 2 \leq t \leq \frac{2pe}{p-1}.$$

Continued fraction expansion: $\frac{\ell}{p} = [a_0; a_1, \dots, a_n]$.

For $0 \leq i \leq n$, the $i$-th convergent is $\frac{p_i}{q_i} = [a_0, \dots, a_i]$.

$q_0 = 1$, $q_1 = a_1$, $q_{i+2} = a_{i+2}q_{i+1} + q_i$.

$\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free in the following (equivalent) cases:

- $n \leq 2$.
- $a = 0$ or $a \mid p - 1$.
- $\mathfrak{A}_\theta = \mathfrak{A}_{L/K}$.

Finally, we consider the cases in which

$$\frac{2pe}{p-1} - 2 \leq t \leq \frac{2pe}{p-1}.$$

Continued fraction expansion: $\frac{\ell}{p} = [a_0; a_1, \dots, a_n]$.

For $0 \leq i \leq n$, the $i$-th convergent is $\frac{p_i}{q_i} = [a_0, \dots, a_i]$.

$q_0 = 1$, $q_1 = a_1$, $q_{i+2} = a_{i+2}q_{i+1} + q_i$.

$\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free in the following (equivalent) cases:

- $n \leq 2$.
- $a = 0$ or $a \mid p - 1$.
- $\mathfrak{A}_\theta = \mathfrak{A}_{L/K}$.

Let us assume that $n \geq 3$.

# The strategy

For $\theta = \pi_L^a$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

# The strategy

For $\theta = \pi_L^a$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

We shall characterize when $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

# The strategy

For $\theta = \pi_L^a$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

We shall characterize when $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

For $\alpha \in \mathfrak{A}_\theta$, we consider the $\mathcal{O}_K$-linear map

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

Let $M(\alpha)$ be the matrix of $\psi_\alpha$ (w.r.t. the already known bases).

# The strategy

For $\theta = \pi_L^a$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

We shall characterize when $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

For $\alpha \in \mathfrak{A}_\theta$, we consider the $\mathcal{O}_K$-linear map

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

Let $M(\alpha)$ be the matrix of $\psi_\alpha$ (w.r.t. the already known bases).

$\alpha$ is an $\mathfrak{A}_{L/K}$-generator of $\mathfrak{A}_\theta$ if and only if

$$\det(M(\alpha)) \not\equiv 0 \pmod{\mathfrak{p}_K}.$$

# The strategy

For $\theta = \pi_L^a$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

We shall characterize when $\mathfrak{A}_\theta$ is $\mathfrak{A}_{L/K}$-principal.

For $\alpha \in \mathfrak{A}_\theta$, we consider the $\mathcal{O}_K$-linear map

$$\begin{array}{rccc} \psi_\alpha : & \mathfrak{A}_{L/K} & \longrightarrow & \mathfrak{A}_\theta, \\ & \lambda & \longmapsto & \lambda\alpha. \end{array}$$

Let $M(\alpha)$ be the matrix of $\psi_\alpha$ (w.r.t. the already known bases).

$\alpha$ is an $\mathfrak{A}_{L/K}$-generator of $\mathfrak{A}_\theta$ if and only if

$$\det(M(\alpha)) \not\equiv 0 \pmod{\mathfrak{p}_K}.$$

$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \Longrightarrow M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k)$.

$$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \implies M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k).$$

$$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \Longrightarrow M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k).$$

Denote $\overline{M(\pi_K^{-\nu_k} w^k)} = (\overline{\mu}_{j,i}^{(k)})_{j,i=0}^{p-1}$.

$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \Longrightarrow M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k)$.

Denote $\overline{M(\pi_K^{-\nu_k} w^k)} = (\overline{\mu}_{j,i}^{(k)})_{j,i=0}^{p-1}$.

We are interested in determining when $\overline{\mu}_{j,i}^{(k)} = 0$.

$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \implies M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k)$.

Denote $\overline{M(\pi_K^{-\nu_k} w^k)} = (\overline{\mu}_{j,i}^{(k)})_{j,i=0}^{p-1}$.

We are interested in determining when $\overline{\mu}_{j,i}^{(k)} = 0$.

This is closely related with the set

$$E = \left\{ h \in \mathbb{Z} \,\middle|\, 1 \leq h < p,\, 1 \leq h' < h \implies \widehat{h'\frac{a}{p}} > \widehat{h\frac{a}{p}} \right\}.$$

$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \Longrightarrow M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k)$.

Denote $\overline{M(\pi_K^{-\nu_k} w^k)} = (\overline{\mu}_{j,i}^{(k)})_{j,i=0}^{p-1}$.

We are interested in determining when $\overline{\mu}_{j,i}^{(k)} = 0$.

This is closely related with the set

$$E = \left\{ h \in \mathbb{Z} \,\middle|\, 1 \leq h < p,\, 1 \leq h' < h \Longrightarrow \widehat{h'\frac{a}{p}} > \widehat{h\frac{a}{p}} \right\}.$$

$E$ is parametrized from the continued fraction expansion of $\frac{\ell}{p}$.

$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \Longrightarrow M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k)$.

Denote $\overline{M(\pi_K^{-\nu_k} w^k)} = (\overline{\mu}_{j,i}^{(k)})_{j,i=0}^{p-1}$.

We are interested in determining when $\overline{\mu}_{j,i}^{(k)} = 0$.

This is closely related with the set

$$E = \left\{ h \in \mathbb{Z} \,\middle|\, 1 \leq h < p,\, 1 \leq h' < h \Longrightarrow \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \right\}.$$

$E$ is parametrized from the continued fraction expansion of $\frac{\ell}{p}$.

$$E = \Big\{ a'_{2i+2} q_{2i+1} + q_{2i} \,|\, 0 \leq i < \frac{n-1}{2}, \\ 0 \leq a'_{2i+2} \leq a_{2i+2} \text{ or } a_{2i+2} - 1 \Big\}.$$

$\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k \implies M(\alpha) = \sum_{k=0}^{p-1} x_k M(\pi_K^{-\nu_k} w^k)$.

Denote $\overline{M(\pi_K^{-\nu_k} w^k)} = (\overline{\mu}_{j,i}^{(k)})_{j,i=0}^{p-1}$.

We are interested in determining when $\overline{\mu}_{j,i}^{(k)} = 0$.

This is closely related with the set

$$E = \left\{ h \in \mathbb{Z} \,\middle|\, 1 \leq h < p,\, 1 \leq h' < h \implies \widehat{h' \frac{a}{p}} > \widehat{h \frac{a}{p}} \right\}.$$

$E$ is parametrized from the continued fraction expansion of $\frac{\ell}{p}$.

$$E = \Big\{ a'_{2i+2} q_{2i+1} + q_{2i} \,|\, 0 \leq i < \frac{n-1}{2}, \quad 0 \leq a'_{2i+2} \leq a_{2i+2} \text{ or } a_{2i+2} - 1 \Big\}.$$

If $n = 3$, $E = \{q_0, q_1 + q_0, \ldots, (a_2 - 1) q_1 + q_0, q_2\}$.

The $\mu_{j,i}^{(k)}$ are defined by

$$\pi_K^{-\nu_k - n_i} w^{k+i} = \sum_{j=0}^{p-1} \mu_{j,i}^{(k)} \pi_K^{-\nu_j} w^j.$$

The $\mu_{j,i}^{(k)}$ are defined by

$$\pi_K^{-\nu_k - n_i} w^{k+i} = \sum_{j=0}^{p-1} \mu_{j,i}^{(k)} \pi_K^{-\nu_j} w^j.$$

Hence,

$$v_K(\mu_{j,i}^{(k)}) = v_K(C(w^j, w^{k+i})) + \nu_j - \nu_k - n_i,$$

where $C(w^j, w^{k+i})$ is the coefficient of $w^j$ in the expression of $w^{k+i}$.

For $0 \leq i \leq p-1$, we call $h = p - i$.

For $0 \leq i \leq p-1$, we call $h = p - i$.

Assume that $k + i \leq p - 1$.

For $0 \leq i \leq p-1$, we call $h = p - i$.

Assume that $k + i \leq p - 1$.

(1) If $j \neq k + i$, then $\overline{\mu}_{j,i}^{(k)} = 0$.

(2) If $h \notin E$,

$$\overline{\mu}_{k+i,i}^{(k)} = \begin{cases} 1 & \text{if } h = p \\ 1 & \text{if } \widehat{(k+1)\frac{a}{p}} < \widehat{h\frac{a}{p}} \\ 0 & \text{otherwise} \end{cases}$$

(3) If $h \in E$, $\overline{\mu}_{k+i,i}^{(k)} = 1$.

Assume that $k + i > p - 1$ and let $m = k + i - (p - 1)$.

Assume that $k+i > p-1$ and let $m = k+i-(p-1)$.

Call $d_m = \max\{d \in \mathbb{Z} \mid d \text{ even}, \nu_{m+d} = \nu_m + \frac{d}{2}\}$.

(1) If $j \not\equiv 2 \pmod{m}$, then $\overline{\mu}_{j,i}^{(k)} = 0$.

(2) If $m < p-1$ and $j < m$ or $j > m + d_m$, then $\overline{\mu}_{j,i}^{(k)} = 0$.

(3) If $h \notin E$ and $m \leq j \leq m + d_m$,

$$\begin{cases} \overline{\mu}_{j,i}^{(k)} \neq 0 & \text{if } \frac{a}{p} + \widehat{(k+1)}\frac{a}{p} < \widehat{h\frac{a}{p}}, \\ \overline{\mu}_{j,i}^{(k)} = 0 & \text{otherwise.} \end{cases}$$

(4) If $h \in E$ and $m \leq j \leq m + d_m$,

$$\begin{cases} \overline{\mu}_{j,i}^{(k)} \neq 0 & \text{if } \frac{a}{p} + \widehat{(k+1)}\frac{a}{p} < \widehat{h\frac{a}{p}} + 1, \\ \overline{\mu}_{j,i}^{(k)} = 0 & \text{otherwise.} \end{cases}$$

# Sufficiency

## Proposition

*If $n \leq 4$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

# Sufficiency

**Proposition**

*If $n \leq 4$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof:

# Sufficiency

**Proposition**

*If $n \leq 4$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Take $\alpha = u + \pi_K^{-\nu_k} w^k$, $k = q_2 - 1$, $u \in \mathcal{O}_K^*$.

# Sufficiency

## Proposition

*If $n \leq 4$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Take $\alpha = u + \pi_K^{-\nu_k} w^k$, $k = q_2 - 1$, $u \in \mathcal{O}_K^*$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

# Sufficiency

## Proposition

*If $n \leq 4$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Take $\alpha = u + \pi_K^{-\nu_k} w^k$, $k = q_2 - 1$, $u \in \mathcal{O}_K^*$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

$M(1)$ is diagonal; $\overline{\mu}_{i,i}^{(0)} = \begin{cases} 1 & \text{if } \nu_i = n_i, \\ 0 & \text{otherwise.} \end{cases}$

# Sufficiency

**Proposition**

*If $n \leq 4$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Take $\alpha = u + \pi_K^{-\nu_k} w^k$, $k = q_2 - 1$, $u \in \mathcal{O}_K^*$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

$M(1)$ is diagonal; $\overline{\mu}_{i,i}^{(0)} = \begin{cases} 1 & \text{if } \nu_i = n_i, \\ 0 & \text{otherwise.} \end{cases}$

Since $\mathfrak{A}_\theta \neq \mathfrak{A}_{L/K}$, $\nu_i \neq n_i$ for some $i$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

- $\overline{\det(M(\alpha))} = \overline{u}\det(M')$, $M' \in \mathcal{M}_{p-1}(\mathcal{O}_K/\mathfrak{p}_K)$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

- $\overline{\det(M(\alpha))} = \overline{u}\det(M'),\ M' \in \mathcal{M}_{p-1}(\mathcal{O}_K/\mathfrak{p}_K)$.
- $\overline{\mu}_{k+i,i}^{(k)} = 1$ for $1 \leq i \leq p-k-1$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

- $\overline{\det(M(\alpha))} = \overline{u}\det(M'),\ M' \in \mathcal{M}_{p-1}(\mathcal{O}_K/\mathfrak{p}_K)$.
- $\overline{\mu}_{k+i,i}^{(k)} = 1$ for $1 \leq i \leq p-k-1$.
- $\overline{\mu}_{k+i-(p-1),i}^{(k)} \neq 0$ for $p-k \leq i \leq p-1$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

- $\overline{\det(M(\alpha))} = \overline{u}\det(M')$, $M' \in \mathcal{M}_{p-1}(\mathcal{O}_K/\mathfrak{p}_K)$.
- $\overline{\mu}_{k+i,i}^{(k)} = 1$ for $1 \leq i \leq p-k-1$.
- $\overline{\mu}_{k+i-(p-1),i}^{(k)} \neq 0$ for $p-k \leq i \leq p-1$.

The only non-zero addend independent of $u$ is $b_0 = \prod_{i=p-k}^{p-1} \overline{\mu}_{k+i-(p-1),i}$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

- $\overline{\det(M(\alpha))} = \overline{u}\det(M'),\ M' \in \mathcal{M}_{p-1}(\mathcal{O}_K/\mathfrak{p}_K)$.
- $\overline{\mu}_{k+i,i}^{(k)} = 1$ for $1 \leq i \leq p-k-1$.
- $\overline{\mu}_{k+i-(p-1),i}^{(k)} \neq 0$ for $p-k \leq i \leq p-1$.

The only non-zero addend independent of $u$ is $b_0 = \prod_{i=p-k}^{p-1} \overline{\mu}_{k+i-(p-1),i}$.

$\Longrightarrow \overline{\det(M(\alpha))} = \overline{u}\overline{P(u)},\ P \in \mathcal{O}_K[x]$.

$$M(\alpha) = uM(1) + M(\pi_K^{-\nu_k} w^k).$$

The condition $n \leq 4$ allows us to control most of the entries of $M(\pi_K^{-\nu_k} w^k)$.

- $\overline{\det(M(\alpha))} = \overline{u}\det(M'),\ M' \in \mathcal{M}_{p-1}(\mathcal{O}_K/\mathfrak{p}_K)$.
- $\overline{\mu}_{k+i,i}^{(k)} = 1$ for $1 \leq i \leq p-k-1$.
- $\overline{\mu}_{k+i-(p-1),i}^{(k)} \neq 0$ for $p-k \leq i \leq p-1$.

The only non-zero addend independent of $u$ is $b_0 = \prod_{i=p-k}^{p-1} \overline{\mu}_{k+i-(p-1),i}$.

$\Longrightarrow \overline{\det(M(\alpha))} = \overline{u}\overline{P(u)},\ P \in \mathcal{O}_K[x]$.

$\deg(P) \leq p-2 \Longrightarrow \overline{\det(M(\alpha))} \neq 0$ for some $u$.

# Necessity

**Proposition**

*If $n \geq 5$, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.*

# Necessity

**Proposition**

*If $n \geq 5$, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof:

# Necessity

**Proposition**

*If $n \geq 5$, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Let $\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k$. Call $n = 2s+2$ or $2s+1$.

# Necessity

**Proposition**

*If $n \geq 5$, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Let $\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k$. Call $n = 2s+2$ or $2s+1$.

Consider the $i$-th column of $M(\alpha)$, where $h = p - i$ takes the values

$$h = 2q_{2s-2},$$
$$h = q_{2s-2} + a'_{2s} q_{2s-1} + q_{2s}, \quad 0 \leq a'_{2s} \leq a_{2s}.$$

# Necessity

**Proposition**

*If $n \geq 5$, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Let $\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k$. Call $n = 2s+2$ or $2s+1$.

Consider the $i$-th column of $M(\alpha)$, where $h = p - i$ takes the values

$$h = 2q_{2s-2},$$
$$h = q_{2s-2} + a'_{2s} q_{2s-1} + q_{2s}, \quad 0 \leq a'_{2s} \leq a_{2s}.$$

These are $a_{2s}+2$ columns have at most $a_{2s}+1$ non-zero elements allocated in the same rows.

# Necessity

**Proposition**

*If $n \geq 5$, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.*

Sketch of the proof: Let $\alpha = \sum_{k=0}^{p-1} x_k \pi_K^{-\nu_k} w^k$. Call $n = 2s + 2$ or $2s + 1$.

Consider the $i$-th column of $M(\alpha)$, where $h = p - i$ takes the values

$$h = 2q_{2s-2},$$
$$h = q_{2s-2} + a'_{2s} q_{2s-1} + q_{2s}, \quad 0 \leq a'_{2s} \leq a_{2s}.$$

These are $a_{2s} + 2$ columns have at most $a_{2s} + 1$ non-zero elements allocated in the same rows.

$$\implies \det(M(\alpha)) \equiv 0 \pmod{\mathfrak{p}_K}.$$

# Table of contents

## Proposition

*If $L/K$ is absolutely unramified (in particular, if $K = \mathbb{Q}_p$), then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

## Proposition

*If $L/K$ is absolutely unramified (in particular, if $K = \mathbb{Q}_p$), then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

$$1 \leq t \leq \frac{2p}{p-1} \quad \Longrightarrow \quad t = 1 \quad \text{or} \quad p = 3 \text{ and } t = 3.$$

## Proposition

*If $L/K$ is absolutely unramified (in particular, if $K = \mathbb{Q}_p$), then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

$$1 \leq t \leq \frac{2p}{p-1} \quad \Longrightarrow \quad t = 1 \quad \text{or} \quad p = 3 \text{ and } t = 3.$$

If $p = 3$ and $t = 3$, $L/K$ is maximally ramified.

### Proposition

*If $L/K$ is absolutely unramified (in particular, if $K = \mathbb{Q}_p$), then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

$$1 \leq t \leq \frac{2p}{p-1} \quad \Longrightarrow \quad t = 1 \quad \text{or} \quad p = 3 \text{ and } t = 3.$$

If $p = 3$ and $t = 3$, $L/K$ is maximally ramified.

If $t = 1$, then $t > \frac{2p}{p-1} - 2$ and $\ell = a = \frac{p+1}{2}$.

## Proposition

*If $L/K$ is absolutely unramified (in particular, if $K = \mathbb{Q}_p$), then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

$$1 \leq t \leq \frac{2p}{p-1} \implies t = 1 \quad \text{or} \quad p = 3 \text{ and } t = 3.$$

If $p = 3$ and $t = 3$, $L/K$ is maximally ramified.

If $t = 1$, then $t > \frac{2p}{p-1} - 2$ and $\ell = a = \frac{p+1}{2}$.

$\frac{\ell}{p} = \left[0; 1, 1, \frac{p-1}{2}\right] \implies \mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

## Proposition

*Let $M/K$ be a ramified quadratic extension of p-adic fields with $\xi_p \in M - K$ and assume that*

(a) $t = \frac{2pe}{p-1}$.

(b) $1 \leq t < \frac{2pe}{p-1}$, *t is coprime with p and t is odd.*

*Then there is some field extension $E$ of $M$ such that $E/K$ is a dihedral degree 2p extension and its ramification jump is $t$.*

**Proposition**

*Let $M/K$ be a ramified quadratic extension of p-adic fields with $\xi_p \in M - K$ and assume that*

(a) $t = \frac{2pe}{p-1}$.

(b) $1 \leq t < \frac{2pe}{p-1}$, *t is coprime with p and t is odd.*

*Then there is some field extension $E$ of $M$ such that $E/K$ is a dihedral degree 2p extension and its ramification jump is $t$.*

Given some ramification parameters, we may choose $L/K$.

**Example**

Assume that $p > 3$. There is some degree $p$ extension $L/K$ such that $\widetilde{L}/K$ is weakly ramified and $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

### Example

Assume that $p > 3$. There is some degree $p$ extension $L/K$ such that $\widetilde{L}/K$ is weakly ramified and $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $L/K$ be such that $t = 1$ and $e > 1$.

**Example**

Assume that $p > 3$. There is some degree $p$ extension $L/K$ such that $\widetilde{L}/K$ is weakly ramified and $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $L/K$ be such that $t = 1$ and $e > 1$.

$$\frac{2pe}{p-1} - 2 \geq \frac{4p}{p-1} - 2 > 1, \quad a = \frac{p+1}{2} \nmid p-1$$

### Example

Assume that $p > 3$. There is some degree $p$ extension $L/K$ such that $\widetilde{L}/K$ is weakly ramified and $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $L/K$ be such that $t = 1$ and $e > 1$.

$$\frac{2pe}{p-1} - 2 \geq \frac{4p}{p-1} - 2 > 1, \quad a = \frac{p+1}{2} \nmid p - 1$$

$\implies \mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

## Example

There is some degree $p$ extension $L/K$ of $p$-adic fields such that $\mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free but $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

## Example

There is some degree $p$ extension $L/K$ of $p$-adic fields such that $\mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free but $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $p = 13$ and choose $L/K$ with $t = 3$, $e = 2$.

**Example**

There is some degree $p$ extension $L/K$ of $p$-adic fields such that $\mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free but $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $p = 13$ and choose $L/K$ with $t = 3$, $e = 2$.

$3 \mid 12 \quad \Longrightarrow \quad \mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free.

## Example

There is some degree $p$ extension $L/K$ of $p$-adic fields such that $\mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free but $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $p = 13$ and choose $L/K$ with $t = 3$, $e = 2$.

$3 \mid 12 \quad \Longrightarrow \quad \mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free.

$3 > \frac{2pe}{p-1} - 2, \quad a = \ell = 8, \quad \frac{8}{13} = [0; 1, 1, 1, 1, 2]$

### Example

There is some degree $p$ extension $L/K$ of $p$-adic fields such that $\mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free but $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

Let $p = 13$ and choose $L/K$ with $t = 3$, $e = 2$.

$3 \mid 12 \quad \Longrightarrow \quad \mathcal{O}_{\widetilde{L}}$ is $\mathfrak{A}_{\widetilde{L}/M}$-free.

$3 > \frac{2pe}{p-1} - 2, \quad a = \ell = 8, \quad \frac{8}{13} = [0; 1, 1, 1, 1, 2]$

$\Longrightarrow \mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free.

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., Paris, No. 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., Paris, No. 18 Vol. 274 (1972), 1388-1391.

M. J. Ferton; *Sur l'anneau des entiers d'extensions cycliques de degré p et d'extensions diédrales de degré* 2*p d'un corps local,* PhD thesis, University of Grenoble, 1972.

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,* Journal de Thórie des Nombres de Bordeaux **30** (2018), 19-40.

D. Gil-Muñoz, A. Rio; *Induced Hopf-Galois structures and their Local Hopf-Galois modules,* Publications Matemàtiques **66** (2022), 99-128.

# Thank you for your attention