



# ANNALES

DE

# L'INSTITUT FOURIER

Jérémy LE BORGNE

**Optimisation du théorème d'Ax-Sen-Tate et application à un calcul de cohomologie galoisienne  $p$ -adique**

Tome 60, n° 3 (2010), p. 1105-1123.

[http://aif.cedram.org/item?id=AIF\\_2010\\_\\_60\\_3\\_1105\\_0](http://aif.cedram.org/item?id=AIF_2010__60_3_1105_0)

© Association des Annales de l'institut Fourier, 2010, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du  
Centre de diffusion des revues académiques de mathématiques  
<http://www.cedram.org/>*

# OPTIMISATION DU THÉORÈME D'AX-SEN-TATE ET APPLICATION À UN CALCUL DE COHOMOLOGIE GALOISIENNE $p$ -ADIQUE

par Jérémy LE BORGNE

---

RÉSUMÉ. — Soit  $K$  un corps  $p$ -adique,  $G$  son groupe de Galois absolu et  $v$  la valuation sur  $\mathbf{C}_p$ . Dans sa démonstration du théorème d'Ax-Sen-Tate, Ax montre que si pour un  $A \in \mathbf{R}$ ,  $x \in \mathbf{C}_p$  vérifie  $v(\sigma x - x) \geq A$  pour tout  $\sigma \in G$ , alors il existe  $y \in K$  tel que  $v(x - y) \geq A - c$ , avec  $c = p/(p - 1)^2$ . Ax se pose la question de l'optimalité de la constante  $c$ , que nous étudions ici. En utilisant l'extension de  $K$  engendrée par les racines  $p^m$ -es d'une uniformisante fixée de  $K$ , nous déterminons la constante optimale, ainsi que des informations supplémentaires sur les  $x \in \mathbf{C}_p$  tels que  $v(\sigma x - x) \geq A$  pour tout  $\sigma \in G$ , ce qui nous permet de donner une description du premier groupe de cohomologie de  $G$  à coefficients dans l'anneau des entiers de  $K$ .

ABSTRACT. — Let  $K$  be a  $p$ -adic field,  $G$  its absolute Galois group and  $v$  the valuation on  $\mathbf{C}_p$ . In his proof of the Ax-Sen-Tate theorem, Ax shows that if for some  $A \in \mathbf{R}$ ,  $x \in \mathbf{C}_p$  satisfies  $v(\sigma x - x) \geq A$  for all  $\sigma \in G$ , then there exists  $y \in K$  such that  $v(x - y) \geq A - c$ , with  $c = p/(p - 1)^2$ . Ax questions the optimality of the constant  $c$ , which we study here. Using the extension of  $K$  generated by  $p^m$ -th roots of a fixed uniformizer of  $K$ , we find the optimal constant and some more information about those elements in  $\mathbf{C}_p$  satisfying  $v(\sigma x - x) \geq A$  for all  $\sigma \in G$ , which allows us to give a description the first cohomology group of  $G$  with coefficients in the ring of integers of  $K$ .

## Introduction

Soit  $p$  un nombre premier,  $k$  un corps parfait de caractéristique  $p$ , et  $F = \text{Frac } \mathcal{O}_k$ . Soit  $K$  une extension finie totalement ramifiée de  $F$ . On note  $\mathcal{O}_K$  l'anneau des entiers de  $K$ ,  $\mathfrak{m}_K$  son unique idéal maximal, et  $\pi_K$  (ou  $\pi$  s'il n'y a pas de confusion possible) une uniformisante de  $K$ . L'indice

---

*Mots-clés* : constante, optimalité, Ax-Sen-Tate, cohomologie galoisienne,  $p$ -adique, ramification, suite twist-récurrente.

*Classification math.* : 11S15, 11S25.

de ramification de  $K$  sur  $F$  est noté  $e$  (c'est le degré de  $K$  sur  $F$ ). Enfin, on note  $\bar{K}$  une clôture algébrique de  $K$ , et  $C$  le complété de  $\bar{K}$ , auquel on étend la valuation de  $F$  notée  $v$ , et normalisée par  $v(p) = 1$ . Le théorème d'Ax-Sen-Tate dit que les points fixes de  $C$  sous l'action de  $G = \text{Gal}(\bar{K}/K)$  sont exactement les éléments de  $K$ . La démonstration d'Ax (voir [1]) de ce théorème s'appuie sur le résultat suivant :

**THÉORÈME (Ax).** — *Soit  $x \in C$  et  $A \in \mathbb{R}$ . On suppose que pour tout  $\sigma \in G$ ,  $v(\sigma x - x) \geq A$ . Alors, il existe  $y \in K$  tel que  $v(x - y) \geq A - \frac{p}{(p-1)^2}$ .*

Ax pose sans y répondre la question de l'optimalité de la constante  $\frac{p}{(p-1)^2}$  intervenant dans le théorème précédent, en précisant qu'une borne inférieure pour cette constante optimale est effectivement  $\frac{1}{p-1}$ . Pour traiter cette question nous introduisons ici la tour d'extensions de  $K$  par les racines  $p^m$ -ièmes de l'uniformisante  $\pi$  de  $K$  :  $\pi_0 = \pi$ ,  $\pi_{m+1}^p = \pi_m$  et  $K_m = K(\pi_m)$  pour tout  $m \geq 0$ , et  $K_\infty = \cup_{m \geq 0} K_m$ . La première partie est consacrée à l'étude de l'extension  $K_\infty/K$ . Dans sa démonstration du théorème d'Ax-Sen-Tate (voir [10]), Tate présente des calculs de la cohomologie galoisienne à coefficients dans l'extension cyclotomique de  $K$ . Dans cet article, nous démontrons des résultats du même type lorsque  $K_\infty$  est une extension infinie, arithmétiquement profinie (APF) de  $K$  (intervenant dans les travaux de Fontaine et Wintenberger sur la théorie du corps des normes, voir [11]). Ces résultats s'appliquent à l'extension  $K_\infty$ , et une étude *ad hoc* de l'extension  $K_\infty/K$ , qui constitue la partie essentiellement originale de cet article, nous permettra de démontrer le :

**THÉORÈME (Théorème 1.7).** — *Soit  $x \in C$  et  $A \in \mathbb{R}$ . Si on suppose que pour tout  $\sigma \in G$ ,  $v(\sigma x - x) \geq A$ , alors, pour tout  $m \in \mathbb{N}$ , il existe  $y_m \in K_m$  tel que  $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$ . Réciproquement, si pour tout  $m \in \mathbb{N}$  il existe  $y_m \in K_m$  tel que  $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$ , alors pour tout  $\sigma \in G$ ,  $v(\sigma x - x) \geq A$ .*

Le cas particulier où  $m = 0$  implique que la constante optimale dans le théorème d'Ax est  $\frac{1}{p-1}$ . Le cas  $m = 1$  est utilisé par Caruso (voir [3], théorème 3.5.4) pour prouver une formule de réciprocité explicite entre un  $(\varphi, N)$ -module filtré de torsion et la  $\mathbb{F}_p$ -représentation de  $G$  associée ; la version d'Ax du théorème, et même le cas  $m = 0$  de notre théorème 1.7, s'avèrent insuffisants pour l'utilisation faite par Caruso dans le cas général.

La caractérisation donnée par le théorème nous permet en outre de décrire la structure de  $H^1(G, \mathcal{O}_{\bar{K}})$ . La deuxième partie est dédiée à cette étude. Nous redémontrons notamment un résultat dû à Sen (voir [8], théorème 3) qui dit que si l'entier  $n$  vérifie  $n \geq \frac{e}{p-1}$ , alors  $H^1(G, \mathcal{O}_{\bar{K}})$  est tué

par  $\pi_K^n$ . Dans le cas où  $K = F$ , on montre que  $H^1(G, \mathcal{O}_{\bar{K}})$  est isomorphe au sous-espace de  $k^{\mathbb{N}}$  formée des suites vérifiant une relation de récurrence linéaire tordue par le Frobenius, introduites sous le nom de suites *twist-récurrentes* par Kedlaya dans le but de donner une description de  $\bar{K}$ . On donne finalement quelques indications pour obtenir une description analogue dans le cas ramifié, qui pourrait être le point de départ à un analogue en torsion de la théorie de Sen.

## 1. Optimisation du théorème d'Ax

Nous démontrons dans cette partie le théorème 1.7 de l'introduction. Nous introduisons l'extension de  $K$  engendrée par les racines d'ordre une puissance de  $p$  de  $\pi$ , que nous étudions à l'aide de la théorie des extensions APF. Nous étudions en détail les propriétés de  $K_\infty$ , et nous en déduisons une caractérisation des éléments de  $K_\infty$  vérifiant une condition du type « Pour tout  $\sigma \in G$ ,  $v(\sigma x - x) \geq A$  ».

### 1.1. Extensions APF

Soit  $K_\infty$  une extension infinie, arithmétiquement profinie (APF) (cf. [11], §1) de  $K$ . On se propose dans cette partie de décrire la cohomologie de  $\text{Gal}(\bar{K}/K_\infty)$  à coefficients dans  $C$ , en cherchant à généraliser les résultats de [10] concernant l'extension cyclotomique de  $K$ . On utilise la numérotation supérieure des groupes de ramification, comme défini dans [9], chap. IV. Pour  $\mu \geq -1$ , si  $M$  est une extension finie de  $K$ , on pose

$$M^\mu = M \cap \bar{K}^{\text{Gal}(\bar{K}/K)^\mu}.$$

Si  $e$  désigne l'indice de ramification absolu de  $K$ , on sait d'après [4], proposition 3.22, que

$$v(\mathfrak{d}_{M/K}) = \frac{1}{e} \int_{-1}^{+\infty} \left( 1 - \frac{1}{[M : M^\mu]} \right) d\mu.$$

**PROPOSITION 1.1.** — Soit  $L_\infty$  une extension galoisienne finie de  $K_\infty$ . Alors  $\text{Tr}_{L_\infty/K_\infty}(\mathcal{O}_{L_\infty}) \supset \mathfrak{m}_{K_\infty}$ .

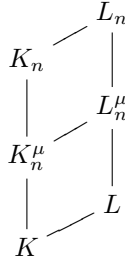
*Démonstration.* — Suivant [11] §1, nous définissons comme dans *loc. cit.* la suite  $\mu_n$  comme la suite strictement croissante des  $\mu \in \mathbb{R}_+$  tels que pour tout  $\varepsilon > 0$ ,

$$(1.1) \quad \text{Gal}(\bar{K}/K)^\mu \text{Gal}(\bar{K}/K_\infty) \neq \text{Gal}(\bar{K}/K)^{\mu+\varepsilon} \text{Gal}(\bar{K}/K_\infty),$$

et nous notons  $(K_n)_{n \in \mathbb{N}}$  la tour des extensions élémentaires de  $K_\infty$  définie comme dans [11] :  $K_n$  est le sous-corps de  $K_\infty$  fixé par

$$\text{Gal}(\bar{K}/K)^{\mu_n} \text{Gal}(\bar{K}/K_\infty).$$

Quitte à remplacer  $K$  par l'un des  $K_n$ , on sait d'après [9], Chap V, §4, Lemme 6, qu'il existe une extension  $L$  de  $K$  linéairement disjointe de  $K_\infty$  telle que  $L_\infty = LK_\infty$ . On note pour tout  $n \in \mathbb{N}$ ,  $L_n = LK_n$ . La configuration des extensions considérées est la suivante :



Suivons pas à pas la méthode de Colmez ([5], 1.4.) : pour tout  $\mu \geq -1$ ,  $[K_n : K_n^\mu] = [K_n L_n^\mu : L_n^\mu]$  (car  $K_n^\mu = K_n \cap L_n^\mu$ ). On a bien sûr  $v(\mathfrak{d}_{L_n/K_n}) = v(\mathfrak{d}_{L_n/K}) - (\mathfrak{d}_{K_n/K})$ . Ainsi, en appliquant la formule pour le calcul de la valuation de la différentielle, il vient :

$$\begin{aligned}
 v(\mathfrak{d}_{L_n/K_n}) &= \frac{1}{e} \int_{-1}^{+\infty} \left( \frac{1}{[K_n : K_n^\mu]} - \frac{1}{[L_n : L_n^\mu]} \right) d\mu \\
 &= \frac{1}{e[K_n : K]} \int_{-1}^{+\infty} [K_n^\mu : K] \left( 1 - \frac{1}{[L_n : K_n L_n^\mu]} \right) d\mu.
 \end{aligned}$$

Soit  $n_0$  un entier tel que  $L^{n_0} = L$ . Si  $\mu \geq n \geq n_0$ , alors  $L^\mu = L \subset L_n^\mu$ . Ainsi,  $L_n = K_n L \subset K_n L_n^\mu$ , c'est à dire  $[L_n : K_n L_n^\mu] = 1$ . Par conséquent,

$$\begin{aligned}
 e[K_n : K]v(\mathfrak{d}_{L_n/K_n}) &= \int_{-1}^{n_0} [K_n^\mu : K] \left( 1 - \frac{1}{[L_n : K_n L_n^\mu]} \right) d\mu \\
 &\leq \int_{-1}^{n_0} [K_n^\mu : K] d\mu.
 \end{aligned}$$

Pour  $\mu \leq \mu_n$ , et pour  $m \leq n$ ,  $K_n^\mu = K_m^\mu$ . Comme  $K_\infty/K$  est APF,  $\mu_n$  tend vers  $+\infty$ , et on a pour  $n$  assez grand :

$$\int_{-1}^{n_0} [K_n^\mu : K] d\mu = \int_{-1}^{n_0} [K_{n_0}^\mu : K] d\mu,$$

qui est une constante. Par conséquent,  $v(\mathfrak{d}_{L_n/K_n}) = O\left(\frac{1}{[K_n : K]}\right)$ . On a alors ([9], Chap V, §3, Lemme 4) :

$$v(\text{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n})) = O([K_n : K]^{-1}),$$

et donc un élément de  $\mathfrak{m}_{K_\infty}$  se trouve dans  $\mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n})$  pour  $n$  assez grand, et par conséquent dans  $\mathrm{Tr}_{L_\infty/K_\infty}(\mathcal{O}_{L_\infty})$ .  $\square$

Il résulte immédiatement de cette proposition qu'étant donné  $\varepsilon > 0$ , il existe  $y_\varepsilon \in \mathcal{O}_{L_\infty}$  tel que  $v(\mathrm{Tr}_{L_\infty/K_\infty}(y_\varepsilon)) < \varepsilon$ .

**COROLLAIRE 1.2.** — *Soit  $L_\infty$  une extension galoisienne finie de  $K_\infty$  de groupe de Galois  $G$ , et soient  $x \in L_\infty$  et  $\varepsilon > 0$ . Alors il existe  $y \in L_\infty$  tel que*

$$v(x - \mathrm{Tr}_{L_\infty/K_\infty}(y)) \geq \min_{\sigma \in G} v(\sigma x - x) - \varepsilon \text{ et } v(y) \geq v(x) - \varepsilon.$$

*Démonstration.* — Soit  $y_\varepsilon \in \mathcal{O}_{L_\infty}$  tel que  $v(\mathrm{Tr}_{L_\infty/K_\infty}(y_\varepsilon)) < \varepsilon$ , et soit  $z = \mathrm{Tr}_{L_\infty/K_\infty}(y_\varepsilon)$ .

On pose  $y = \frac{1}{z}xy_\varepsilon$ . Alors  $v(y) \geq v(x) - \varepsilon$  et

$$\begin{aligned} \mathrm{Tr}_{L_\infty/K_\infty}(y) &= \frac{1}{z} \sum_{\sigma \in G} \sigma(y_\varepsilon)\sigma(x) = \frac{1}{z} \sum_{\sigma \in G} \sigma(y_\varepsilon)(\sigma x - x + x) \\ &= x + \frac{1}{z} \sum_{\sigma \in G} \sigma(y_\varepsilon)(\sigma x - x). \end{aligned}$$

Ainsi,  $v(\mathrm{Tr}_{L_\infty/K_\infty}(y) - x) \geq \min_{\sigma \in G} v(\sigma x - x) - \varepsilon$ .  $\square$

Donnons au passage une proposition qui ne nous servira pas par la suite, mais qui découle directement du corollaire 1.2 en reprenant les arguments de [10], dont elle généralise la proposition 10 aux extensions APF.

**PROPOSITION 1.3.** — *Soit  $K_\infty/K$  une extension APF infinie, on note  $\mathcal{H} = \mathrm{Gal}(\bar{K}/K_\infty)$ , et  $\widehat{K_\infty}$  la fermeture de  $K_\infty$  dans  $C$ . Alors :*

$$H^0(\mathcal{H}, C) = \widehat{K_\infty} \text{ et } H^r(\mathcal{H}, C) = 0 \text{ pour } r \geq 1.$$

## 1.2. Étude de l'extension $K_\infty/K$

On peut maintenant appliquer le résultat précédent à une extension APF bien choisie. On définit  $\pi_0 = \pi$ , pour tout  $n \in \mathbb{N}$ ,  $\pi_{n+1}$  une racine  $p$ -ième de  $\pi_n$ ,  $K_n = K(\pi_n)$ , et  $K_\infty = \bigcup_{n \in \mathbb{N}} K_n$ . L'extension  $K_\infty$ , étudiée par Breuil dans [2] est APF. Nous redonnons ici une démonstration plus élémentaire (dans le sens où elle n'a pas recours aux groupes de Lie  $p$ -adiques) de ce résultat, qui est le lemme 2.1.1 de *loc. cit.*

**PROPOSITION 1.4.** — *L'extension  $K_\infty/K$  est APF.*

*Démonstration.* — On sait que  $v(\mathfrak{d}_{K_n/K}) = e(n + 1) - \frac{e}{p^n}$ . Un rapide calcul à partir de l'expression intégrale de  $v(\mathfrak{d}_{K_n/K})$  et une récurrence immédiate montrent alors que pour tout  $n \geq 1$ , la famille  $(\mu_n)_{n \in \mathbb{N}}$  étant définie comme en (1.1),

$$\mu_n = ne - 1 + \frac{pe}{p - 1}.$$

La suite  $\mu_n$  tend vers  $+\infty$ , il résulte de [11], 1.4.2. que  $K_\infty/K$  est APF et que  $(K_n)$  est la tour d'extensions élémentaires de  $K_\infty$ .  $\square$

On a le corollaire suivant :

**COROLLAIRE 1.5.** — *Soit  $\varepsilon > 0$ , soit  $x \in \bar{K}$  tel que pour tout  $\sigma \in G$ ,  $v(\sigma x - x) \geq A$ . Il existe  $y_\varepsilon \in K_\infty$  tel que  $v(x - y_\varepsilon) \geq A - \varepsilon$ .*

*Démonstration.* — On note  $M$  la clôture galoisienne de  $K_\infty(x)$ , alors  $\text{Gal}(\bar{K}/M)$  agit trivialement sur  $x$ , et donc pour tout  $\sigma \in \text{Gal}(M/K)$ ,  $v(\sigma x - x) \geq A$ , et en particulier pour tout  $\sigma \in \text{Gal}(M/K_\infty)$ ,  $v(\sigma x - x) \geq A$ . D'après le corollaire 1.2, il existe pour tout  $\varepsilon > 0$  un  $z_\varepsilon \in K_\infty$  tel que

$$v(x - z_\varepsilon) \geq A - \varepsilon \text{ et } v(z_\varepsilon) \geq v(x) - \varepsilon.$$

$\square$

**THÉORÈME 1.6.** — *Soit  $x \in K_\infty$ . Les deux assertions suivantes sont équivalentes :*

- (i)  $\forall \sigma \in G = \text{Gal}(\bar{K}/K)$ ,  $v(\sigma x - x) \geq A$
- (ii)  $\forall m \in \mathbb{N}$ ,  $\exists y_m \in K_m$  tel que  $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$ .

*En particulier, si  $x$  vérifie (i), il existe  $y \in K$  tel que  $v(x - y) \geq A - \frac{1}{p-1}$ .*

*Démonstration.* — Pour simplifier l'écriture, on notera  $A_m = A - \frac{1}{p^m(p-1)}$ . (i)  $\Rightarrow$  (ii). Soit  $n \in \mathbb{N}$  tel que  $x \in K_n$ . L'élément  $x$  s'écrit

$$x = \sum_{i=0}^{p^n-1} a_i \pi_n^i,$$

avec les  $a_i$  dans  $K$ . Pour  $\sigma \in G$ ,  $\sigma \pi_n$  est de la forme  $\zeta \pi_n$ , avec  $\zeta$  racine  $p^n$ -ième de l'unité. De plus, il existe  $\sigma \in G$  tel que  $\zeta$  soit une racine primitive  $p^n$ -ième de l'unité. Fixons un tel  $\sigma$ . On a :

$$\sigma x - x = \sum_{i=1}^{p^n-1} a_i \pi_n^i (\zeta^i - 1).$$

L'ordre de  $\zeta^i$  en tant que racine de l'unité est  $p^{n-v(i)}$ . En effet, écrivant  $i = p^{v(i)}d$  avec  $d$  non divisible par  $p$ . Alors  $\zeta^i = (\zeta^d)^{p^{v(i)}}$ ,  $\zeta^d$  est une racine

primitive  $p^n$ -ième de 1, donc  $(\zeta^d)^{p^{v(i)}}$  est une racine primitive  $p^{n-v(i)}$ -ième de 1.

Par conséquent, pour  $i \in \{1, \dots, p^n - 1\}$ , on a

$$v(a_i \pi_n^i (\zeta^i - 1)) = v(a_i) + \frac{i}{ep^n} + \frac{1}{p^{n-v(i)-1}(p-1)}.$$

Soient  $i, j \in \{1, \dots, p^n - 1\}$  tels que  $v(a_i \pi_n^i (\zeta^i - 1)) = v(a_j \pi_n^j (\zeta^j - 1))$ . Alors

$$\frac{i-j}{ep^n} + \frac{p^{v(i)} - p^{v(j)}}{p^{n-1}(p-1)} = v(a_j) - v(a_i) \in \frac{1}{e}\mathbb{Z}.$$

Les entiers  $v(i)$  et  $v(j)$  sont inférieurs ou égaux à  $n-1$ , on peut de plus supposer que  $v(i) \leq v(j)$ . On a alors  $(i-j)(p-1) - ep^{v(i)+1}(1-p^{v(j)-v(i)}) \in p^n(p-1)\mathbb{Z}$ . Si  $v(i) < v(j)$ , alors

$$v((i-j)(p-1)) = v(i), \text{ et } v(ep^{v(i)+1}(1-p^{v(j)-v(i)})) = v(e) + v(i) + 1.$$

Par conséquent,  $v((i-j)(p-1) - ep^{v(i)+1}(1-p^{v(j)-v(i)})) = v(i) < n-1$ .

On a donc nécessairement  $v(i) = v(j)$ . Ainsi,  $\frac{i-j}{p^n} \in \mathbb{Z}$ , et comme  $i$  et  $j$  sont inférieurs strictement à  $p^n$ ,  $i = j$ . Finalement,

$$v(a_i \pi_n^i (\zeta^i - 1)) = v(a_j \pi_n^j (\zeta^j - 1)) \Leftrightarrow i = j.$$

En particulier,

$$v(\sigma x - x) = \min_{1 \leq i \leq p^n - 1} \left( v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)} \right).$$

Soit  $0 \leq m \leq n-1$ . D'après le calcul précédent, si  $i \in \{1, \dots, p^n - 1\}$  et  $v(i) < n-m$ , on a sous les hypothèses du théorème :

$$v(a_i) + \frac{i}{ep^n} \geq A - \frac{p^{n-m-1}}{p^{n-1}(p-1)} \geq A_m.$$

D'autre part,

$$y_m = \sum_{\substack{0 \leq j \leq p^n - 1 \\ p^{n-m} | j}} a_j \pi_n^j = \sum_{j=0}^{p^m - 1} a_{p^{n-m}j} \pi_m^j \in K_m.$$

Finalement, on a

$$v(x - y_m) = \min_{\substack{1 \leq j \leq p^n - 1 \\ p^{n-m} \nmid j}} v(a_j \pi_n^j) = \min_{\substack{1 \leq j \leq p^n - 1 \\ v(j) < n-m}} \left( v(a_j) + \frac{j}{ep^n} \right) \geq A_m,$$

avec  $y_m \in K_m$ .

Pour  $m \geq n$ , il suffit de choisir  $y_m = x$ .



Réciproquement,  $(ii) \Rightarrow (i)$  : On suppose que  $x \in K_n$ . On écrit  $x = \sum_{i=0}^{p^n-1} a_i \pi_n^i$ . On fixe  $\sigma_0 \in \text{Gal}(\bar{K}/K)$  tel que  $\sigma_0 \pi_n = \zeta \pi_n$  avec  $\zeta$  racine primitive  $p^n$ -ième de l'unité. On pose pour tout  $m < n$  :

$$z_m = \sum_{j=0}^{p^m-1} a_{p^n-m_j} \pi_m^j.$$

La démonstration comporte trois étapes : tout d'abord, on montre que  $v(\sigma x - x) \geq v(\sigma_0 x - x)$  pour tout  $\sigma \in \text{Gal}(\bar{K}/K)$ . Ensuite, on vérifie que  $v(x - z) \leq v(x - z_m)$  pour tout  $z \in K_m$ . Enfin, on montre qu'il existe  $m < n$  tel que  $v(x - z_m) \leq v(\sigma_0 x - x) - \frac{1}{p^m(p-1)}$ , et on conclut.

Soit  $\sigma \in G$ . Il existe une racine  $p^n$ -ième de l'unité  $\omega$  telle que  $\sigma \pi_n = \omega \pi_n$ . Notons  $p^r$  l'ordre de  $\omega$  en tant que racine de l'unité. On a alors  $\sigma x - x = \sum_{i=1}^{p^n-1} a_i \pi_n^i (\omega^i - 1)$ . Pour tout  $i \in \{1, \dots, p-1\}$ ,  $v(a_i \pi_n^i (\omega^i - 1)) = v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{r-1}(p-1)}$ . Or  $r \leq n$ , donc

$$\forall i \in \{1, \dots, p-1\}, v(a_i \pi_n^i (\omega^i - 1)) \geq v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)}.$$

Or, on sait que  $v(\sigma_0 x - x) = \min_{1 \leq i \leq p^n-1} \left( v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)} \right)$ , et donc

$$v(\sigma x - x) \geq \min_{1 \leq i \leq p^n-1} (v(a_i \pi_n^i (\omega^i - 1))) \geq v(\sigma_0 x - x).$$

Soit  $0 \leq m \leq n-1$ , et soit  $z \in K_m$ . On va montrer que  $v(z - z_m) \neq v(x - z_m)$ . Tout d'abord, comme  $z$  et  $z_m$  sont dans  $K_m$ ,  $v(z - z_m) \in \frac{1}{ep^m} \mathbb{Z}$ .

D'autre part,  $v(x - z_m) = \min_{v(i) < n-m} \left( v(a_i) + \frac{i}{ep^n} \right)$ . Ainsi,

$$ep^m v(x - z_m) = \min_{v(i) < n-m} \left( ep^m v(a_i) + \frac{i}{p^{n-m}} \right).$$

Si  $v(i) < n-m$ ,  $\frac{i}{p^{n-m}} \notin \mathbb{Z}$ . Comme  $ev(a_i) \in \mathbb{Z}$  pour tout  $i$ , on en déduit que  $ep^m v(x - z_m) \notin \mathbb{Z}$ , et donc que  $v(z - z_m) \neq v(x - z_m)$ . Par conséquent,  $v(x - z) = \min(v(x - z_m), v(z - z_m)) \leq v(x - z_m)$ .

On sait que  $v(\sigma_0 x - x) = \min_{1 \leq i \leq p^n-1} \left( v(a_i) + \frac{i}{ep^n} + \frac{p^{v(i)}}{p^{n-1}(p-1)} \right)$ . Notons  $i_0$  l'indice pour lequel ce minimum est atteint ; fixons  $m \in \{0, \dots, n-1\}$  tel que  $v(i_0) = n-1-m$ . On a

$$v(x - z_m) = \min_{v(i) < n-m} \left( v(a_i) + \frac{i}{ep^n} \right) \leq v(a_{i_0}) + \frac{i_0}{ep^n}.$$

Or, par définition de  $i_0$ ,  $v(\sigma_0 x - x) = v(a_{i_0}) + \frac{i_0}{ep^n} + \frac{1}{p^m(p-1)}$ , et donc  $v(x - z_m) \leq v(\sigma_0 x - x) - \frac{1}{p^m(p-1)}$ .

Fixons-nous maintenant  $\sigma \in G$ . D'après les hypothèses du théorème, il existe un  $y_m \in K_m$  tel que  $v(x - y_m) \geq A_m$ . On fixe un tel  $y_m$ , on a en particulier  $v(x - z_m) \geq A_m$ . Ainsi,

$$v(\sigma x - x) \geq v(\sigma_0 x - x) \geq v(x - z_m) + \frac{1}{p^m(p-1)} \geq A.$$

□

### 1.3. Optimisation du théorème d'Ax

Dans cette partie, on utilise les résultats de la partie précédente et de l'étude menée sur les extensions APF pour donner la constante optimale dans le théorème d'Ax. Remarquons d'emblée que la constante optimale est minorée par  $\frac{1}{p-1}$ . En effet,  $v(\sigma\pi_1 - \pi_1) = v(\pi_1) + \frac{1}{p-1}$ , et  $\sup_{y \in K} v(\pi_1 - y) = v(\pi_1)$ . On va montrer que  $\frac{1}{p-1}$  est en fait la constante optimale.

**THÉORÈME 1.7.** — *Soit  $x \in C$ . Les deux assertions suivantes sont équivalentes :*

(i)  $\forall \sigma \in G = \text{Gal}(\bar{K}/K), v(\sigma x - x) \geq A$

(ii)  $\forall m \in \mathbb{N}, \exists y_m \in K_m$  tel que  $v(x - y_m) \geq A - \frac{1}{p^m(p-1)}$ .

*En particulier, si  $x$  vérifie (i), il existe  $y \in K$  tel que  $v(x - y) \geq A - \frac{1}{p-1}$ .*

*Démonstration.* — (i)  $\Rightarrow$  (ii) On commence par supposer  $x \in \bar{K}$ . Pour tout  $\varepsilon > 0$ , on fixe  $z_\varepsilon \in K_\infty$  tel que  $v(x - z_\varepsilon) \geq A - \varepsilon$ , comme dans le corollaire 1.5. On a  $v(\sigma z_\varepsilon - z_\varepsilon) \geq A - \varepsilon$ .

Soit  $m \in \mathbb{N}$ . D'après le théorème 1.6, il existe  $y_\varepsilon \in K_m$  tel que  $v(z_\varepsilon - y_\varepsilon) \geq A_m - \varepsilon$ . Fixons un tel  $y_\varepsilon$ , on a alors  $v(x - y_\varepsilon) \geq A_m - \varepsilon$ .

Si  $0 < \varepsilon' < \varepsilon$ ,

$$v(y_\varepsilon - y_{\varepsilon'}) \geq A_m - \varepsilon.$$

Mais  $ep^m v(y_\varepsilon - y_{\varepsilon'}) \in \mathbb{Z}$ . Ainsi, pour  $\varepsilon$  suffisamment petit (de manière à ce que les entiers immédiatement supérieurs à  $ep^m(A_m - \varepsilon)$  et à  $ep^m A_m$  soient égaux), on a  $v(y_\varepsilon - y_{\varepsilon'}) \geq A_m$ . Fixons un tel  $\varepsilon$  et posons  $y_m = y_\varepsilon$ . Alors, pour tout  $0 < \varepsilon' < \varepsilon$ ,

$$v(x - y_m) \geq \min(v(x - y_{\varepsilon'}), v(y_{\varepsilon'} - y_m)) \geq A_m - \varepsilon'.$$

Cette minoration étant valable pour tout  $\varepsilon'$ , on a  $v(x - y_m) \geq A_m$ . Maintenant, lorsque  $x \in C$ , soit  $y \in \bar{K}$  tel que  $v(x - y) \geq A$ . On a alors pour tout

$\sigma \in G$ ,  $v(\sigma y - y) \geq A$ . Par conséquent, il existe pour tout  $m$  un  $y_m \in K_m$  tel que  $v(y - y_m) \geq A_m$ , et on a pour tout  $m \in \mathbb{N}$ ,

$$v(x - y_m) \geq A - \frac{1}{p^m(p-1)}.$$

(ii)  $\Rightarrow$  (i) Supposons d'abord  $x \in \bar{K}$ . Soit  $n \in \mathbb{N}$ , pour  $m < n$  on pose  $z_m = y_m$ , et pour  $m \geq n$ , on pose  $z_m = y_n$ . On a alors, pour tout  $m \in \mathbb{N}$ ,  $z_m \in K_m$  et  $v(y_n - z_m) \geq A_m$ . D'après le théorème 1.6, pour tout  $\sigma \in G$ , on a  $v(\sigma y_n - y_n) \geq A$ . On en déduit immédiatement que pour tout  $\sigma \in G$ ,

$$v(\sigma x - x) \geq \min(v(\sigma y_n - y_n), v(\sigma(x - y_n)), v(x - y_n)) \geq A_n.$$

Cette inégalité étant vraie pour tout  $n \in \mathbb{N}$ , il en résulte que  $v(\sigma x - x) \geq A$  quel que soit  $\sigma \in G$ .

On en déduit le résultat pour  $x \in C$  comme précédemment. □

Le théorème 1.7 peut se reformuler de la manière suivante :

COROLLAIRE 1.8. — Soit  $x \in C$ . Alors :

$$\inf_{\sigma \in G} v(\sigma x - x) = \sup_{n \in \mathbb{N}} \inf_{y \in K_n} \left\{ v(x - y) + \frac{1}{p^n(p-1)} \right\}.$$

## 2. Application au calcul de $H^1(G, \mathcal{O}_{\bar{K}})$

On a la suite exacte  $0 \rightarrow \mathcal{O}_{\bar{K}} \rightarrow \bar{K} \rightarrow \bar{K}/\mathcal{O}_{\bar{K}} \rightarrow 0$ . En passant aux points fixes par  $G = \text{Gal}(\bar{K}/K)$ , on a :

$$0 \rightarrow K/\mathcal{O}_K \rightarrow (\bar{K}/\mathcal{O}_{\bar{K}})^G \rightarrow H^1(G, \mathcal{O}_{\bar{K}}) \rightarrow 0$$

car  $H^1(G, \bar{K}) = 0$  (ici,  $\bar{K}$  est muni de la topologie discrète). Il en résulte que  $H^1(G, \mathcal{O}_{\bar{K}})$  est isomorphe au quotient  $(\bar{K}/\mathcal{O}_{\bar{K}})^G / (K/\mathcal{O}_K)$ , identification que l'on fera par la suite. On a déjà le résultat suivant :

PROPOSITION 2.1. — Soit  $n$  un entier  $\geq \frac{e}{p-1}$ . Alors  $H^1(G, \mathcal{O}_{\bar{K}})$  est tué par  $\pi^n$ . En particulier,  $H^1(G, \mathcal{O}_{\bar{K}})$  est tué par  $p$ .

*Démonstration.* — Soit  $x \in (\bar{K}/\mathcal{O}_{\bar{K}})^G$ . C'est l'image modulo  $\mathcal{O}_{\bar{K}}$  d'un élément  $\xi$  de  $\bar{K}$  vérifiant pour tout  $\sigma \in G$ ,  $v(\sigma \xi - \xi) \geq 0$ . Il existe  $y \in K$  tel que  $v(\xi - y) \geq -\frac{1}{p-1}$ . On a alors  $v(\pi^n \xi - \pi^n y) \geq \frac{n}{e} - \frac{1}{p-1} \geq 0$ , donc  $\pi^n \xi = 0$  dans  $H^1(G, \mathcal{O}_{\bar{K}})$ , c'est à dire  $\pi^n x = 0$ . □

*Remarque 2.2.* — Ce résultat était déjà connu de Sen, voir [8], théorème 3. Il n'implique pas le théorème 1.7, ni même l'obtention de la constante optimale dans le théorème d'Ax, car  $n$  est supposé être entier. Cependant, bien que Sen n'en dise rien, il semble possible d'adapter sa preuve du théorème 3 de [8] pour en déduire la constante optimale dans le théorème d'Ax, en montrant d'abord que si  $x \in \bar{K}$  et  $\sigma x - x \in \mathcal{O}_{\bar{K}}$  pour tout  $\sigma \in G$ , alors il existe  $y \in K$  tel que  $v(x - y) \geq -\frac{1}{p-1}$ .

Dans la suite, on note

$$\mathfrak{a}_n = \left\{ z \in \bar{K} / v(z) \geq -\frac{1}{p^n(p-1)} \right\}.$$

## 2.1. Cas non ramifié

Dans cette sous-partie, on suppose que  $K = F$ , c'est à dire  $K/F$  absolument non ramifiée.

On rappelle que l'on identifie  $(\bar{K}/\mathcal{O}_{\bar{K}})^G / (K/\mathcal{O}_K)$  et  $H^1(G, \mathcal{O}_{\bar{K}})$ . On va montrer que l'on peut associer à  $x \in H^1(G, \mathcal{O}_{\bar{K}})$  une suite d'éléments de  $k$  dont nous étudierons ensuite les propriétés. Pour  $n \in \mathbb{N}$ , on note  $\eta_n = \pi_n^{-1}$ .

**PROPOSITION 2.3.** — *Soit  $x \in H^1(G, \mathcal{O}_{\bar{K}})$ , il existe un antécédent  $\xi$  de  $x$  dans  $\bar{K}$  et une suite  $(x_n)_{n \in \mathbb{N}^*}$  d'éléments de  $k$  telle que pour tout  $n \in \mathbb{N}$ ,*

$$\xi = \sum_{i=1}^n [x_i] \eta_i \pmod{\mathfrak{a}_n},$$

où pour tout  $i$ ,  $[x_i]$  est le représentant de Teichmüller de  $x_i$ . De plus, la suite  $(x_n)$  ne dépend que de  $x$ .

*Démonstration.* — Soit  $\xi$  un antécédent de  $x$  dans  $\bar{K}$ . D'après le théorème 1.7, il existe pour tout  $m \in \mathbb{N}$  un  $y_m \in K_m$  tel que  $\xi = y_m \pmod{\mathfrak{a}_m}$ . On fixe une telle famille  $(y_m)$ . Comme  $v(\xi - y_0) \geq -\frac{1}{p-1}$ , on peut supposer, quitte à remplacer  $\xi$  par  $\xi - y_0$ , que  $v(\xi) \geq -\frac{1}{p-1}$ . On construit la suite  $(x_n)_{n \in \mathbb{N}}$  par récurrence. Le cas  $n = 0$  est trivial.

On suppose construite la suite jusqu'à l'indice  $n$ , et on écrit :

$$\xi = [x_1] \eta_1 + \cdots + [x_n] \eta_n + z, \text{ avec } z \in \mathfrak{a}_n, \text{ et } y_{n+1} = \sum_{i \geq -n_0} c'_i \pi_{n+1}^i,$$

où les  $c'_i$  sont pris parmi les représentants de Teichmüller des éléments de  $k$  et  $n_0 \geq 0$ . En posant  $c_i = c'_{-i}$ , on a  $y_{n+1} = \sum_{i=1}^{n_0} c_i \eta_{n+1}^i \pmod{\mathcal{O}_{\bar{K}}}$ . Il en résulte que  $\xi = \sum_{i=1}^{n_0} c_i \eta_{n+1}^i + z'$ , avec  $z' \in \mathfrak{a}_{n+1}$ . Pour  $k \geq 1$ ,

$$\eta_{n+1}^k \in \mathfrak{a}_n \Leftrightarrow (p \geq 3 \text{ et } k = 1) \text{ ou } (p = 2 \text{ et } k \in \{1, 2\}).$$

Ainsi, pour  $p \geq 3$ , en réduisant modulo  $\mathfrak{a}_n$ , on a  $\sum_{i=2}^{n_0} c_i \eta_{n+1}^i = [x_1] \eta_1 + \dots + [x_n] \eta_n \pmod{\mathfrak{a}_n}$ . Par conséquent, en identifiant les coefficients dans  $K_{n+1}$ , on a

$$x = [x_1] \eta_1 + \dots + [x_n] \eta_n + c_1 \eta_{n+1} + z',$$

ce qui achève la récurrence en posant  $x_{n+1} = c_1 \pmod p$ .

Lorsque  $p = 2$ , on a (toujours en réduisant modulo  $\mathfrak{a}_n$ )  $\sum_{i=3}^{n_0} c_i \eta_{n+1}^i = [x_1] \eta_1 + \dots + [x_{n-1}] \eta_{n-1}$ . Ainsi,  $\xi = c_1 \eta_{n+1} + c_2 \eta_{n+1}^2 + [x_1] \eta_1 + \dots + [x_{n-1}] \eta_{n-1} + z'$ . Mais  $\eta_{n+1}^2 = \eta_n$ , et donc  $\xi$  s'écrit encore  $\xi = [x_1] \eta_1 + \dots + [x_n] \eta_n \pmod{\mathfrak{a}_{n+1}}$  (car  $\eta_{n+1} \in \mathfrak{a}_{n+1}$ ).

La suite  $(x_n)_{n \in \mathbb{N}}$  ainsi associée à  $x \in H^1(G, \mathcal{O}_{\bar{K}})$  ne dépend pas de  $\xi \in \mathfrak{a}_0$ . De plus si  $\xi \pmod{\mathfrak{a}_n} = \sum_{i=1}^n [x_i] \eta_i = \sum_{i=1}^n [x'_i] \eta_i$ , alors en réduisant modulo  $\mathfrak{a}_i$ , on a

$$\sum_{j=1}^i [x_j] \eta_j = \sum_{j=1}^i [x'_j] \eta_j \text{ si } p \geq 3, \text{ et } \sum_{j=1}^{i-1} [x_j] \eta_j = \sum_{j=1}^{i-1} [x'_j] \eta_j \text{ si } p = 2.$$

On en déduit par récurrence sur  $i$  que pour tout  $i \in \mathbb{N}$ ,  $v([x_i] - [x'_i]) \geq \frac{1}{p^i} > 0$ . Comme les  $[x_i]$  sont dans  $K$ , ils sont égaux modulo  $p$ , et la suite  $(x_n)$  est unique. □

On peut donc définir l'application

$$\begin{aligned} \psi : H^1(G, \mathcal{O}_{\bar{K}}) &\longrightarrow k^{\mathbb{N}^*} \\ x &\longmapsto (x_n)_{n \in \mathbb{N}^*} \end{aligned}$$

telle que pour tout  $n \in \mathbb{N}^*$ ,  $x - \sum_{i=1}^n [x_i] \eta_i \in \mathfrak{a}_n$ . C'est un morphisme  $\mathcal{O}_K$ -linéaire (ou  $k$ -linéaire puisque  $H^1(G, \mathcal{O}_{\bar{K}})$  est tué par  $p$ ), injectif. Il nous reste à identifier son image. On va adapter à notre cas des constructions proposées par Kedlaya dans un cadre un peu différent (il s'agissait de donner une description d'une clôture algébrique de  $\mathbb{F}_p((t))$ , voir [6]). Compte tenu du fait que nous étudions des objets plus simples, nous avons préféré réécrire l'étude de Kedlaya dans le langage de notre problème.

DÉFINITION 2.4. — Soit  $(x_n)_{n \in \mathbb{N}^*} \in k^{\mathbb{N}^*}$ . On dit que la suite  $(x_n)$  est twist-récurrente s'il existe  $d_0, \dots, d_r \in k$  non tous nuls tels que

$$\forall n \in \mathbb{N}^*, d_0 x_n + d_1 x_{n+1}^p + \dots + d_r x_{n+r}^{p^r} = 0.$$

PROPOSITION 2.5. — L'application  $\psi$  définie précédemment induit un isomorphisme de  $H^1(G, \mathcal{O}_{\bar{K}})$  sur le sous-espace de  $k^{\mathbb{N}^*}$  formé des suites twist-récurrentes.

Démonstration. — On commence par montrer que si  $x \in H^1(G, \mathcal{O}_{\bar{K}})$ , alors  $\psi(x)$  est twist-récurrente. L'élément  $x$  provient d'un élément  $\xi_0 \in \bar{K}$ , que l'on peut supposer de valuation  $\geq -\frac{1}{p-1}$ . Calculons  $\xi_0^p$  lorsque

$\psi(x) = (x_n)$ . Soit  $n \in \mathbb{N}^*$ , écrivons  $\xi_0 = \sum_{i=1}^n [x_i] \eta_i + z$ , avec  $z \in \mathfrak{a}_n$  et les  $[x_i]$  les représentants de Teichmüller. Alors  $\xi_0^p = \sum_{i=0}^{n-1} [x_{i+1}]^p \eta_i + \tilde{z}$ , avec  $\tilde{z} = \sum_{j=1}^p \binom{p}{j} (\sum_{i=1}^n [x_i] \eta_i)^{p-j} z^j$ . Or pour tout  $j \in \{1, \dots, p-1\}$ ,

$$v \left( \binom{p}{j} \left( \sum_{i=1}^n [x_i] \eta_i \right)^{p-j} z^j \right) \geq 1 - \frac{j}{p^n(p-1)} - \frac{p-j}{p^n} \geq 0.$$

Ainsi,  $\xi_0^p = [x_1]^p \eta_0 + \sum_{i=1}^{n-1} [x_{i+1}]^p \eta_i \pmod{\mathfrak{a}_{n-1}}$ . En particulier,  $\xi_0^p$  vérifie  $v(\sigma \xi_0^p - \xi_0^p) \geq 0$  pour tout  $\sigma \in G$ , et se réduit dans  $H^1(G, \mathcal{O}_{\bar{K}})$  sur un élément dont l'image par  $\psi$  est  $(x_{n+1}^p)$ . Pour tout  $s \in \mathbb{N}$ , on pose  $\xi_{s+1} = \xi_s^p - [x_s]^{p^s} \eta_0$ . On vérifie facilement que  $v(\sigma \xi_s^p - \xi_s^p) \geq 0$  pour tout  $\sigma \in G$ , et que la réduction dans  $H^1(G, \mathcal{O}_{\bar{K}})$  a pour image par  $\psi$  la suite  $[x_{n+s}]^{p^s}$ . Comme par ailleurs tous les  $\xi_s$  sont dans  $K(\xi_0)$ , ils forment une famille liée sur  $K$ . Il existe donc  $\delta_0, \dots, \delta_r \in K$  tels que  $\delta_0 \xi_0 + \dots + \delta_r \xi_r = 0$ . Quitte à multiplier par une puissance de  $p$ , on peut supposer que les  $\delta_s$  sont dans  $\mathcal{O}_K$  et qu'au moins l'un d'entre eux est non divisible par  $p$ . L'application  $\psi$  étant  $\mathcal{O}_K$ -linéaire, on en déduit que pour tout  $n \in \mathbb{N}^*$ ,

$$d_0 x_n + d_1 x_{n+1}^p + \dots + d_r x_{n+r}^{p^r} = 0,$$

où  $d_s$  désigne la réduction de  $\delta_s$  modulo  $p$ . Donc  $(x_n)$  est twist-récurrente.

Réciproquement, il nous reste à prouver que si  $(x_n)_{n \in \mathbb{N}^*}$  est twist-récurrente, alors c'est l'image par  $\psi$  d'un élément de  $H^1(G, \mathcal{O}_{\bar{K}})$ . Soit donc  $(x_n)_{n \in \mathbb{N}^*}$  twist-récurrente et soient  $d_0, \dots, d_r \in k$  non tous nuls tels que

$$\forall n \in \mathbb{N}^*, d_0 x_n + \dots + d_r x_{n+r}^{p^r} = 0.$$

On note  $\delta_0, \dots, \delta_r$  les représentants de Teichmüller des  $d_k$  dans  $\mathcal{O}_K$ , et pour  $n \geq 1$ , on note  $[x_n]$  le représentant de Teichmüller de  $x_n$  dans  $\mathcal{O}_K$ , et on considère le polynôme

$$P = - \left( \delta_r [x_r]^{p^r} \eta_1 + \dots + (\delta_1 [x_r]^p + \dots + \delta_r [x_{2r-1}]^{p^r}) \eta_r \right) + \delta_0 X + \dots + \delta_r X^{p^r}.$$

On va montrer qu'il admet une racine dans  $\mathcal{O}_{\bar{K}}$  dont l'image dans  $H^1(G, \mathcal{O}_{\bar{K}})$  s'envoie par  $\psi$  sur la suite  $(0, \dots, x_{r+1}, x_{r+2}, \dots)$  (la suite commence par  $r$  zéros). On fixe  $n \geq 1$  et on cherche une racine  $\xi$  de  $P$  sous la forme  $\xi = [x_{r+1}] \eta_{r+1} + \dots + [x_{n+r}] \eta_{n+r} + y \eta_{n+r+1}$  avec  $y \in \mathcal{O}_{\bar{K}}$ .

Tout d'abord, on a pour  $0 \leq s \leq r$ ,

$$\xi^{p^s} = \left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^s} + \eta_{n+r+1}^{p^s} y^{p^s} + \sum_{j=1}^{p^s-1} \binom{p^s}{j} \left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^s-j} \eta_{n+r+1}^j y^j.$$

Comme  $P(\xi) = 0$ , on a :

$$\sum_{k=0}^r \delta_k \left[ \left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^k} + \sum_{j=1}^{p^k-1} \binom{p^k}{j} \left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^k-j} \eta_{n+r+1}^j y^j + \eta_{n+r+1}^{p^k} y^{p^k} \right] = \delta_r [x_r]^{p^r} \eta_1 + \dots + (\delta_1 [x_r]^p + \dots + \delta_r [x_{2r-1}]^{p^r}) \eta_r.$$

On voit donc que  $y$  est annulé par un polynôme  $Q$  de degré  $p^r$ , dont le coefficient constant est

$$\sum_{k=0}^r \delta_k \left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^k} - (\delta_r [x_r]^{p^r} \eta_1 + \dots + (\delta_1 [x_r]^p + \dots + \delta_r [x_{2r-1}]^{p^r}) \eta_r),$$

et dont le coefficient dominant est  $\delta_r \eta_{n+r+1}^{p^r} = \delta_r \eta_{n+1}$ . Par ailleurs, on a :

$$\left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^p = \sum_{\varepsilon_1 + \dots + \varepsilon_n = p} \frac{p!}{\varepsilon_1! \dots \varepsilon_n!} [x_{r+1}]^{\varepsilon_1} \dots [x_{n+r}]^{\varepsilon_n} \eta_{r+1}^{\varepsilon_1} \dots \eta_{n+r}^{\varepsilon_n}.$$

On remarque que si tous les  $\varepsilon_i$  sont  $< p$ ,  $v(\frac{p!}{\varepsilon_1! \dots \varepsilon_n!}) = 1$  et  $v(\eta_{r+1}^{\varepsilon_1} \dots \eta_{n+r}^{\varepsilon_n}) = -\frac{\varepsilon_1}{p^{r+1}} - \dots - \frac{\varepsilon_n}{p^{n+r}} > -1$ . Donc tous les termes correspondants de la somme sont nuls modulo  $\mathcal{O}_{\bar{K}}$ , et donc

$$\left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^p = [x_{r+1}]^p \eta_r + [x_{r+2}]^p \eta_{r+1} + \dots + [x_{n+r}]^p \eta_{n+r-1} \pmod{\mathcal{O}_{\bar{K}}}.$$

Un calcul analogue montre que pour tout  $s \in \{1, \dots, r\}$ , on a :

$$\left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^s} = [x_{r+1}]^{p^s} \eta_{r+1-s} + [x_{r+2}]^{p^s} \eta_{r+2-s} + \dots + [x_{n+r}]^{p^s} \eta_{r+n-s} \pmod{\mathcal{O}_{\bar{K}}}.$$

En additionnant, on a donc :

$$\sum_{s=0}^r \delta_s \left( \sum_{i=r+1}^{n+r} [x_i] \eta_i \right)^{p^s} = \delta_r [x_r]^{p^r} \eta_1 + \dots + (\delta_1 [x_r]^p + \dots + \delta_r [x_{2r-1}]^{p^r}) \eta_r + \eta_{n+1} z,$$

avec  $z \in \mathcal{O}_{\bar{K}}$ . Le coefficient constant de  $Q$  est donc de valuation  $\geq -\frac{1}{p^{n+1}}$  qui est la valuation de son coefficient dominant. En traçant son polygone de Newton, on en déduit que ce polynôme a une racine de valuation positive. Le polynôme  $P$  a donc bien une racine de la forme  $x = [x_{r+1}] \eta_{r+1} + \dots + [x_{n+r}] \eta_{n+r} + y \eta_{n+r+1}$  avec  $y \in \mathcal{O}_{\bar{K}}$ . Comme  $P$  a  $p^r$  racines, il y a au moins l'une d'entre elles qui est obtenue pour une infinité de  $n$  à l'aide de la construction précédente. Notons  $\xi_0$  une telle racine. En réduisant modulo  $\mathfrak{a}_n$ , on voit que pour toute  $n \in \mathbb{N}^*$ , on a  $\xi_0 - \sum_{i=r+1}^{r+n} [x_i] \eta_i \in \mathfrak{a}_n$ . On a donc  $\xi_0 \in H^1(G, \mathcal{O}_{\bar{K}})$ , et  $\psi(\xi_0) = (0, 0, \dots, 0, x_{r+1}, x_{r+2}, \dots, x_n, \dots)$ . Comme

$(x_1, \dots, x_r, 0, 0, \dots)$  est l'image de  $\sum_{i=1}^r [x_i] \eta_i \in H^1(G, \mathcal{O}_{\bar{K}})$ , on en déduit que  $(x_n)$  est dans l'image de  $\psi$ .  $\square$

**COROLLAIRE 2.6.** — *Si  $K = F$ ,  $H^1(G, \mathcal{O}_{\bar{K}})$  est un  $k$ -espace vectoriel de dimension infinie. Plus précisément, si  $k$  est fini, la dimension de  $H^1(G, \mathcal{O}_{\bar{K}})$  est dénombrable. Si  $k$  est infini, elle est égale à la cardinalité de  $k$ .*

*Démonstration.* —  $H^1(G, \mathcal{O}_{\bar{K}})$  est l'ensemble des suites twist-récurrentes à valeurs dans  $k$ . Pour  $d_0, \dots, d_r$  non tous nuls fixés, l'ensemble des suites vérifiant la relation de twist-réurrence

$$\forall n \in \mathbb{N}, d_0 x_n + \dots + d_r x_{n+r}^p = 0$$

forme un  $k$ -espace vectoriel de dimension finie. La réunion des espaces déterminés par l'ensemble des  $(d_0, \dots, d_r) \in k^{r+1}$ , pour  $r \geq 0$ , est de dimension dénombrable si  $k$  est fini, et de dimension la cardinalité de  $k$  si  $k$  est infini.  $\square$

## 2.2. Vers le cas ramifié

Dans cette partie, on entame une étude analogue à la précédente, en ne supposant plus cette fois-ci que  $e = 1$ . Les preuves sont souvent esquissées.

### 2.2.1. Cas $e \leq p - 1$

On étudie ici le cas où  $e \leq p - 1$ , pour lequel les constructions proposées dans le cas non ramifié s'adaptent facilement. La proposition précédente nous dit que  $H^1(G, \mathcal{O}_{\bar{K}})$  est tué par  $\pi$ , en particulier il a une structure naturelle de  $k$ -espace vectoriel. On peut en fait associer à un élément de  $H^1(G, \mathcal{O}_{\bar{K}})$  une famille de suites d'éléments de  $k$ .

**PROPOSITION 2.7.** — *Soit  $x \in H^1(G, \mathcal{O}_{\bar{K}})$ , il existe  $e$  suites  $(x_{1,n}), \dots, (x_{e,n})$  d'éléments de  $k$  telles que pour tout  $n \in \mathbb{N}$ ,  $x = \sum_{i=1}^n \sum_{j=1}^e [x_{j,i}] \eta_i^j \pmod{\mathfrak{a}_n}$ ,  $[x_{j,n}]$  désignant le représentant de Teichmüller de  $x_{j,n}$ .*

*Démonstration.* — On procède comme dans le cas non ramifié, la différence ici étant que la réduction modulo  $\mathfrak{a}_n$  de  $y_{n+1}$  ne tue plus seulement  $c_1 \eta_{n+1}$  mais la somme  $c_1 \eta_{n+1} + \dots + c_e \eta_{n+1}^\rho$  lorsque  $e < p - 1$ ,  $\rho$  désignant le plus grand entier inférieur à  $\frac{ep}{p-1}$ . Le cas  $e = p - 1$  entraîne la même modification que dans le cas  $e = 1, p = 2$ .  $\square$



On a donc comme précédemment une application :

$$\begin{aligned} \psi : H^1(G, \mathcal{O}_{\bar{K}}) &\longrightarrow (k^{\mathbb{N}^*})^e \\ x &\longmapsto ((x_{1,n})_{n \in \mathbb{N}^*}, \dots, (x_{e,n})_{n \in \mathbb{N}^*}) \end{aligned}$$

THÉOREME 2.8. — *L'application qui à  $x \in H^1(G, \mathcal{O}_{\bar{K}})$  associe  $((x_{1,n}), (x_{2,n}), \dots, (x_{e,n}))$  est injective, et son image est l'ensemble des  $e$ -uplets de suites twist-récurrentes à valeurs dans  $k$ , qui est donc isomorphe à  $H^1(G, \mathcal{O}_{\bar{K}})$ .*

Démonstration. — Nous ne donnerons pas ici la démonstration de ce résultat, les idées sont similaires à celles de la preuve dans le cas non ramifié. □

### 2.2.2. Cas général

Il nous reste à traiter le cas  $e \geq p$ .  $H^1(G, \mathcal{O}_{\bar{K}})$  n'est pas tué par  $\pi$ . On note  $\tau = \lfloor \frac{e}{p-1} \rfloor$  et  $\rho = \lfloor \frac{ep}{p-1} \rfloor$  (où  $\lfloor t \rfloor$  désigne le plus grand entier inférieur ou égal à  $t$ ). Un calcul direct montre que  $\rho - \tau = e$ . Soit  $x \in H^1(G, \mathcal{O}_{\bar{K}})$ . On dispose d'une suite  $(y_n)$  avec pour tout  $n \in \mathbb{N}$ ,  $y_n \in K_n$  et  $x = y_n \pmod{\mathfrak{a}_n}$ . On écrit pour tout  $n \in \mathbb{N}$  que  $y_n = \sum_{j=1}^{N_n} c_{j,n} \eta_n^j$ , avec les  $c_{j,n}$  pris dans une famille de représentants des éléments de  $k$  dans  $\mathcal{O}_K$  de valuation nulle ou infinie (on ne suppose plus ici qu'il s'agit des représentants de Teichmüller). Pour tout  $n \in \mathbb{N}^*$ , il existe  $z_n \in \mathfrak{a}_n$  tel que  $x = \sum_{j=1}^{N_n} c_{j,n} \eta_n^j + z_n$ . On remarque que  $\eta_n^j \in \mathfrak{a}_n$  si et seulement si  $j \leq \tau$ , on peut donc supposer que la somme commence à  $j = \tau + 1$ .

Réduisons modulo  $\mathfrak{a}_n$  l'égalité précédente écrite aux rangs  $n$  et  $n + 1$ . On a pour  $j \geq 1$  :

$$\eta_{n+1}^j \in \mathfrak{a}_n \Leftrightarrow \frac{j}{ep^{n+1}} \leq \frac{1}{p^n(p-1)} \Leftrightarrow j \leq \frac{ep}{p-1} \Leftrightarrow j \leq \rho.$$

Par conséquent,

$$\sum_{j=\tau+1}^{N_n} c_{j,n} \eta_n^j = \sum_{j=\rho+1}^{N_{n+1}} c_{j,n+1} \eta_{n+1}^j \pmod{\mathfrak{a}_n}$$

Il découle de ces calculs la proposition suivante :

PROPOSITION 2.9. — *Soit  $x \in H^1(G, \mathcal{O}_{\bar{K}})$ . Il existe  $e$  suites  $(\alpha_{n,\tau+1})_{n \in \mathbb{N}^*}, \dots, (\alpha_{n,\rho})_{n \in \mathbb{N}^*}$  d'éléments de  $\mathcal{O}_K$  telles que pour tout  $n \in \mathbb{N}^*$ ,  $x = \sum_{i=1}^n \sum_{j=\tau+1}^{\rho} \alpha_{i,j} \eta_i^j \pmod{\mathfrak{a}_n}$ .*

*Démonstration.* — On procède par récurrence, en conservant les notations précédentes. Le cas  $n = 1$  est immédiat, compte tenu du fait que pour  $j \geq \rho$ ,  $\eta_1^j \in K$ .

Pour  $n \geq 1$ , on a  $\sum_{j=\rho+1}^{N_{n+1}} c_{j,n+1} \eta_{n+1}^j = \sum_{i=1}^n \sum_{j=\tau+1}^{\rho} \alpha_{i,j} \eta_i^j \pmod{\mathfrak{a}_n}$  par hypothèse de récurrence, et donc

$$x = \sum_{k=\tau+1}^{\rho} c_{k,n+1} \eta_k^k + \sum_{i=1}^n \sum_{k=\tau+1}^{\rho} \alpha_{i,k} \eta_i^k + z_{n+1},$$

ce qui prouve la proposition en posant  $\alpha_{n+1,j} = c_{j,n+1}$ .  $\square$

Remarquons que dans cette écriture, un  $\eta_i^j$  n'apparaît qu'une fois; autrement dit, il n'existe pas de couples  $(i, j)$ ,  $(i', j')$  distincts d'indices dans cette somme tels que  $\eta_i^j = \eta_{i'}^{j'}$ . En effet, on a :

$$p(\tau + 1) > p \frac{e}{p-1} \geq \rho.$$

En conséquence, si  $j, j' \in \{\tau + 1, \dots, \rho\}$  et  $j < j'$ , on a  $pj > j'$ , et donc  $p^i j \neq p^i j'$  pour tous  $i, i'$ . De plus, comme on calcule modulo  $K$ , on peut supprimer de cette somme les  $\alpha_{j,i}$  tels que  $j|p^i$ ; on peut également regrouper les termes indexés par  $(i, j - \lambda p^i)$  pour  $\lambda \in \mathbb{N}$  car alors  $\eta_i^{j-\lambda p^i} = \pi^\lambda \eta_i^j$ . Pour  $i \in \mathbb{N}^*$  et  $j \in \{\tau + 1, \dots, \rho\}$ ,  $j \nmid p^i$ , on note  $\gamma_{i,j} = \max\{s \in \{\tau + 1, \dots, \rho\} / p^s \mid s - j\}$  et  $I = \{(i, \gamma_{i,j}) / i \in \mathbb{N}^*, j \in \{\tau + 1, \dots, \rho\}, p^i \nmid j\}$ . On peut encore écrire pour tout  $n \in \mathbb{N}$ ,

$$x = \sum_{(i,\gamma) \in I, i \leq n} \beta_{i,\gamma} \eta_i^\gamma \pmod{\mathfrak{a}_n},$$

en regroupant les termes comme expliqué précédemment. Une telle écriture est alors unique : il n'y a aucune sous-somme finie de  $\sum_{(i,\gamma) \in I} \beta_{i,\gamma} \eta_i^\gamma$  égale à un élément non nul de  $K$ , et aucun  $\beta_{i,\gamma} \eta_i^\gamma$  non nul n'est de valuation positive. En effet, si  $\gamma - \lambda p^i \in \{\tau + 1, \dots, \rho\}$  et  $\gamma - (\lambda + 1)p^i \notin \{\tau + 1, \dots, \rho\}$ , alors dès que  $\beta_{i,\gamma}$  est non nul, on a  $ev(\beta_{i,\gamma}) \leq \lambda$ , et donc  $ev(\beta_{i,\gamma}) < \lambda + \frac{\tau}{p^i} \leq -ev(\eta_i^\gamma)$ . On peut donc bien définir une application de  $H^1(G, \mathcal{O}_{\bar{K}})$  vers  $\mathcal{O}_{\bar{K}}^f$ , qui à  $x$  associe les  $\beta_{i,\gamma}$ .

**PROPOSITION 2.10.** — *Soit  $r \geq 1$  et  $H_{\pi^r}$  le sous-module de  $\pi^r$ -torsion de  $H^1(G, \mathcal{O}_{\bar{K}})$ , alors  $H^1(G, \mathcal{O}_{\bar{K}}) / H_{\pi^r}$  est un  $\mathcal{O}_K$ -module de type fini engendré par au plus  $\frac{pe}{r(p-1)^2}$  éléments.*

*Démonstration.* — On note  $I_r = \{(i, \gamma) \in I, rp^i < \gamma\}$ . La  $\pi^r$ -torsion de  $H^1(G, \mathcal{O}_{\bar{K}})$  est l'ensemble des  $x \in H^1(G, \mathcal{O}_{\bar{K}})$  tels que  $\pi^r x = 0$ , c'est à dire  $v(\pi^r x) \geq 0$ . En associant à  $x$  la famille des  $\beta_{i,\gamma}$  et en considérant les valuations,  $\pi^r x = 0$  si et seulement si pour tout  $(i, \gamma) \in I$ ,  $\frac{r}{e} + v(\beta_{i,\gamma}) \geq \frac{\gamma}{ep^i}$ .

Notons  $H_{\pi^r}$  le sous-module de  $\pi^r$ -torsion de  $H^1(G, \mathcal{O}_{\bar{K}})$ , la proposition et les calculs précédents montrent que l'application composée

$$\mathcal{O}_K^{I_r} \rightarrow \sum_{(i, \gamma) \in I_r} \eta_i^\gamma \mathcal{O}_K \rightarrow H^1(G, \mathcal{O}_{\bar{K}})/H_{\pi^r}$$

est surjective. Le  $\mathcal{O}_K$ -module  $H^1(G, \mathcal{O}_{\bar{K}})/H_{\pi^r}$  est donc de type fini, engendré par des éléments en nombre fini majoré par le cardinal de  $I_r$ . À  $i$  fixé, il y a au plus  $p^i$  éléments de la forme  $(i, \gamma)$  dans  $I$ . De plus, si  $(i, \gamma) \in I_r$ ,  $p^i < \frac{p}{r}$  et donc  $i < \log_p(\rho/r)$ . Le cardinal de  $I_r$  est donc majoré par  $\sum_{1 \leq i < \log_p(\rho/r)} p^i$ . Cette somme est majorée par  $\frac{\log_p(\rho/r)}{p-1} \leq \frac{pe}{r(p-1)^2}$ .  $\square$

*Remarque 2.11.* — Le  $\mathcal{O}_K$ -module  $H_\pi$  a une structure naturelle de  $k$ -espace vectoriel, on a un morphisme injectif  $H_\pi \rightarrow k^{\mathbb{N}}$ , et il semble possible d'espérer que les résultats de Kedlaya s'adaptent pour montrer que l'image de cette injection peut se décrire en terme de suites twist-récurrentes dans leur définition la plus générale (voir [6] et [7]). Nous ne ferons pas ici cette interprétation.

*Remarque 2.12.* — Les méthodes utilisées dans cet article peuvent peut-être se généraliser au calcul de  $H^1(G, GL_n(\mathcal{O}_{\bar{K}}))$ . En effet, en utilisant la suite exacte

$$1 \rightarrow GL_n(K)/GL_n(\mathcal{O}_K) \rightarrow GL_n(\bar{K})/GL_n(\mathcal{O}_{\bar{K}}) \rightarrow H^1(G, GL_n(\mathcal{O}_{\bar{K}})) \rightarrow 1,$$

et la réduction de Hermite des éléments de  $GL_n(\mathcal{O}_{\bar{K}})$ , on devrait pouvoir donner une description de  $H^1(G, GL_n(\mathcal{O}_{\bar{K}}))$ , ce qui pourrait donner un avatar de la théorie de Sen dans le cas des représentations de torsion.

**Remerciements.** Je tiens à remercier ici Xavier Caruso<sup>(1)</sup> pour ses nombreuses et pertinentes remarques, ses relectures constructives de ma prose, et en particulier pour la suggestion qui est la clé de ce travail, à savoir le fait de s'intéresser aux extensions engendrées par des racines de l'uniformisante. Je remercie également le referee pour ses remarques, ainsi que sa relecture minutieuse de ce travail.

## BIBLIOGRAPHIE

- [1] J. AX, « Zeros of polynomials over local fields », *Journal of Algebra* **15** (1970), p. 417-428.
- [2] C. BREUIL, « Une application du corps des normes », *Compositiones Mathematicae* **117** (1999), p. 189-203.

---

(1) IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

- [3] X. CARUSO, «  $\mathbf{F}_p$ -représentations semi-stables », préprint, 2008.
- [4] P. COLMEZ, « Notes du cours de M2 », Corps locaux, <http://people.math.jussieu.fr/colmez>.
- [5] ———, « Notes du cours de M2 », Introduction aux anneaux de Fontaine, <http://people.math.jussieu.fr/colmez>.
- [6] K. KEDLAYA, « The algebraic closure of the power series field in positive characteristic », *Proceedings of the American Mathematical Society* **129** (2001), p. 3461-3470.
- [7] ———, « Power Series and  $p$ -adic Algebraic Closures », *Journal of Number Theory* **89** (2001), p. 24-339.
- [8] S. SEN, « On automorphisms of local fields », *Annals of Mathematics* **90** (1969), p. 33-46.
- [9] J.-P. SERRE, *Corps locaux*, Hermann, 1968.
- [10] J. TATE, «  $p$ -divisible groups », in *Proceedings of a conference on Local fields* (Driebergen), Springer, 1966, p. 158-183.
- [11] J.-P. WINTENBERGER, « Le corps des normes de certaines extensions infinies de corps locaux ; applications », *Annales Scientifiques de l'Ecole Normale Supérieure* **16** (1983), p. 59-89, 4ème série.

Manuscrit reçu le 9 janvier 2009,  
révisé le 28 septembre 2009,  
accepté le 19 octobre 2009.

Jérémy LE BORGNE  
Université de Rennes 1  
IRMAR  
Campus de Beaulieu  
35042 Rennes Cedex (France)  
[jeremy.le-borgne@univ-rennes1.fr](mailto:jeremy.le-borgne@univ-rennes1.fr)