Autour du théorème d'Ax-Sen-Tate.

Jérémy Le Borgne

Table des matières

Introduction

Soit p un nombre premier, on note $\mathbb{Q}_p$ le corps des nombres p-adiques, $\overline{\mathbb{Q}_p}$ sa clôture algébrique, et $\mathbb{C}_p$ le complété de $\overline{\mathbb{Q}_p}$ pour la distance p-adique.

Ce document présente deux points de vue pour la démonstration du théorème d'Ax-Sen-Tate. Une version simplifiée de ce théorème peut s'énoncer ainsi :

Théorème 1 (Ax-Sen-Tate)**.** *Soit $\mathcal{G} = Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Alors $\mathbb{C}_p^{\mathcal{G}} = \mathbb{Q}_p$.*

La démonstration d'Ax, décrite dans la première partie, est très astucieuse et plus élémentaire que celle de Tate. Cette dernière utilise des arguments de théorie de la ramification d'ordre supérieur, et s'intéresse également à la cohomologie de $\mathcal{G}$ dans $\mathbb{C}_p$. Ces outils seront brièvement présentés avant que nous exposions la démonstration de Tate.

1 Théorème d'Ax-Sen-Tate : la démonstration d'Ax

Si L est une extension finie de $\mathbb{Q}_p$, on note $\mathcal{G}_L$ le groupe de Galois absolu de L. La valuation p-adique sur L normalisée par $v(\pi) = 1$ (si π est une uniformisante de L) est notée v_L, la valuation normalisée sur $\mathbb{Q}_p$ étant notée v.

Théorème 1.1 (Ax)**.** *Soit L une extension finie de $\mathbb{Q}_p$. Soit $x \in \mathbb{C}_p$. On suppose qu'il existe $A \in \mathbb{R}$ tel que*

$$\forall \sigma \in \mathcal{G}_L,\ v(x - \sigma(x)) \geq A.$$

Alors il existe $y \in L$ tel que

$$v(x - y) \geq A - \frac{p}{(p-1)^2}.$$

La démonstration de ce théorème repose sur le lemme suivant :

Lemme 1.1. *Soit $P \in \overline{\mathbb{Q}_p}[X]$ unitaire de degré n, tel que toute racine α de P vérifie $v(\alpha) \geq A$. Alors :*

- *si $n = p^k d$ avec $d > 1$ non divisible par p, alors $P^{(p^k)}$ a au moins une racine β telle que $v(\beta) \geq A$,*
- *si $n = p^{k+1}$, alors $P^{(p^k)}$ a au moins une racine β telle que $v(\beta) \geq A - \frac{1}{p^k(p-1)}$.*

Démonstration. On écrit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = (X - \alpha_1)\dots(X - \alpha_n)$, avec les $a_i \in \overline{\mathbb{Q}_p}$. On sait que

$$\forall i \in 1, \dots, n,\ a_{n-i} = (-1)^i \sum_{\{j_1,\dots,j_i\} \subset \{1,\dots,n\}} \prod \alpha_{j_1} \dots \alpha_{j_i}.$$

Ainsi,

$$v(a_{n-i}) = v\left(\sum_{\{j_1,\dots,j_i\} \subset \{1,\dots,n\}} \prod \alpha_{j_1} \dots \alpha_{j_i}\right) \geq \inf_{\{j_1,\dots,j_i\} \subset \{1,\dots,n\}} v\left(\prod \alpha_{j_1} \dots \alpha_{j_i}\right) \geq iA.$$

D'autre part,

$$\frac{1}{p^k!}P^{(p^k)} = \sum_{i=0}^{n-p^k} \binom{n-i}{p^k} a_{n-i} X^{n-p^k-i}.$$

En particulier, le produit des racines de $P^{(p^k)}$ est $\pm a_{p^k}/\binom{n}{p^k}$. Or

$$v\left(a_{p^k}/\binom{n}{p^k}\right) \geq (n-p^k)A - v\left(\binom{n}{p^k}\right).$$

Comme $\binom{n}{p^k} = \frac{n(n-1)\ldots(n-p^k+1)}{p^k(p^k-1)\ldots 1}$, et que pour tout $i \in \{1,\ldots,p^k-1\}$, $v(n-i) = v(i)$ (car n est multiple de p^k), on a

$$v\left(a_{p^k}/\binom{n}{p^k}\right) \geq (n-p^k)A - v\left(\frac{n}{p^k}\right).$$

Le membre de gauche étant la somme des valuations des $n-p^k$ racines de $P^{(p^k)}$, on en déduit qu'il existe une racine β de $P^{(p^k)}$ vérifiant

$$v(\beta) \geq A - \frac{1}{n-p^k} v\left(\frac{n}{p^k}\right) \geq \begin{cases} A & \text{si } n = p^k d \text{ avec } d > 1 \\ & \text{non divisible par p} \\ A - \frac{1}{p^k(p-1)} & \text{si } n = p^{k+1}, \end{cases}$$

d'où le lemme.
On en déduit le théorème d'Ax. En effet, soit d'abord $x \in \overline{\mathbb{Q}_p}$ comme dans l'énoncé du théorème. Soit P le polynôme minimal unitaire de x sur L, et soit n le degré de P. On va montrer par récurrence sur n qu'il existe $y \in L$ tel que

$$v(x-y) \geq A - \sum_{k=0}^{\lfloor \frac{\log n}{\log p} \rfloor - 1} \frac{1}{p^k(p-1)} \geq A - \sum_{k=0}^{+\infty} \frac{1}{p^k(p-1)} = A - \frac{p}{(p-1)^2}.$$

Pour $n = 1$, le résultat est évident avec $y = x$.
Pour $n \geq 1$, n est de l'une des deux formes considérées dans le lemme. Par hypothèse sur x, les racines α de $P(X+x)$ vérifient toutes $v_p(\alpha) \geq A$ (car α est racine de $P(X+x)$ si et seulement si il existe $\sigma \in \mathcal{G}_L$ tel que $\alpha + x = \sigma(x)$, *i.e.* $\alpha = \sigma(x) - x$).
On sait donc que (k étant défini comme dans le lemme), $P^{(p^k)}(X+x)$ a une racine y_0 de valuation supérieure ou égale à A si n n'est pas une puissance de p, et à $A - \frac{1}{p^k(p-1)}$ si $n = p^{k+1}$.
On applique maintenant l'hypothèse de récurrence à $x + y_0$, dont le polynôme minimal est de degré au plus $n - p^k$. On a

$$\left\lfloor \frac{\log(n-p^k)}{\log p} \right\rfloor = \begin{cases} \left\lfloor \frac{\log(n)}{\log p} \right\rfloor & \text{si } n \text{ n'est pas une puissance de } p \\ \left\lfloor \frac{\log(n)}{\log p} \right\rfloor - 1 & \text{si } n \text{ est une puissance de } p, \end{cases}$$

Ainsi, par hypothèse de récurrence, il existe un $y \in L$ tel que

$$v_p(x+y_0-y) \geq \begin{cases} A & -\sum_{j=0}^{\lfloor \frac{\log n}{\log p} \rfloor - 1} \frac{1}{p^j(p-1)} \\ A - \frac{1}{p^k(p-1)} & -\sum_{j=0}^{\lfloor \frac{\log n}{\log p} \rfloor - 2} \frac{1}{p^j(p-1)} \end{cases} = A - \sum_{j=0}^{\lfloor \frac{\log n}{\log p} \rfloor - 1} \frac{1}{p^j(p-1)}.$$

Comme il est clair d'après le lemme que $v_p(y_0) \geq A - \sum_{j=0}^{\lfloor \frac{\log n}{\log p} \rfloor - 1} \frac{1}{p^j(p-1)}$, il en résulte que

$$v_p(x-y) \geq A - \sum_{k=0}^{\lfloor \frac{\log n}{\log p} \rfloor - 1} \frac{1}{p^k(p-1)},$$

ce qui achève la récurrence.

On suppose maintenant $x \in \mathcal{O}_{\mathbb{C}_p}$, on note $x_n = x \mod p^n$. Pour tout n, $x_n \in \mathcal{O}_{\overline{\mathbb{Q}_p}}$. Ainsi, il existe $y_n \in \mathcal{O}_L$ tel que $v(x_n - y_n) \geq A - \frac{p}{(p-1)^2}$. On a alors $v(x-y_n) \geq A - \frac{p}{(p-1)^2}$ pour n assez grand, d'où le théorème d'Ax.

Corollaire 1.1. *Soit L une extension finie de $\mathbb{Q}_p$, $\mathcal{G}_L = Gal(\bar{L}/L)$, alors*

$$\mathbb{C}_p^{\mathcal{G}_L} = L.$$

Démonstration. Soit $x \in \mathcal{O}_{\overline{\mathbb{Q}_p}}^{\mathcal{G}_L}$. On a pour tout $n \in \mathbb{N}$ et pour tout $g \in \mathcal{G}_L$:

$$v(gx - x) \geq n.$$

D'après le théorème d'Ax, il existe $y_n \in L$ tel que $v(x_n - y_n) \geq n - \frac{p}{(p-1)^2}$. Par conséquent, $y_n \to x$, et donc $x \in \mathcal{O}_L$.

La démonstration de Sen et Tate, utilisant des raisonnements de théorie de la ramification d'ordre supérieur, n'explicite pas la constante qui apparaît ici $\frac{p}{(p-1)^2}$.

2 Groupes de ramification et différente

2.1 Groupes de ramification

Soit K un corps muni d'une valuation discrète de caractéristique 0, k_K son corps résiduel étant supposé parfait de caractéristique $p > 0$. On sait alors que toutes les extensions de k_K sont séparables, et si L est une extension finie de K, alors $\mathcal{O}_L$ est monogène sur $\mathcal{O}_K$.
Soit L une extension finie de K, v la valuation normalisée de L, x un générateur de la $\mathcal{O}_K$ algèbre $\mathcal{O}_L$. On note $G = Gal(L/K)$, $\mathfrak{m}_K$ et $\mathfrak{m}_L$ les idéaux maximaux respectifs de $\mathcal{O}_K$ et $\mathcal{O}_L$.
On note $e(L/K)$ l'indice de ramification de L sur K, c'est à dire la multiplicité de $\mathfrak{m}_L$ dans $\mathfrak{m}_K$.

Lemme 2.1. *Soit $s \in G$, i un entier ≥ -1. Les trois assertions suivantes sont équivalentes :*

(i) *s opère trivialement sur $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$.*

(ii) *$v(s(a)-a) \geq i+1$ pour tout $a \in \mathcal{O}_L$.*

(iii) *$v(s(x)-x) \geq i+1$.*

Démonstration. $v(s(a)-a) \geq i+1$ signifie que $s(a) \in a + \mathfrak{m}_L^{i+1}$, d'où l'équivalence entre (i) et (ii). Il est clair que $(ii) \Rightarrow (iii)$.

Enfin, si $a \in \mathcal{O}_L$, il existe $P \in \mathcal{O}_K[X]$ tel que $a = P(x)$. Ainsi, $s(a) - a = P(s(x)) - P(x)$ est divisible par $s(x) - x$, et donc $s(a) - a \geq s(x) - x$, d'où $(iii) \Rightarrow (ii)$.

Définition 2.1. *On pose $i(s) = v(s(x) - x)$, ce qui est indépendant du choix du générateur x de $\mathcal{O}_L$.*
Pour $u \in [-1, +\infty[$, on note

$$G_u = \{s \in G \ / \ i(s) \geq u + 1\}.$$

Proposition 2.1. *Pour $u \in [-1, +\infty[$, G_u est un sous-groupe distingué de G. $G_{-1} = G$, et pour u assez grand, $G_u = 1$.*

Démonstration. D'après la caractérisation (i), G_u est le noyau du morphisme $G \to Aut(\mathcal{O}_L/\mathfrak{m}_L^{u+1})$. C'est donc un sous-groupe distingué. Il est clair que $\forall s \in G,\ s(x) - x \in \mathcal{O}_L$, donc $G_{-1} = G$, et pour $i > \max_{s \in G} i(s)$, $G_i = \{1\}$.

Remarque. Si F est un sous-corps de L contenant K et x un générateur de $\mathcal{O}_L$ sur $\mathcal{O}_K$, c'est *a fortiori* un générateur sur $\mathcal{O}_F$. Ainsi, si H est le sous-groupe de G fixant F, $H_u = G_u \cap H$.
Ainsi, cette numérotation des groupes est bien adaptée pour l'inclusion, c'est à dire lorsqu'on regarde les groupes de Galois de type $Gal(L/F)$.
On va maintenant introduire une nouvelle numérotation, bien adaptée aux passages au quotient, c'est à dire lorsque l'on s'intéresse aux groupes de type $Gal(F/K)$. On indexera désormais les applications i en fonction du corps sur lequel agit l'automorphisme s auquel elles s'appliquent.

Proposition 2.2. *Soit H un sous-groupe distingué de G, et $F = L^H$. Alors, si $\sigma \in G/H$, on a*

$$i_F(\sigma) = \frac{1}{e(L/F)} \sum_{s \to \sigma} i_L(s).$$

La notation précédente indique que la somme porte sur les s qui s'envoient sur σ par la surjection canonique $G \to G/H$. *Démonstration.* Si $\sigma = 1$, les deux membres valent $+\infty$, on suppose donc $\sigma \neq 1$. Soit x (resp. y) un génŕateur de $\mathcal{O}_L$ (resp. $\mathcal{O}_F$) sur $\mathcal{O}_K$. Il s'agit de montrer que les deux éléments $a = y - \sigma(y)$ et $b = \prod_{s \to \sigma}(x - s(x))$ engendrent le même idéal de $\mathcal{O}_L$.
Soit P le polynôme minimal de x sur $\mathcal{O}_F$. $P = \prod_{h \in H}(X - h(x))$. Si $s_0 \in G$ a pour image σ dans G/H, les autres antécédents de σ sont de la forme $s_0 h$ avec $h \in H$. $P - s_0(P)$ a tous ses coefficients divisibles par $y - s_0(y)$ (y engendre $\mathcal{O}_F$) et en l'évaluant en x, on voit que $a|b$.
Réciproquement, soit $Q \in \mathcal{O}_K[X]$ tel que $y = Q(x)$. $Q(X) - \sigma(y)$ s'annule pour $X = s_0 h(x)$ car $Q(s_0 h(x) = s_0 h(Q(x)) = \sigma(y)$. Il est donc divisible dans $\mathcal{O}_F[X]$ par $s_0(P)$. En évaluant en x, il vient $b|a$.

Définition 2.2. *On définit*

$$\varphi_{L/K}(u) = \int_{-1}^{u} \frac{dt}{(G_0 \ : \ G_t)} = \int_{-1}^{u} \frac{|G_t|}{|G_0|} dt,$$

en convenant que pour $-1 \leq t \leq 0$, $(G_0 \ : \ G_t)$ représente l'inverse de $(G_t \ : \ G_0)$.

On vérifie aisément que φ est continue, affine par morceaux, croissante, concave, et qu'elle réalise un homéomorphisme de $[-1, +\infty[$ sur lui-même. On note ψ l'application réciproque.

Définition 2.3. *On définit la numérotation supérieure des groupes de ramification :*

$$G^v := G_{\psi(v)}.$$

Cette numérotation présente des avantages lorsqu'il s'agit de passer au quotient :

Théorème 2.1 (Herbrand)**.** *Si H est distingué dans G, alors $(G/H)^v = G^v H/H$.*

La démonstration de ce résultat est présentée dans [Ser68], Ch. IV, paragr. 3 et nous ne la referons pas ici.

2.2 Différente d'une extension.

Définition 2.4. *Soit L une extension finie et séparable du corps K, on sait que l'homomorphisme*

$$Tr_{L/K} \ : \ L \to K$$

est surjectif, et que la forme bilinéaire $Tr(xy)$ est non dégénérée.
On note $B^* = \{y \in L \ / \ \forall x \in \mathcal{O}_L, \ Tr(xy) \in \mathcal{O}_K\}$. C'est un idéal fractionnnaire de L, c'est à dire que c'est un sous-$\mathcal{O}_K$-module de L, tel qu'il existe $x \in \mathcal{O}_L$ tel que $xB^* \subset \mathcal{O}_L$. On l'appelé codifférente *de L sur K. Son inverse s'appelle la* différente *de L sur K ; c'est en fait un idéal de $\mathcal{O}_L$. On la note $\mathfrak{d}_{L/K}$.*

On donne dans la suite sans démonstration des propriétés de la différente et quelques liens avec les groupes de ramification. Le lecteur curieux pourra consulter [Ser68].

Proposition 2.3. *Si l'extension M/L est finie et séparable, on a*

$$\mathfrak{d}_{M/K} = \mathfrak{d}_{M/L}\mathfrak{d}_{L/K}.$$

Proposition 2.4. *On a :*

$$v(\mathfrak{d}_{L/K}) = \frac{1}{e(L/K)} \sum_{s \neq 1} i(s) = \sum_{i=0}^{+\infty} (|G_i| - 1)$$

3 Cohomologie galoisienne

3.1 Cohomologie des groupes

Soit A un groupe abélien et G un groupe opérant sur A. Notant Λ l'algèbre $\mathbb{Z}[G]$ du groupe G sur $\mathbb{Z}$, on définit une structure de Λ-module sur A en posant $(\sum n_s s)a = \sum n_s(sa)$. On parlera volontiers de structure de G-module. Si A et A' sont deux G-modules, une application $f \ : \ A \to A'$ est appelée G- *homomorphisme* si c'est un homomorphisme de groupes et si elle commute aux opérations de G. Les G-homomorphismes de A dans A' forment un groupe, noté $Hom_G(A, A')$. Pour ces homomorphismes, les G-modules forment une catégorie

abélienne.

On définit la cohomologie de G à coefficients dans A de la manière suivante. On appelle i-cochaîne covariante toute application $f : G^{i+1} \to A$ vérifiant la condition (dite de *covariance*) suivante :

$$\forall g \in G,\ \forall s_0, \ldots, s_i \in G,\ f(gs_0, \ldots, gs_i) = g \cdot f(s_0, \ldots, s_i).$$

Le *cobord* df d'une i-cochaîne covariante f est une $(i+1)$-cochaîne covariante définie par :

$$df(s_0, \ldots, s_{i+1}) = \sum_{j=0}^{i+1} (-1)^j f(s_0, \ldots, \hat{s_j}, \ldots, s_{i+1}),$$

le chapeau indiquant que l'on omet la variable au-dessus de laquelle il se trouve. Une cochaîne étant bien déterminée par sa restriction aux systèmes de la forme $(1, g_1, g_1g_2, \ldots, g_1 \ldots g_i)$, on est amené à considérer les cochaînes comme des fonctions f de G^i dans A, dont le cobord est donné par

$$df(g_1, \ldots, g_{i+1}) = g_1 f(g_2, \ldots, g_i) + \sum_{j=1}^{i} f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_1, \ldots, g_i).$$

Le groupe $H^i(G, A)$ est le groupe formé par les i-cocycles, c'est à dire les i-cochaînes dont le cobord est nul, quotienté (pour $i \geq 1$) par l'ensemble des cocycles qui sont des cobords (i.e., qu'il existe un $(i-1)$-cocycle dont ils soient le cobord). En particulier, un 0-cocycle est un élément x de A vérifiant

$$\forall g \in G,\ g \cdot x - x = 0;$$

un 1-cocycle est une application $f : G \to A$ vérifiant

$$\forall g, g' \in G,\ f(gg') = gf(g') + f(g).$$

Remarque. Si on note A^G le sous-groupe de A formé des éléments invariants par G, et si $f : A \to A'$ est un G-homomorphisme, f applique A^G dans A'^G. On peut donc parler du foncteur A^G. Si on a une suite exacte de G-modules

$$0 \to A \to A' \to A'',$$

la suite de groupes abéliens

$$0 \to A^G \to A'^G \to A''^G$$

est encore exacte.
Les groupes de cohomologie de G à coefficients dans A sont les foncteurs dérivés droits du foncteur A^G. Si on a une suite exacte

$$0 \to A \to A' \to A'' \to 0,$$

alors pour tout $q \geq 0$, la suite

$$\cdots \to H^q(G, A') \to H^q(G, A'') \xrightarrow{d} H^{q+1}(G, A) \to H^{q+1}(G, A') \to \cdots$$

est exacte.

3.2 Cohomologie galoisienne.

Un cas particulier d'étude de cohomologie est celui où A est un corps et G le groupe de Galois d'une extension en lien avec ce corps. Un résultat connu, présenté dans [Ser68], est le suivant.

Théorème 3.1. *Si L est une extension galoisienne finie de K et $G = Gal(L/K)$, alors pour tout $n \in \mathbb{N}$, $H^n(G, L) = 0$. D'autre part, $H^1(G, L^*) = 0$.*

Le cas $H^1(G, L) = 0$ est connu sous le nom de Théorème Hilbert 90.

Rappelons que dans une extension infinie $K \to L$, le groupe de Galois G est la limite projective des $Gal(K'/K)$, où K' parcourt l'ensemble des extensions finies de K. Les groupes de cohomologie sont définis en considérant les cochaînes *continues* (pour la topologie de la limite projective), L étant lui muni de la topologie discrète.

4 Théorème d'Ax-Sen-Tate : point de vue cohomologique

La démonstration de Tate du théorème d'Ax-Sen-Tate, utilisant des raisonnements de cohomologie galoisienne, est certainement moins élémentaire que celle d'Ax, mais nettement plus instructive.

4.1 Étude d'une extension totalement ramifiée.

On note $K = \mathbb{Q}_p$. On note $C = \mathbb{C}_p$ la complétion de sa clôture algébrique $\bar{K}$. On étend de manière canonique la valeur absolue de K à C, on note π une uniformisante de K.
Soit $K_n = K(\sqrt[p^n]{1})$, extension galoisienne de K de groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$. On pose $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$, de groupe $\mathcal{C} = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^* = \mathbb{Z}_p^*$.
Soit X la complétion de K_∞ dans C.

Théorème 4.1. *$H^0(\mathcal{C}, X) = K$ et $H^1(\mathcal{C}, X)$ est un K-espace vectoriel de dimension 1.*

On va voir X comme somme directe de K et d'un certain sous-espace X_0 dont on montrera que les groupes de cohomologie H^0 et H^1 sont triviaux. Précisons cette idée.

Définition 4.1. *Pour $x \in K_n$, on pose $t(x) = p^{-n}Tr_{K_n/K}(x)$. Cette définition est indépendante de n et permet donc de définir t sur K_∞.*

En effet, si $x \in K_n$, $Tr_{K_{n+1}/K}(x) = pTr_{K_n/K}(x)$ car $[K_{n+1} : K_n] = p$.
On va d'abord montrer que t est continue sur K_∞.

Proposition 4.1. *On a :*

$$v(\mathfrak{d}_{K_n/K}) = n - \frac{p}{p-1} + p^{-n}\frac{p}{p-1}.$$

Démonstration. Les groupes de ramification G_u de $Gal(K_n/K)$ sont donnés par :

$$G_u = Gal(K_n/K_r) \text{ si } p^{r-1} \leq u \leq p^r - 1.$$

Ainsi, $|G_u| = p^{n-r}$ pour $p^{r-1} \leq u \leq p^r - 1$.
D'après la formule reliant la valuation de la différente et les cardinaux des groupes de Galois numérotés, on a :

$$e(K_n/K)v(\mathfrak{d}_{K_n/K}) = \sum_{i=1}^{+\infty}(|G_i| - 1).$$

Par conséquent, on a

$$e(K_n/K)v(\mathfrak{d}_{K_n/K}) = \sum_{i=1}^{n}(p^{n-i} - 1)(p^i - p^{i-1}) = np^{n-1}(p-1) - p^n - 1.$$

De plus, $e(K_n/K) = [K_n/K] = p^{n-1}(p-1)$. Finalement, on obtient :

$$v(\mathfrak{d}_{K_n/K}) = n - \frac{p}{p-1} + \frac{1}{p^{n-1}(p-1)} = n - \frac{p}{p-1} + p^{-n}\frac{1}{1-\frac{1}{p}}.$$

Corollaire 4.1. $v(\mathfrak{d}_{K_{n+1}/K_n}) = 1 - p^{-n}$.

Démonstration. Cela résulte de la multiplicativité de la différente : $\mathfrak{d}_{K_{n+1}/K} = \mathfrak{d}_{K_{n+1}/K_n}\mathfrak{d}_{K_n/K}$. On a donc $v(\mathfrak{d}_{K_{n+1}/K_n}) = v(\mathfrak{d}_{K_{n+1}/K}) - v(\mathfrak{d}_{K_n/K}) = 1 + p^{-n}\frac{1}{1-\frac{1}{p}}\left(\frac{1}{p} - 1\right)$.

Corollaire 4.2. *Pour $x \in K_{n+1}$,*

$$|Tr_{K_{n+1}/K_n}(x)| \leq |p|^{1-ap^{-n}}|x|$$

avec $a = \left(\frac{p}{p-1}\right)^2$.

Démonstration. Notons $\mathcal{O}_n$ l'anneau de valuation de K_n et $\mathfrak{m}_n$ son idéal maximal. Soit $\mathfrak{d}_{K_{n+1}/K_n} = \mathfrak{m}_{n+1}^d$. Alors on sait, d'après [Ser68], Ch. V, paragr. 3, Lemme 4, que

$$Tr_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}_n^j,$$

avec $j = \left\lfloor \frac{i+d}{p} \right\rfloor$.
Comme $v(\mathfrak{m}_n) = p^{-n}\frac{1}{p-1}$, $d = p^n(p-1) - p(p-1)$. Ainsi, si $x \in \mathfrak{m}_{n+1}^i \setminus \mathfrak{m}_{n+1}^{i+1}$, on a

$$v(Tr_{K_{n+1}/K}(x)) \geq \left(\frac{d+i}{p} - 1\right)\frac{1}{p^{n-1}(p-1)} = 1 - \alpha_n p^{-n} + \frac{i}{p^n(p-1)}.$$

(avec $\alpha_n = \frac{1}{p^{n-1}} + \frac{1}{p^{n-1}(p-1)} \leq \left(\frac{p}{p-1}\right)^2 = a$). Comme $v(x) = \frac{i}{p^n(p-1)}$, il vient

$$|Tr_{K_{n+1}/K_n}(x)| \leq |p|^{1-ap^{-n}}|x|.$$

On a finalement le corollaire suivant, qui nous fournit la continuité de t :

Corollaire 4.3. *On a pour $x \in K_n$,*

$$|Tr_{K_n/K}(x)| \leq |p|^{n-c}|x|,$$

avec $c = \left(\frac{p}{p-1}\right)^3$.

Rappelons que si l'on a une tour d'extensions $K \to L \to M$, alors $Tr_{M/K} = Tr_{M/L} \circ Tr_{L/K}$. Ainsi, l'inégalité du Corollaire 4.2 se propage en

$$|Tr_{K_n/K}(x)| \leq |p|^{\sum_{k=0}^{n-1}(1-ap^{-k})}|x| \leq |p|^{n-\frac{ap}{p-1}}|x|.$$

On sait maintenant que l'application linéaire t est continue sur K_∞. On la prolonge en une application linéaire continue (toujours notée t) sur X. On note $X_0 = \ker t$.
$t^2(x) = t(x)$ pour tout $x \in X$, donc $X = X_0 \oplus t(X)$. De plus, t est surjectif (car son image est non nulle et c'est un sous-espace vectoriel de K, c'est donc K). Ainsi, $X = X_0 \oplus K$. Soit σ un générateur de $\mathcal{C}$. La prochaine étape de notre raisonnement consiste à montrer que $H^0(\mathcal{C}, X_0) = H^1(\mathcal{C}, X_0) = 0$ (σ stabilise X_0, cette écriture a donc un sens). Pour cela, on montre que $(\sigma - 1)_{|X_0}$ est un homéomorphisme.

Lemme 4.1. *Pour $x \in K_{n+1}$, on a*

$$|x - p^{-1}Tr_{K_{n+1}/K_n}(x)| \leq p|\sigma^{p^n}x - x|.$$

Démonstration. Soit $\tau = \sigma^{p^n}$. τ est un générateur de $Gal(K_{n+1}/K_n)$ (il est bien dans ce groupe, et d'ordre p), donc :

$$\begin{aligned} px - Tr_{K_{n+1}/K_n}(x) &= \sum_{k=0}^{p-1}(x - \tau^k(x)) \\ &= \sum_{k=1}^{p-1}(1 + \tau + \cdots + \tau^{k-1})(1-\tau)(x). \end{aligned}$$

Ainsi, comme $|\tau x| = |x|$, on a

$$|px - Tr_{K_{n+1}/K_n}(x)| \leq |(1-\tau)x|$$

et on divise par $|p| = p^{-1}$.

Proposition 4.2. *Il existe une constante $d > 0$ telle que pour tout $x \in K_\infty$,*

$$|x - t(x)| \leq d|\sigma x - x|.$$

Démonstration. On montre par récurrence sur n l'inégalité

$$|x - t(x)| \leq c_n|\sigma x - x| \text{ si } x \in K_n$$

avec $c_{n+1} = |p|^{-ap^{-n}}c_n$. On aura alors $c_n \leq c_1|p|^{-a\frac{p}{p-1}}$, ce qui démontrera la proposition.
Pour $n = 1$, on a

$$|x - t(x)| = |x - p^{-1}Tr_{K_1/K}(x)| \leq p|\sigma x - x|,$$

on peut prendre $c_1 = p$.
Pour $n \geq 1$, on se donne $x \in K_{n+1}$. Par hypothèse de récurrence, on a

$$\begin{aligned} |Tr_{K_{n+1}/K_n}(x) - t(Tr_{K_{n+1}/K_n}(x))| &\leq c_n|\sigma Tr_{K_{n+1}/K_n}(x) - Tr_{K_{n+1}/K_n}(x)| \\ |Tr_{K_{n+1}/K_n}(x) - p^{-n}Tr_{K_n/K}(Tr_{K_{n+1}/K_n}(x))| &\leq c_n|Tr_{K_{n+1}/K_n}(\sigma x - x)| \\ |Tr_{K_{n+1}/K_n}(x) - pt(x)| &\leq c_n|p|^{1-ap^{-n}}|\sigma x - x| \end{aligned}$$

En utilisant l'inégalité ultramétrique, on a alors

$$\begin{aligned} |x - t(x)| &\leq \max(|x - p^{-1}Tr_{K_{n+1}/K_n}(x)|, |p|^{-ap^{-n}}c_n|\sigma x - x|) \\ &\leq \max(p, |p|^{-ap^{-n}}c_n)|\sigma x - x| \\ &= p^{ap^{-n}}c_n|\sigma x - x|. \end{aligned}$$

Proposition 4.3. *L'opérateur $\sigma - 1$ annule K et induit un homéomorphisme de X_0 sur lui-même.*

Démonstration. La première partie de la proposition est claire.
Pour $n \in \mathbb{N}$, on pose $K_{n,0} = K_n \cap X_0$, et $K_{\infty,0} = \bigcup_{n\in\mathbb{N}} K_{n,0}$. On a $K_n = K \oplus K_{n,0}$, et X_0 est l'adhérence de $K_{\infty,0}$ dans X. Sur chacun des $K_{n,0}$, l'opérateur $\sigma - 1$ est injectif. En effet, si $x \in K_{n,0}$ et $\sigma x = x$, alors $x = t(x) = 0$. $K_{n,0}$ étant de dimension finie sur K, $\sigma - 1$ est une bijection de $K_{n,0}$. Il réalise donc une bijection de $K_{\infty,0}$.
Soit ρ son inverse, la proposition précédente montre que si $x \in K_{n,0}$,

$$|x| \leq d|\sigma x - x|,$$

c'est à dire que pour tout $y = (\sigma - 1)x \in K_{\infty,0}$, $|\rho y| \leq y$.
Par conséquent, on peut prolonger ρ par continuité à X_0, et ce prolongement est un inverse continu de $\sigma - 1$.

On peut maintenant démontrer le théorème principal de cette partie. En effet, $H^0(\mathcal{C}, X) = X^{\mathcal{C}} = K \oplus X_0^{\mathcal{C}}$. Or $X_0^{\mathcal{C}} = \ker((\sigma - 1)_{|X_0}) = 0$. Donc

$$H^0(\mathcal{C}, X) = K.$$

D'autre part, un 1-cocycle est déterminé par sa valeur en σ (car alors, $f(\sigma^k) = \sum_{i=0}^{k-1} \sigma^i f(\sigma)$). Par conséquent, comme $\sigma - 1$ est bijectif, pour un 1-cocyle f il existe $x \in X_0$ tel que $f(\sigma) = \sigma x - x$, et donc f est un cobord, d'où $H^1(\mathcal{C}, X_0) = 0$ et donc $H^1(\mathcal{C}, X)$ est un K-espace vectoriel de dimension 1.

4.2 Extensions finies de K_∞.

On note $\mathcal{G} = Gal(\bar{K}/K)$. On va utiliser l'étude précédente couplée à celle des extensions finies de K_∞ pour décrire la cohomologie de $\mathcal{G}$ à coefficients dans C.
Soit L une extension finie de K_∞, et $\mathcal{H} = Gal(\bar{K}/K_\infty)$.

Proposition 4.4.

$$\mathfrak{m}_\infty \subset Tr_{L/K_\infty}(\mathcal{O}_L)$$

Démonstration. D'après [Ser68], Ch. V, paragr. 4, Lemme 6, on peut supposer qu'il existe une extension galoisienne finie L_0 de K, linéairement disjointe de K_∞ sur K, telle que $L = L_0K_\infty$. Soit $L_n = L_0K_n$. Alors, d'après la Proposition 2.4 et la transitivité de la différente,

$$v(\mathfrak{d}_{L_n/K_n}) = \int_{-1}^{+\infty} \left(\frac{1}{|Gal(K_n/K)^v|} - \frac{1}{|Gal(L_n/K)^v|} \right) dv.$$

D'après le théorème de Herbrand, on sait que

$$Gal(L_0/K)^v = \{1\} \Leftrightarrow Gal(L_n/K)^v \subset Gal(L_n/L_0)^v$$

et

$$Gal(K_n/K)^v = Gal(L_n/K)^v / (Gal(L_n/K)^v \cap Gal(L_n/K_n)).$$

Comme $Gal(L_n/K_n) \cap Gal(L_n/L_0) = \{1\}$ (un automorphisme de L_n préservant L_0 et K_n est trivial), si $Gal(L_0/K)^v = \{1\}$ on a $Gal(L_n/K)^v \cap Gal(L_n/K_n) = \{1\}$ et donc

$$|Gal(K_n/K)^v| = |Gal(L_n/K)^v|.$$

Soit $h \geq 0$ tel que $Gal(L_0/K)^h = \{1\}$. On a

$$v(\mathfrak{d}_{L_n/K_n}) \leq \int_{-1}^{h} \frac{dv}{|Gal(K_n/K)^v|} \leq C \cdot p^{-n},$$

où C est une constante positive, en vertu des calculs des cardinaux de groupes de ramification de K_n/K menés dans la démonstration de la Proposition 4.1. On sait alors que

$$v(Tr_{L_n/K_n}(\mathfrak{m}_{L_n})) \leq \frac{1}{e(L_n/K)} + v(\mathfrak{d}_{L_n/K_n}),$$

et donc

$$v(Tr_{L_n/K_n}(\mathfrak{m}_{L_n}))_{n \to +\infty} 0.$$

Ainsi, un élément de $\mathfrak{m}_\infty$ se trouve dans $Tr_{L_n/K_n}(\mathfrak{m}_{L_n})$ pour n assez grand, et donc dans $Tr_{L/K_\infty}(\mathcal{O}_L)$.

Corollaire 4.4. *Soit L une extension galoisienne finie de K_∞ de groupe de Galois G, et soit $x \in L$ et $c > 1$. Alors il existe $y \in L$ tel que*

$$|x - Tr_{L/K_\infty}(y)| \leq c \max_{\sigma \in G} |\sigma x - x| \text{ et } |y| \leq c|x|.$$

Démonstration Soit $z \in K_\infty$ tel que $|z| > c^{-1}$. D'après la Proposition 4.4, il existe un $y_0 \in \mathcal{O}_L$ tel que $Tr_{L/K_\infty}(y_0) = z$.
On pose $y = \frac{1}{z} y_0 x$. Alors $|y| \leq c|x|$ et

$$Tr_{L/K\infty}(y) = \frac{1}{z} \sum_{\sigma \in G} \sigma(y_0)\sigma(x) = \frac{1}{z} \sum_{\sigma \in G} \sigma(y_0)(\sigma x - x + x) = x + \sum_{\sigma \in G} \sigma(y_0)(\sigma x - x).$$

Ainsi,

$$|Tr_{L/K_\infty}(y) - x| \leq c \max_{\sigma \in G} |\sigma x - x|.$$

Remarque. Ceci nous dit qu'en particulier, si $x \in L^G$, alors $x \in K_\infty$.

Corollaire 4.5. *Soit $x \in \bar{K}$ et $c > 1$. Alors, il existe $y \in K_\infty$ tel que*

$$|x - y| \leq c \max_{\sigma \in \mathcal{H}} |\sigma x - x|.$$

En particulier, $H^0(\mathcal{H}, \bar{K}) = K_\infty$.

Démonstration. Soit L une extension galoisienne finie de K_∞ contenant x, de groupe de Galois G. Soit $\Gamma = Gal(\bar{K}/L)$. D'après le Corollaire 4.4, il existe $y \in K_\infty$ tel que

$$|x - y| \leq c \max_{\sigma \in G} |\sigma x - x|.$$

De plus, si $\sigma \in \mathcal{H}$, σx ne dépend que de la classe de σ modulo Γ (car x est fixé par les éléments de Γ), et donc

$$|x - y| \leq c \max_{\sigma \in \mathcal{H}} |\sigma x - x|.$$

Corollaire 4.6. *Soit L/K_∞ une extension galoisienne finie de groupe G. Soit f une 1-cochaîne de G à coefficients dans L, et soit $c > 1$. Alors il existe une 0-cochaîne $g \in L$ telle que*

$$|f - dg| \leq c|df| \text{ et } |g| \leq c|f|.$$

Ici, $|f|$ note le maximum des valeurs absolues des coefficients de f.
Démonstration. Soit $z \in \mathfrak{m}_\infty$ tel que $|z| > c^{-1}$. D'après la Proposition 4.4, il existe un $y \in \mathcal{O}_L$ tel que $Tr_{L/K_\infty}(y) = z$.
On pose

$$g = -\frac{1}{z} \sum_{s \in G} (s \cdot y) f(s).$$

Déjà, $|g| \leq c|f|$. D'autre part,

$$dg(\sigma) = \frac{1}{z} \sum_{s \in G} (s \cdot y) f(s) - (\sigma s \cdot y)(\sigma \cdot f)(s)$$

Or, on a $\sigma f(s) = df(\sigma, s) - f(\sigma) + f(\sigma s)$. Ainsi,

$$dg(\sigma) = \frac{1}{z} \sum_{s \in G} (s \cdot y) f(s) - (\sigma s \cdot y)(\delta f(\sigma, s) - f(\sigma) + f(\sigma s))$$

Par changement de variable, $\sum_{s \in G} (\sigma s \cdot y) f(\sigma s) = \sum_{s \in G} (s \cdot y) f(s)$, et donc

$$dg(\sigma) = \frac{1}{z} f(\sigma) \sum_{s \in G} sy - \sum_{s \in G} (\sigma s \cdot y) df(\sigma, s) = f(\sigma) - \frac{1}{z} \sum_{s \in G} (\sigma s \cdot y) df(\sigma, s).$$

On en déduit que

$$|(f - dg)(\sigma)| \leq c| \sum_{s \in G} (\sigma s \cdot y) df(\sigma, s)| \leq c|df|.$$

Corollaire 4.7. *Le groupe $\mathcal{H}$ étant muni de la topologie de la limite projective et $\bar{K}$ de la topologie discrète, soit f une 1-cochaîne continue de $\mathcal{H}$ à valeurs dans $\bar{K}$. Soit $c > 1$. Alors il existe $g \in \bar{K}$ tel que*

$$|f - dg| \leq c|df| \text{ et } |g| \leq c|f|.$$

Démonstration. Soit f une cochaîne continue de $\mathcal{H}$ dans $\bar{K}$. $\{f^{-1}(x)\}_{x\in\bar{K}}$ est compacte, on peut donc la recouvrir par un nombre fini d'ouverts, et donc par un nombre fini de translatés de groupes de la forme $Gal(L/K_\infty)$ ($[L : K_\infty]$ fini). L'extension engendrée par ces L est une extension M finie de $\bar{K}$, et pour $\sigma \in \mathcal{H}$, $f(\sigma)$ ne dépend que de la classe de σ dans $Gal(M/K_\infty)$. En particulier, f vérifie les propriétés du Corollaire 4.6.

Proposition 4.5. *On a :*

$$H^0(\mathcal{H}, C) = X \text{ et } H^1(\mathcal{H}, C) = 0$$

Démonstration. Soit $x \in H^0(\mathcal{H}, C)$, et $(x_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\bar{K}$ convergeant vers x. D'après le Corollaire 4.5, pour tout $n \geq 0$, il existe $y_n \in K_\infty$ tel que $|x_n - y_n| \leq c \max_{\sigma\in\mathcal{H}} |\sigma x_n - x_n| \to 0$. Donc $x = \lim y_n$, et donc $x \in X$. Ainsi, $H^0(\mathcal{H}, C) = X$.
Pour le cas de H^1, on considère les cochaînes continues, C étant muni de la topologie induite par sa valuation.
On va montrer que pour toute cochaîne continue f, il existe une suite (f_ν) de cochaînes continues sur $\mathcal{H}$ à valeurs dans $\bar{K}$, telle que $|f - f_\nu| \to 0$. Soit $\psi_\nu : C \to C/p^\nu\mathcal{O}_C$ la projection canonique. Comme pour tout ν, $C = \bar{K} + p^\nu\mathcal{O}_C$, il existe une application $\varphi_\nu : C/p^\nu\mathcal{O}_C \to \bar{K}$ telle que $\psi_\nu\varphi_\nu = Id_{\bar{K}}$. $C/p^\nu\mathcal{O}_C$ étant discret, les φ_ν sont continues.
Soit $f_\nu = \varphi_\nu\psi_\nu f$. Alors $\psi_\nu f_\nu = f_\nu$, donc $|f_\nu - f| \leq |p|^\nu \to 0$.
D'après le Corollaire 4.5, il existe alors (g_ν) telle que $|f_\nu - dg_\nu| \leq c|df_\nu|$, et $|g_\nu| \leq c|f_\nu|$. Soit f un 1-cocycle sur $\mathcal{H}$ à valeurs dans $\bar{K}$. La suite g_ν converge alors vers une cochaîne continue g car la suite (g_ν) est de Cauchy (la formule donnant g dans la démonstration du Corollaire 4.6 le montre, à condition d'avoir choisi les mêmes y et z pour tous les g_ν). Par passage à la limite,

$$|f - dg| = 0,$$

donc f est un cobord, et donc $H^1(\mathcal{H}, C) = 0$.

Théorème 4.2. *$H^0(\mathcal{G}, C) = K$ et $H^1(\mathcal{G}, C)$ est un K-espace vectoriel de dimension 1.*

Démonstration. On a un isomorphisme

$$H^0(\mathcal{G}, C) \simeq H^0(\mathcal{G}/\mathcal{H}, H^0(\mathcal{H}, C)),$$

c'est à dire

$$H^0(\mathcal{G}, C) \simeq H^0(\mathcal{G}/\mathcal{H}, X) = H^0(\mathcal{C}, X) = K.$$

De même, on a une suite exacte

$$0 \to H^1(\mathcal{G}/\mathcal{H}, H^0(\mathcal{H}, C)) \to H^1(\mathcal{G}, C) \to H^1(\mathcal{H}, C).$$

En effet, on a une flèche $H^1(\mathcal{G}/\mathcal{H}, H^0(\mathcal{H}, C)) \to H^1(\mathcal{G}, C)$ (plus précisément, si $f \in H^1(\mathcal{G}/\mathcal{H}, H^0(\mathcal{H}, C))$, on envoie f sur le cocycle $\sigma \mapsto f(\sigma \mod \mathcal{H})$, en voyant un élément de $H^0(\mathcal{H}, C)$ comme un élément de C. D'autre part, l'application $H^1(\mathcal{G}, C) \to H^1(\mathcal{H}, C)$ est clairement définie (un cocycle sur $\mathcal{G}$ induit un cocycle sur $\mathcal{H}$).
Vérifions l'exactitude de la suite. Tout d'abord, la première flèche est injective.

En effet, soit $f : \mathcal{G}/\mathcal{H} \to H^0(\mathcal{H}, C)$, telle que f soit envoyée sur un cobord, c'est à dire :

$$\exists x \in C \ / \ \forall \sigma \in \mathcal{G}, \ f(\sigma \mod \mathcal{H}) = \sigma x - x.$$

En particulier, pour $\sigma \in \mathcal{H}$, $\sigma x - x = f(1) = 0$, donc $x \in H^0(\mathcal{H}, C)$. σx ne dépend donc pas de la classe de σ modulo $\mathcal{H}$, donc f est un cobord.
Soit $f \in H^1(\mathcal{G}/\mathcal{H}, H^0(\mathcal{H}, C))$, soit $\sigma \in \mathcal{G}$. $f(\sigma)$ est un élément de C vérifiant $sf(\sigma) = f(\sigma)$ pour tout $s \in H$. Si $\sigma \in H$, on a $f(s\sigma) = sf(\sigma) - f(s) = f(\sigma) - f(s) = 0$ car σ et s sont égaux modulo $\mathcal{H}$.
Passons à l'exactitude "au centre". Soit $f : \mathcal{G} \to C$ un 1-cocycle. On suppose qu'il existe $x \in C$ tel que pour tout $h \in \mathcal{H}$, $f(h) = hx - x$. On pose pour $\sigma \in \mathcal{G}$, $g(\sigma) = f(\sigma) - (\sigma x - x)$. g est un 1-cocycle, égal à f dans $H^1(\mathcal{G}, C)$, et $g(h) = 0$ si $h \in \mathcal{H}$.
Ainsi, si $\sigma \in \mathcal{G}$ et $h \in \mathcal{H}$,

$$g(\sigma h) = \sigma g(h) + g(\sigma) = g(\sigma).$$

Donc g passe au quotient et définit une application $\tilde{g} : \mathcal{G}/\mathcal{H} \to C$. Pour $\sigma \in \mathcal{G}$ et $h \in \mathcal{H}$, σ et $h\sigma$ étant égaux modulo $\mathcal{H}$, on a :

$$g(\sigma) = g(h\sigma) = hg(\sigma).$$

g prend donc ses valeurs dans $H^0(\mathcal{H}, C)$. On vérifie finalement que $\tilde{g}$ est un 1-cocycle, et donc définit un élément de $H^1(\mathcal{G}/\mathcal{H}, H^0(\mathcal{H}, C))$, qui s'envoie bien sur $f \in H^1(\mathcal{G}, C)$.
La suite exacte ci-dessus se traduit en :

$$H^1(\mathcal{G}, C) \simeq H^1(\mathcal{G}/\mathcal{H}, X) = H^1(\mathcal{C}, X).$$

Références

[Fou] Fourquaux, L., Logarithme de Perrin-Riou pour des extensions associées à un groupe de Lubin-Tate, Thèse de Doctorat de l'Université Paris VI, 2005

[Ser68] Serre, J.-P., Corps Locaux, Hermann, 1968

[Ser02] Serre, J.-P., Galois Cohomology, Springer-Verlag, 2002

[Tat] Tate, J., p-Divisible Groups, Proc. Conf. Local Fields, 1966