INTRODUCTION AUX ANNEAUX DE FONTAINE, NOTES DU COURS DE M2

par

Pierre Colmez

Table des matières

1. L'extension cyclotomique d'une extension finie de $\mathbf{Q}_p$ et son complété

1.1. L'extension cyclotomique d'une extension non ramifiée de $\mathbf{Q}_p$

Soit F un corps de caractéristique $\neq p$, soit $\overline{F}$ une clôture algébrique de F, et soit $\mathrm{G}_F = \mathrm{Aut}(\overline{F}/F)$. Si $\zeta_{p^n} \in \overline{F}$ est une racine primitive p^n-ième de l'unité, et si $\sigma \in \mathrm{G}_F$, alors $\sigma(\zeta_{p^n})$ est une racine primitive p^n-ième de l'unité. Il existe donc $\chi_n(\sigma) \in (\mathbf{Z}/p^n\mathbf{Z})^*$, uniquement déterminé, tel que $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_n(\sigma)}$. De plus, si $\zeta \in \boldsymbol{\mu}_{p^n}$, il existe $a \in \mathbf{Z}/p^n\mathbf{Z}$ unique, tel que $\zeta = \zeta_{p^n}^a$, et on a

$$\sigma(\zeta) = \sigma(\zeta_{p^n}^a) = \sigma(\zeta_{p^n})^a = \zeta_{p^n}^{a\chi_n(\sigma)} = \zeta^{\chi_n(\sigma)}.$$

Les calculs précédents montre que l'on a $\chi_n(\sigma\tau) = \chi_n(\sigma)\chi_n(\tau)$, si $\sigma, \tau \in \mathrm{G}_F$, et, en prenant $a = p$, que $\chi_{n-1}(\sigma)$ est l'image de $\chi_n(\sigma)$ par l'application naturelle de $(\mathbf{Z}/p^n\mathbf{Z})^*$ dans $(\mathbf{Z}/p^{n-1}\mathbf{Z})^*$. Il existe donc un caractère $\chi : \mathrm{G}_F \to \mathbf{Z}_p^*$, uniquement déterminé par la condition $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ quel que soit $\zeta \in \boldsymbol{\mu}_{p^\infty}$, groupe des racines de l'unité d'ordre une puissance de p. Ce caractère est le *caractère cyclotomique*.

Soit F une extension non ramifiée de $\mathbf{Q}_p$. Choisissons pour chaque n une racine p^n-ième primitive de l'unité $\varepsilon^{(n)}$, de telle sorte que $(\varepsilon^{(n+1)})^p = \varepsilon^{(n)}$. Si $n \geqslant 1$, soit $F_n = F(\varepsilon^{(n)})$, et soit $F_\infty = \cup_n F_n$.

Proposition 1.1. — (i) *Si $n \geqslant 1$, F_n est une extension totalement ramifiée de degré $(p-1)p^{n-1}$ de F, et $\pi_n = \varepsilon^{(n)} - 1$ en est une uniformisante.*

(ii) *Si $n \geqslant 1$, F_n est une extension galoisienne de F, et χ induit un isomorphisme de* $\mathrm{Gal}(F_n/F)$ *sur $(\mathbf{Z}/p^n\mathbf{Z})^*$.*

(iii) *F_∞ est une extension galoisienne de F, et χ induit un isomorphisme de* $\Gamma_F = \mathrm{Gal}(F_\infty/F)$ *sur $\mathbf{Z}_p^*$.*

Démonstration. — Soit P_n le polynôme cyclotomique d'indice p^n donné par la formule $P_n(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$. Le polynôme $Q_n(X) = P_n(X+1)$ est un polynôme d'Eisenstein (son terme constant est p et sa réduction modulo p est $X^{p^n - p^{n-1}}$) donc est irréductible sur F. On en déduit le (i).

Le corps F_n est le corps de décomposition du polynôme $X^{p^n} - 1$; il est donc galoisien sur F. De plus, $\mathrm{Gal}(F_n/F)$ et $(\mathbf{Z}/p^n\mathbf{Z})^*$ ont même cardinal, et χ_n est injectif de manière évidente ; on en déduit le (ii), et le (iii) en passant à la limite projective.

Si $n \geqslant 1$, notons $G(n)$ le groupe $(\mathbf{Z}/p^n\mathbf{Z})^*$, et soit $G(\infty) = \mathbf{Z}_p^*$. Si $k \in \mathbf{N}$, soit $G(\infty)^k$ le sous-groupe de $G(\infty)$ défini par $G(\infty)^0 = G(\infty)$, et $G(\infty)^k = 1 + p^k\mathbf{Z}_p$, si $k \geqslant 1$. Si $n \geqslant 1$, on définit le sous-groupe $G(n)^k$ de $G(n)$ comme l'image de $G(\infty)^k$. On a donc, en particulier, $G(n)^k = \{1\}$, si $k \geqslant n$. On identifie $G(n)$ et $\mathrm{Gal}(F_n/F)$, ainsi que $G(\infty)$ et Γ_F, via le caractère cyclotomique χ.

Proposition 1.2. — (i) *Si $n \geqslant 1$, alors* $\mathrm{Gal}(F_n/F)_u = G(n)^0$ *si $u \leqslant 0$, et* $\mathrm{Gal}(F_n/F)_u = G(n)^k$, *si $p^{k-1} - 1 < u \leqslant p^k - 1$, et si $k \geqslant 1$.*

(ii) *Si $n \geqslant 1$, alors* $\mathrm{Gal}(F_n/F)^v = G(n)^0$ *si $v \leqslant 0$, et* $\mathrm{Gal}(F_n/F)^v = G(n)^k$, *si $k-1 < v \leqslant k$ et si $k \geqslant 1$.*

(iii) *Si $n \geqslant 1$, alors $c(F_n/F) = n$.*

(iv) *$\Gamma_F^v = G(\infty)^0$ si $v \leqslant 0$, et $\Gamma_F^v = G(\infty)^k$, si $k-1 < v \leqslant k$ et si $k \geqslant 1$.*

Démonstration. — L'extension F_n/F est totalement ramifiée et $\pi_n = \varepsilon^{(n)} - 1$ en est une uniformisante (et donc un générateur de $\mathscr{O}_{F_n}$ comme algèbre sur $\mathbf{Z}_p$). Par définition, si $\sigma \in \mathrm{Gal}(F_n/F)$, on a donc $i_{F_n}(\sigma) = v_{F_n}(\sigma(\pi_n) - \pi_n) = v_{F_n}(\sigma(1+\pi_n) - (1+\pi_n))$. Supposons $\sigma \neq 1$. On peut alors écrire $\chi(\sigma)$ sous la forme $1 + p^k a$, avec $a \in \mathbf{Z}_p^*$, et $0 \leqslant k \leqslant n-1$. Comme $(1+\pi_n)$ est une racine de l'unité d'ordre une puissance de p, on a $\sigma(1+\pi_n) - (1+\pi_n) = (1+\pi_n)((1+\pi_n)^{ap^k} - 1)$, et comme $(1+\pi_n)^{ap^k}$ est une racine primitive p^{n-k}-ième de l'unité, on obtient

$$v_{F_n}(\sigma(1+\pi_n) - (1+\pi_n)) = \frac{v_p((1+\pi_n)^{ap^k} - 1)}{v_p(\pi_n)} = \frac{1/(p-1)p^{n-k-1}}{1/(p-1)p^{n-1}} = p^k.$$

On en déduit que $\sigma \in \mathrm{Gal}(F_n/F)_u$ si et seulement si $p^k \geqslant u+1$, ce qui démontre le (i).

On a $[G(n)_0 : G(n)_u] = (p-1)p^{k-1}$ si $p^{k-1}-1 < u \leqslant p^k - 1$ et $1 \leqslant k \leqslant n$. On en déduit que, sur $[0, +\infty[$, la fonction $\varphi_{F_n/F}$ est affine sur chacun des segments $[p^{k-1}-1, p^k-1]$, et sur $[p^n-1, +\infty[$. comme la dérivée de $\varphi_{F_n/F}$ sur $[p^{k-1}-1, p^k-1]$ est $\frac{1}{(p-1)p^{k-1}}$, on a $\varphi_{F_n/F}(k) = \varphi_{F_n/F}(k-1) + 1$, si $1 \leqslant k \leqslant n$. La fonction $\psi_{F_n/F}$ est donc affine de dérivée $(p-1)p^k$ sur chacun des segments $[k, k+1]$, si $k \leqslant n-1$, et affine de dérivée $(p-1)p^{n-1}$ sur $[n, +\infty[$. En particulier, les sauts de la filtration par les $\mathrm{Gal}(F_n/F)^v$ sont aux entiers $\leqslant n$. On en déduit le (ii). Les (iii) et (iv), quant à eux, sont des conséquences immédiates du (ii).

Remarque 1.3. — Le conducteur de F_n sur F est un entier, comme prédit par le théorème de Hasse-Arf

Exercice 1. — (i) Montrer que le polynôme minimal de π_1 sur F est $\frac{(1+X)^p-1}{X}$. En déduire que $v_p(\mathfrak{d}_{F_1/F}) = 1 - \frac{1}{p-1}$.

(ii) Montrer que, si $n \geqslant 2$, le polynôme minimal de π_n sur F_{n-1} est $(1+X)^p - (1+\pi_{n-1})$. En déduire que $v_p(\mathfrak{d}_{F_n/F_{n-1}}) = 1$.

(iii) Montrer que $v_p(\mathfrak{d}_{F_n/F}) = n - \frac{1}{p-1}$.

(iv) En déduire que l'on a $F_n^{(v)} = F_k$ si $k \leqslant v < k+1$, et $0 \leqslant k \leqslant n$.

(v) Retrouver le (ii) de la prop. 1.2.

1.2. Le complété de l'extension cyclotomique de F. — Soit $\widehat{F}_\infty$ le complété de F_∞ pour v_p ; c'est aussi l'adhérence de F_∞ dans $\mathbf{C}_p$. L'action de Γ_F sur F_∞ s'étend par continuité à $\widehat{F}_\infty$, et l'objet de ce n$^{\mathrm{o}}$ est d'étudier cette action.

Remarque 1.4. — Si $k \geqslant v_p(2p)$, et si $v_p(u-1) = k$, l'application $x \mapsto \frac{\log x}{\log u}$ induit un isomorphisme de groupes de $1 + p^k\mathbf{Z}_p$ sur $\mathbf{Z}_p$, l'isomorphisme inverse étant $y \mapsto u^y = \exp(y \log u)$. Cela montre que le groupe (multiplicatif) $1 + p^k\mathbf{Z}_p$ est *procyclique* (i.e. est topologiquement engendré par un élément). Si $p \geqslant 3$, on a $\mathbf{Z}_p^* = \boldsymbol{\mu}_{p-1} \times (1 + p\mathbf{Z}_p)$, et comme $\boldsymbol{\mu}_{p-1}$ est cyclique d'ordre premier à p, le groupe $\mathbf{Z}_p^*$ est lui aussi procyclique. Par contre, $\mathbf{Z}_2^* = \{\pm 1\} \times (1 + 4\mathbf{Z}_2)$ n'est pas procyclique.

Lemme 1.5. — *Si $n \geqslant 1$ et $x \in F_\infty$, alors $p^{-k}\mathrm{Tr}_{F_{n+k}/F_n}(x)$ de dépend pas de l'entier k tel que $x \in F_{n+k}$.*

Démonstration. — Cela suit de ce que $\mathrm{Tr}_{F_{n+k+i}/F_n}(x) = [F_{n+k+i} : F_{n+k}]\mathrm{Tr}_{F_{n+k}/F_n}(x)$ si $x \in F_{n+k}$ et de ce que $[F_{N+k+i} : F_{n+k}] = p^i$.

Notons $\mathrm{R}_n : F_\infty \to F_n$ l'application dont le lemme ci-dessus assure l'existence. Si $n \geqslant 1$, soit $Y_n = \{x \in F_n,\ \mathrm{Tr}_{F_n/F_{n-1}}(x) = 0\}$, et soit $\mathrm{R}_n^* = \mathrm{R}_n - \mathrm{R}_{n-1}$.

Proposition 1.6. — (i) *L'application $\mathrm{R}_n : F_\infty \to F_n$ est F_n-linéaire, commute avec l'action de Γ_F, et on a $\mathrm{R}_n \circ \mathrm{R}_{n+k} = \mathrm{R}_n$.*

(ii) *Si $x \in F_\infty$, alors $\mathrm{R}_{n+i}^*(x) \in Y_{n+i}$, est nul si $i \gg 0$, et on a*

$$x = \mathrm{R}_n(x) + \sum_{i=1}^{+\infty} \mathrm{R}_{n+i}^*(x).$$

(iii) *Si $k \in \mathbf{Z}$, alors « $v_p(x) \geqslant kv_p(\pi_n)$ » $\Leftrightarrow$ « $v_p(\mathrm{R}_n(x)) \geqslant kv_p(\pi_n)$ et $v_p(\mathrm{R}_{n+i}^*(x)) \geqslant kv_p(\pi_n)$, quel que soit $i \geqslant 1$ ».*

Démonstration. — R_n commute à l'action de Γ_F car, si L/K est une extension de corps, et si $\sigma : L \to L^\sigma$ est un isomorphisme de corps, alors $\mathrm{Tr}_{L^\sigma/K^\sigma}(\sigma(x)) = \sigma(\mathrm{Tr}_{L/K}(x))$. Le reste du (i) est immédiat.

Le (ii) suit de ce qu'il existe $k \in \mathbf{N}$ tel que $x \in F_{n+k}$ et alors $\mathrm{R}_{n+i}(x) = x$ si $i \geqslant k$.

Dans le (iii), l'implication $\Leftarrow$ est immédiate. Pour démontrer l'implication réciproque, constatons que les π_{n+k}^i, pour $0 \leqslant i \leqslant p^k - 1$ forment une base de $\mathscr{O}_{F_{n+k}}$ sur $\mathscr{O}_{F_n}$ puisque l'extension F_{n+k}/F_n est totalement ramifiée. On peut donc écrire $x \in \mathscr{O}_{F_{n+k}}$ de manière unique sous la forme

$$x = \sum_{j=0}^{p^k-1} a_j (1 + \pi_{n+k})^j, \quad \text{avec } a_j \in \mathscr{O}_{F_n}.$$

Maintenant, on a $(1 + \pi_{n+k})^{p^{k-i}} = 1 + \pi_{n+i}$ si $i \leqslant k$, et

$$p^{-1}\mathrm{Tr}_{F_{n+i}/F_{n+i-1}}((1 + \pi_{n+i})^j) = \begin{cases} (1 + \pi_{n+i})^j & \text{si } p \mid j, \\ 0 & \text{si } (p, j) = 1. \end{cases}$$

En écrivant $j \in \{0, \dots, p^k - 1\}$ sous la forme $j = p^{k-i} j'$, avec $(j', p) = 1$, on en déduit les formules

$$\mathrm{R}_n(x) = a_0 \quad \text{et} \quad \mathrm{R}^*_{n+i}(x) = \sum_{(j',p)=1} a_{p^{k-i}j'} (1 + \pi_{n+i})^{j'}.$$

Ceci permet de montrer que, si $v_p(x) \geqslant 0$, alors $v_p(\mathrm{R}_n(x)) \geqslant 0$ et $v_p(\mathrm{R}^*_{n+i}(x)) \geqslant 0$. Le cas général s'en déduit en remarquant que « $v_p(x) \geqslant k v_p(\pi_n)$ » équivaut à « $x \in \pi_n^k \mathscr{O}_{F_n}$ », et en utilisant la F_n-linéarité de R_{n+i}, si $i \in \mathbf{N}$.

Si $k \in \mathbf{N}$, on note $\Gamma_{F_k} = \mathrm{Gal}(F_\infty/F_k)$; c'est le sous-groupe de Γ_F image inverse de $1 + p^k \mathbf{Z}_p$ par χ. En particulier, Γ_{F_k} est un groupe procyclique si $k \geqslant v_p(2p)$.

Lemme 1.7. — *Soit $j \geqslant v_p(2p)$, soit γ_j un générateur de Γ_{F_j}, et soit $i \geqslant j + 1$. Alors $\gamma_j - 1$ est inversible sur Y_i. De plus, si $k \in \mathbf{N}$, et $v_p(x) \geqslant k v_p(\pi_{i-1})$, alors $v_p((\gamma_j - 1)^{-1} x) \geqslant k v_p(\pi_{i-1}) - \frac{1}{p-1}$.*

Démonstration. — Commençons par traiter le cas $j = i - 1$. Si $x \in Y_i$, on peut écrire x sous la forme $x = \sum_{a=1}^{p-1} x_a (1 + \pi_i)^a$, avec $x_a \in F_{i-1}$. De plus, si $k \in \mathbf{N}$, et $v_p(x) \geqslant k v_p(\pi_{i-1})$, alors $v_p(x_a) \geqslant k v_p(\pi_{i-1})$, quel que soit $a \in \{1, \dots, p-1\}$. Par ailleurs, on peut écrire $\chi(\gamma_j) = 1 + p^j v$, avec $v \in \mathbf{Z}_p^*$. On a alors $\gamma_j((1 + \pi_i)^a) = (1 + \pi_i)^a (1 + \pi_1)^{av}$, et comme x_a et π_1 sont fixes par γ_j, on voit que x a comme antécédent

$$(\gamma_j - 1)^{-1} x = \sum_{a=1}^{p-1} \frac{x_a}{(1 + \pi_1)^{av} - 1} (1 + \pi_i)^a.$$

De plus, comme $v_p((1 + \pi_1)^{av} - 1) = \frac{1}{p-1}$, on obtient la minoration voulue dans le cas $j = i - 1$. Le cas général s'en déduit en remarquant, que $\gamma' = \gamma_j^{p^{i-j-1}}$ est un générateur de $\Gamma_{F_{i-1}}$, et que l'on a $(\gamma_j - 1)^{-1} = (\gamma' - 1)^{-1}(1 + \gamma_j + \cdots + \gamma_j^{p^{i-j-1}-1})$.

Proposition 1.8. — *Soit $n \geqslant v_p(2p)$, et soit γ_n un générateur de Γ_{F_n}.*

(i) *Tout élément x de F_∞ peut être écrit de manière unique sous la forme $x = \mathrm{R}_n(x) + (\gamma_n - 1) y$, avec $\mathrm{R}_n(y) = 0$, et on a*

$$v_p(\mathrm{R}_n(x)) > v_p(x) - v_p(\pi_n), \quad v_p(y) > v_p(x) - v_p(\pi_n) - \frac{1}{p-1}.$$

(ii) R_n *s'étend par continuité à* $\widehat{F}_\infty$ *et, si* $X_n = \{x \in \widehat{F}_\infty,\ \mathrm{R}_n(x) = 0\}$*, on peut écrire tout élément* x *de* $\widehat{F}_\infty$ *de manière unique sous la forme* $x = \mathrm{R}_n(x) + (\gamma_n - 1)y$*, avec* $y \in X_n$*, et on a*

$$v_p(\mathrm{R}_n(x)) > v_p(x) - v_p(\pi_n), \quad v_p(y) > v_p(x) - v_p(\pi_n) - \frac{1}{p-1}.$$

Démonstration. — D'après le lemme précédent et la prop. 1.6, on a

$$x = \mathrm{R}_n(x) + (\gamma_n - 1)y, \quad \text{avec } y = \sum_{i=1}^{+\infty} (\gamma_n - 1)^{-1}\mathrm{R}^*_{n+i}(x).$$

On en déduit le (i).

Par ailleurs, d'après le (i), on a $v_p(\mathrm{R}_n(x)) > v_p(x) - v_p(\pi_n)$, ce qui prouve que l'application F_n-linéaire R_n est uniformément continue, et donc s'étend par continuité à $\widehat{F}_\infty$. Le reste du (ii) se déduit du (i) par passage à la limite.

Remarque 1.9. — (i) Les applications $\mathrm{R}_n : \widehat{F}_\infty \to F_n$ sont connues sous le nom de *Traces de Tate normalisées.*

(ii) D'après la prop. 1.6, elles commutent à l'action de Γ_F (ou G_F).

(iii) On a $\mathrm{R}_n(x) = x$ si $x \in F_\infty$ et $n \gg 0$. Donc $\lim_{n\to+\infty} \mathrm{R}_n(x) = x$ si $x \in \widehat{F}_\infty$.

Exercice 2. — Si G est un groupe topologique, et M est un groupe topologique muni d'une action continue de G, un *cocycle* continu sur G à valeurs dans M, est une application continue $g \mapsto c_g$ de G dans M telle que l'on ait $c_{gh} = g(c_h) + c_g$ quels que soient $h, g \in G$. Le but de cet exercice est d'étudier les cocycles continus sur Γ_F à valeurs dans $\widehat{F}_\infty$. On suppose pour simplifier que p est impair, et donc que $\mathbf{Z}_p^*$ et Γ_F sont procycliques.

(i) Montrer que, si $c \in \widehat{F}_\infty$, alors $\tau \mapsto (\tau - 1)c$ est un cocycle continu sur Γ_F à valeurs dans $\widehat{F}_\infty$.

(ii) Soit γ un générateur topologique de Γ_F. Montrer que tout élément x de F_1 peut s'écrire de manière unique sous la forme $x_0 + (\gamma - 1)y_0$, avec $x_0 \in F$ et $y_0 \in F_1$ vérifiant $\mathrm{Tr}_{F_1/F}(y_0) = 0$. En déduire que tout élément de $\widehat{F}_\infty$ peut s'écrire sous la forme $x_0 + (\gamma - 1)y$, avec $x_0 \in F$.

(iii) Soit $\tau \mapsto c_\tau$ un cocycle continu sur Γ_F, à valeurs dans $\widehat{F}_\infty$. Montrer, en décomposant c_γ sous la forme $x_0 + (\gamma - 1)y$, qu'il existe $a \in F$ uniquement déterminé, et $c \in \widehat{F}_\infty$, tels que l'on ait $c_\tau = a \log \chi(\tau) + (\tau - 1)c$ quel que soit $\tau \in \Gamma_F$.

1.3. Il n'y a pas de $2i\pi$ dans $\mathbf{C}_p$!

Un analogue p-adique de $2i\pi$ devrait être défini par la formule $2i\pi = \lim_{n\to+\infty} p^n \log \varepsilon^{(n)}$. Le problème est que l'on a $\log_p \varepsilon^{(n)} = 0$ quel que soit $n \in \mathbf{N}$ et donc la formule précédente donne $2i\pi = 0$, ce qui n'est pas très raisonnable. Si on regarde ce que donne la formule précédente d'un point de vue galoisien et que l'on utilise la formule $\sigma(\varepsilon^{(n)}) = (\varepsilon^{(n)})^{\chi(\sigma)}$, si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on voit que le minimum que l'on puisse demander à un analogue p-adique de $2i\pi$ est de vérifier la formule $\sigma(2i\pi) = \chi(\sigma)2i\pi$ quel que soit $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$. Malheureusement (ou heureusement...), on a le résultat suivant.

Théorème 1.10. — (i) *Il n'y a pas d'élément* x *de* $\mathbf{C}_p$ *tel que l'on ait* $\sigma(x) = x + \log \chi(\sigma)$*, quel que soit* $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$ (autrement dit, $\mathbf{C}_p$ ne contient pas d'analogue p-adique de $\log 2i\pi$).

(ii) *Si* $k \in \mathbf{Z} - \{0\}$*, alors* $\{x \in \mathbf{C}_p,\ \sigma(x) = \chi(\sigma)^k x,\ \text{quel que soit } \sigma \in \mathrm{G}_{\mathbf{Q}_p}\} = \{0\}$. (autrement dit, $\mathbf{C}_p$ ne contient pas d'analogue p-adique de $(2i\pi)^k$, quel que soit $k \in \mathbf{Z} - \{0\}$.)

Démonstration. — (i) S'il existe un tel x, alors $\sigma(x) = x$ quel que soit $\sigma \in \ker \chi$, et donc $x \in \widehat{F}_\infty$, d'après le théorème d'Ax-Sen-Tate. On a alors

$$\sigma(\mathrm{R}_n(x)) = \mathrm{R}_n(\sigma(x)) = \mathrm{R}_n(x) + \log \chi(\sigma),$$

quel que soit $\sigma \in \Gamma_{\mathbf{Q}_p}$, ce qui est impossible car $\mathrm{R}_n(x) \in F_n$ n'a qu'un nombre fini de conjugués, et $\log \chi(\sigma)$ prend un nombre infini de valeurs.

(ii) Si $x \in \mathbf{C}_p^*$ vérifie $\sigma(x) = \chi(\sigma)^k x$ quel que soit $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, et si $\mathscr{L} \in \mathbf{Q}_p$, alors $y = \frac{1}{k} \log_{\mathscr{L}}(x)$ vérifie $\sigma(y) = y + \log \chi(\sigma)$, quel que soit $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, et le (i) montre que ceci n'est pas possible.

Exercice 3. — Démontrer la non existence de $2i\pi$ sans passer par celle de $\log 2i\pi$.

Exercice 4. — Soit K une extension finie de $\mathbf{Q}_p$ (pas forcément non ramifiée).

(i) Montrer qu'il n'y a pas d'élément x de $\mathbf{C}_p$ tel que l'on ait $\sigma(x) = x + \log \chi(\sigma)$, quel que soit $\sigma \in \mathrm{G}_K$.

(ii) Montrer que, si $k \in \mathbf{Z} - \{0\}$, alors $\{x \in \mathbf{C}_p,\ \sigma(x) = \chi(\sigma)^k x,\ \text{quel que soit } \sigma \in \mathrm{G}_K\} = \{0\}$.

1.4. L'extension cyclotomique d'une extension finie de $\mathbf{Q}_p$

Soit K une extension finie de $\mathbf{Q}_p$ et soit F l'extension maximale non ramifiée de $\mathbf{Q}_p$ contenue dans K. Si $n \in \mathbf{N}$, soit $K_n = KF_n = K(\boldsymbol{\mu}_{p^n})$. Soit $K_\infty = KF_\infty = \cup_{n\in\mathbf{N}} K_n$. Étant la composée d'une extension galoisienne avec K, l'extension K_∞/K est galoisienne et son groupe de Galois Γ_K s'identifie naturellement à un sous-groupe (ouvert car $[K : F] < +\infty$) de $\mathrm{Gal}(F_\infty/\mathbf{Q}_p)$. Finalement, soit $\mathrm{G}_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$, et soit $\mathrm{H}_K \subset \mathrm{G}_K$ le noyau de χ. On a donc $\mathrm{H}_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$ et $\Gamma_K = \mathrm{G}_K/\mathrm{H}_K$.

Si L est une extension finie de F, on note $c(L) = c(L/F)$ le conducteur absolu de L. Soit $n_0(K)$ le plus petit entier $\geqslant c(K)$.

Lemme 1.11. — *Si $n \geqslant n_0(K)$, alors*

(i) $c(K_n) = n$ *;*

(ii) K_{n+1}/K_n *est une extension totalement ramifiée de degré p ;*

(iii) $\mathrm{Gal}(K_{n+k}/K_n) \cong \mathrm{Gal}(F_{n+k}/F_n)$ *et* $\Gamma_{K_n} \cong \Gamma_{F_n}$ *;*

(iv) $K_{n+1}^{(s)} = K_n^{(s)}$ *quel que soit $s < n_0(K)$.*

Démonstration. — On a $c(K_n) = \sup(c(K), c(F_n)) = \sup(c(K), n)$; on en déduit le (i), le (ii) et le (iii). Par ailleurs, $K_n^{(s)} = K_{n+1}^{(s)} \cap K_n$, et donc $K_{n+1}^{(s)}/K_n^{(s)}$ est de degré p si $K_{n+1}^{(s)} \neq K_n^{(s)}$. Ceci implique que l'on a $K_{n+1} = K_{n+1}^{(s)} K_n$, ce qui conduit à une contradiction car $c(K_{n+1}) = n + 1$ et $c(K_{n+1}^{(s)} K_n) = \sup(c(K_{n+1}^{(s)}), c(K_n)) \leqslant \sup(s, n) \leqslant n$ si $s < n_0(K) \leqslant n$. Ceci termine la démonstration.

Corollaire 1.12. — *Si $n \geqslant n_0(K)$, alors*

(i) $f(K_{n+1}/F_{n+1}) = f(K_n/F_n)$, $e(K_{n+1}/F_{n+1}) = e(K_n/F_n)$ *et* $[K_{n+1} : F_{n+1}] = [K_n : F_n]$ *;*

(ii) *les applications naturelles* $\mathrm{Hom}_{\widehat{F}_\infty}(\widehat{K}_\infty, \mathbf{C}_p) \to \mathrm{Hom}_{F_\infty}(K_\infty, \overline{\mathbf{Q}}_p) \to \mathrm{Hom}_{F_n}(K_n, \overline{\mathbf{Q}}_p)$ *sont des bijections ; la restriction de* $\mathrm{Tr}_{\widehat{K}_\infty/\widehat{F}_\infty}$ *à K_∞ (resp. à K_n) est* $\mathrm{Tr}_{K_\infty/F_\infty}$ *(resp. à* Tr_{K_n/F_n}*) ; si, de plus, K/F est une extension galoisienne, alors K_∞/F_∞ et K_n/F_n sont aussi galoisiennes, et* $\mathrm{Gal}(K_n/F_n) = \mathrm{Gal}(K_\infty/F_\infty) = \mathrm{H}_F/\mathrm{H}_K$.

Démonstration. — Tous ces points sont des conséquences immédiates du (ii) du lemme précédent.

On note d_{K_∞} le degré de l'extension K_∞/F_∞. On note e_{K_∞} (resp. f_{K_∞}) la limite de la suite de terme général $e(K_n/F_n)$ (resp. $f(K_n/F_n)$).

Remarque 1.13. — (i) d_{K_∞} est aussi le degré de l'extension K_n/F_n si $n \geqslant n_0(K)$.

(ii) Comme l'extension F_∞/F est totalement ramifiée, f_{K_∞} est aussi le degré de l'extension F'/F, où F' est l'extension non ramifiée maximale de F contenue dans K_∞.

(iii) On a $F' \subset K_n$ si $n \geqslant n_0(K)$.

(iv) $e_{K_\infty} f_{K_\infty} = d_{K_\infty}$.

Proposition 1.14. — *La suite de terme général* $p^n v_p(\mathfrak{d}_{K_n/F_n})$ *est stationnaire pour* $n \geqslant n_0(K)$ *et on a* $p^n v_p(\mathfrak{d}_{K_n/F_n}) \leqslant \frac{1}{p-1} p^{n_0(K)}$ *quel que soit* $n \in \mathbf{N}$.

Démonstration. — On part des formules

$$v_p(\mathfrak{d}_{K_n/F_n}) = v_p(\mathfrak{d}_{K_n/F}) - v_p(\mathfrak{d}_{F_n/F}) = \int_0^{+\infty} \Big(\frac{1}{[F_n : F_n^{(s)}]} - \frac{1}{[K_n : K_n^{(s)}]}\Big)\, ds$$

et $p^n = \frac{p}{p-1}[F_n : F]$. Par ailleurs, on a $F_n^{(s)} = K_n^{(s)} \cap F_n$ et donc $[F_n : F_n^{(s)}] = [F_n K_n^{(s)} : K_n^{(s)}]$, ce qui nous donne

$$p^n v_p(\mathfrak{d}_{K_n/F_n}) = \frac{p}{p-1} \int_0^{+\infty} [F_n^{(s)} : F]\Big(1 - \frac{1}{[K_n : F_n K_n^{(s)}]}\Big)\, ds.$$

Maintenant, si $s \geqslant n_0(K) \geqslant c(K)$, on a $K_n^{(s)} \supset K^{(s)} = K$ et donc $[K_n : F_n K_n^{(s)}] = 1$, ce qui nous fournit la formule

$$p^n v_p(\mathfrak{d}_{K_n/F_n}) = \frac{p}{p-1} \int_0^{n_0(K)} [F_n^{(s)} : F]\Big(1 - \frac{1}{[K_n : F_n K_n^{(s)}]}\Big)\, ds.$$

Pour obtenir la majoration de la proposition, il suffit alors de majorer $1 - \frac{1}{[K_n : F_n K_n^{(s)}]}$ par 1 et d'utiliser la formule

$$\int_0^{n_0(K)} [F_n^{(s)} : F]\, ds = 1 + (p-1) + \cdots + (p-1)p^{n_0(K)-2} = p^{n_0(K)-1}.$$

Il reste à montrer que la suite $p^n v_p(\mathfrak{d}_{K_n/F_n})$ est stationnaire pour $n \geqslant n_0(K)$. Soient donc $n \geqslant n_0(K)$ et $s < n_0(K)$. On a $F_n^{(s)} = F_{n+1}^{(s)} = F_k$, où k est le plus grand entier $\leqslant s \leqslant n_0(K)$, et donc $[F_{n+1}^{(s)} : F] = [F_n^{(s)} : F]$ quel que soit $s \in [0, n_0(K)]$. Par ailleurs, l'extension K_{n+1}/K_n est de degré p et, comme $K_{n+1}^{(s)} = K_n^{(s)}$ est de conducteur $\leqslant s \leqslant n$, l'extension $F_{n+1}K_{n+1}^{(s)}/F_n K_n^{(s)}$ est non triviale et donc de degré p, elle aussi. On a donc $[K_{n+1} : F_{n+1}K_{n+1}^{(s)}] = [K_n : F_n K_n^{(s)}]$, ce qui permet de conclure.

Remarque 1.15. — Une conséquence de la proposition 1.14 est que $v_p(\mathfrak{d}_{K_n/F_n})$ tend vers 0 quand n tend vers $+\infty$: l'extension K_∞/F_∞ est *presque étale*.

Exercice 5. — (i) Montrer que, quel que soit $\delta > 0$ et quel que soit K extension finie de F, il existe $\alpha \in K_\infty$ tel que $v_p(\alpha) \geqslant -\delta$ et $\mathrm{Tr}_{K_\infty/F_\infty}(\alpha) = 1$.

(ii) Soit $\tau \mapsto c_\tau$ un cocycle continu (cf. exercice 2) sur H_F, à valeurs dans $\mathscr{O}_{\mathbf{C}_p}$.

(a) Montrer qu'il existe une extension galoisienne finie K de F telle que l'on ait $c_\tau \in p^2\mathscr{O}_{\mathbf{C}_p}$ si $\tau \in \mathrm{H}_K$.

(b) Soit $\alpha \in K_\infty$ vérifiant $v_p(\alpha) > -1$ et $\mathrm{Tr}_{K_\infty/F_\infty}(\alpha) = 1$, soit T un système de représentants de $\mathrm{H}_F/\mathrm{H}_K$ dans H_F, et soit $c = \sum_{\tau\in T}\tau(\alpha)c_\tau$. Montrer que $c \in p^{-1}\mathscr{O}_{\mathbf{C}_p}$, et que

$$\sigma(c) - c = \Big(\sum_{\tau\in T}\sigma\tau(\alpha)c_{\sigma\tau}\Big) - \Big(\sum_{\tau\in T}\tau(\alpha)c_\tau\Big) - c_\sigma, \quad \text{si } \sigma \in \mathrm{H}_F.$$

(c) Montrer que si $\tau \in T$, il existe $\tau' \in T$ unique tel que $h_\tau = (\tau')^{-1}\sigma\tau \in \mathrm{H}_K$, et que $\tau \mapsto \tau'$ est une bijection de T dans T. En déduire que $c'_\sigma = p^{-1}(c_\sigma - (\sigma-1)c) \in \mathscr{O}_{\mathbf{C}_p}$, quel que soit $\sigma \in \mathrm{H}_F$.

(d) Montrer que $\sigma \mapsto c'_\sigma$ est un cocycle continu sur H_F à valeurs dans $\mathscr{O}_{\mathbf{C}_p}$. En déduire qu'il existe $c \in \mathbf{C}_p$ tel que l'on ait $c_\sigma = (\sigma-1)c$ quel que soit $\sigma \in \mathrm{H}_F$.

(iii) Soit $\sigma \mapsto c_\sigma$ un cocycle continu sur G_F à valeurs dans $\mathbf{C}_p$.

(a) Montrer qu'il existe $c \in \mathbf{C}_p$ tel que le cocycle $\sigma \mapsto c'_\sigma = c_\sigma - (\sigma-1)c$ soit identiquement nul sur H_F.

(b) Montrer qu'il existe un cocycle continu $\sigma \mapsto d_\sigma$ sur Γ_F à valeurs dans $\widehat{F}_\infty$ tel que l'on ait $c'_\sigma = d_{\overline{\sigma}}$, où $\overline{\sigma}$ désigne l'image de σ dans Γ_F.

(c) En utilisant l'exercice 2, montrer qu'il existe $a \in F$, uniquement déterminé, et $c \in \mathbf{C}_p$, tel que l'on ait $c_\sigma = a\log\chi(\sigma) + (\sigma-1)c$ quel que soit $\sigma \in \mathrm{G}_F$.

Lemme 1.16. — *Si $n \geqslant n_0(K)$, et si $x \in K_\infty$, alors $p^{-k}\mathrm{Tr}_{K_{n+k}/K_n}(x)$ ne dépend pas de l'entier k tel que $x \in K_{n+k}$.*

Démonstration. — Exercice.

Notons $\mathrm{R}_{K,n} : K_\infty \to K_n$, si $n \geqslant n_0(K)$, l'application dont le lemme ci-dessus assure l'existence.

Proposition 1.17. — (i) *L'application $\mathrm{R}_{K,n}$ s'étend par continuité en une application K_n-linéaire de $\widehat{K}_\infty$ dans K_n vérifiant les propriétés suivantes.*

(a) *Si $K \subset L$, et si $n \geqslant n_0(L)$, alors $\mathrm{R}_{K,n}$ et $\mathrm{R}_{L,n}$ coïncident sur $\widehat{K}_\infty$.*

(b) *Si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, alors $\sigma \circ \mathrm{R}_{K,n} = \mathrm{R}_{K^\sigma,n} \circ \sigma$.*

(c) $v_p(\mathrm{R}_{K,n}(x)) \geqslant v_p(x) - v_p(\pi_n) - v_p(\mathfrak{d}_{K_n/F_n})$.

(d) $\lim_{n\to+\infty}\mathrm{R}_{K,n}(x) = x$.

(ii) *Soit $X_{K,n} = \{x \in \widehat{K}_\infty,\ \mathrm{R}_{K,n}(x) = 0\}$. Alors tout élément de $\widehat{K}_\infty$ peut s'écrire de manière unique sous la forme $x = \mathrm{R}_{K,n}(x) + (\gamma_n - 1)y$, avec $y \in X_{K,n}$, et on a*

$$v_p(y) \geqslant v_p(x) - \frac{1}{p-1} - v_p(\pi_n) - v_p(\mathfrak{d}_{K_n/F_n}).$$

Démonstration. — Soit $e_1, \dots, e_d$ une base de $\mathscr{O}_{K_n}$ sur $\mathscr{O}_{F_n}$, et soit $e_1^*, \dots, e_d^*$ la base de K_n sur F_n, duale de $e_1, \dots, e_d$ pour $(x,y) \mapsto \mathrm{Tr}_{K_n/F_n}(xy)$. On peut alors écrire tout élément x de $\widehat{K}_\infty$ sous la forme $x = \sum_{i=1}^d x_ie_i^*$, avec $x_i = \mathrm{Tr}_{\widehat{K}_\infty/\widehat{F}_\infty}(xe_i) \in \widehat{F}_\infty$ et $v_p(x_i) \geqslant v_p(x)$. Comme $\mathrm{R}_{K,n}$ est K_n-linéaire sur K_∞, est l'identité sur K_n, et coïncide avec R_n sur F_∞, on a

$$\mathrm{R}_{K,n}(x) = \mathrm{R}_{K,n}(\sum_{i=1}^d x_ie_i^*) = \sum_{i=1}^d \mathrm{R}_n(x_i)e_i^*.$$

Ceci permet de déduire les propriétés de $\mathrm{R}_{K,n}$ de celle de R_n, et la proposition suit de la proposition 1.8, de la remarque 1.9 et de la minoration $v_p(e_i^*) \geqslant -v_p(\mathfrak{d}_{K_n/F_n})$.

Exercice 6. — Soit W un sous K-espace vectoriel de dimension finie d de $\widehat{K}_\infty$ stable par Γ_K. Soit $e_1, \dots, e_d$ une base de W sur K, et si $\gamma \in \Gamma_K$, soit $U_\gamma \in \mathbf{GL}_d(K)$ la matrice $(a_{i,j})_{1\leqslant i,j\leqslant d}$ définie par $\gamma(e_i) = \sum_{j=1}^d a_{i,j}e_j$.

(i) Montrer qu'il existe $n \geqslant n_0(K)$ tel que $U_\gamma \in 1 + p^2\mathbf{M}_d(\mathscr{O}_K)$, si $\gamma \in \Gamma_{K_n}$.

(ii) Soit $f_i = e_i - \mathrm{R}_{K,n}(e_i)$. Montrer que $\gamma(f_i) = \sum_{j=1}^d a_{i,j}f_j$, si $\gamma \in \Gamma_{K_n}$.

(iii) Soit $k \in \{1, \dots, d\}$ tel que $v_p(f_k) \leqslant v_p(f_i)$ quel que soit $i \in \{1, \dots, d\}$. Montrer que $v_p(\gamma(f_k) - f_k) \geqslant v_p(f_k) + 2$, si $\gamma \in \Gamma_{K_n}$. En déduire que $f_k = 0$.

(iv) Montrer que W est inclus dans K_∞ et que Γ_K agit à travers un quotient fini.

Exercice 7. — Soit $\mathbf{B}_{\mathrm{HT}}$ l'anneau $\mathbf{C}_p[T, T^{-1}]$ muni de l'action de Galois définie par

$$\sigma(\sum_{n=a}^{b} x_nT^n) = \sum_{n=a}^{b} \sigma(x_n)\chi(\sigma)^nT^n \quad \text{si } \sigma \in \mathrm{G}_{\mathbf{Q}_p}.$$

(Autrement dit, T est un $2i\pi$ « formel ».) Soit K une extension finie de $\mathbf{Q}_p$.

(i) Montrer que $(\mathbf{B}_{\mathrm{HT}})^{\mathrm{G}_K} = K$.

(ii) Quels sont les éléments inversibles de $\mathbf{B}_{\mathrm{HT}}$?

(iii) Montrer que, si $x \in \mathbf{B}_{\mathrm{HT}} - \{0\}$ est tel que $\sigma(x) = u_\sigma x$, avec u_σ inversible dans $\mathbf{B}_{\mathrm{HT}}$ quel que soit $\sigma \in \mathrm{G}_K$, alors x est inversible dans $\mathbf{B}_{\mathrm{HT}}$. En déduire que $\mathrm{Frac}(\mathbf{B}_{\mathrm{HT}})^{\mathrm{G}_K} = K$.

1.5. Remarques sur les représentations galoisiennes

Si G est un groupe topologique compact (comme $\mathrm{G}_{\mathbf{Q}_\ell}$ ou $\mathrm{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$), une *représentation p-adique* de G, est un module libre V de rang fini sur l'anneau des entiers d'une extension finie E de $\mathbf{Q}_p$, muni d'une action continue de G. Si on veut préciser l'extension de $\mathbf{Q}_p$, on parle de $\mathscr{O}_E$-représentation.

La géométrie algébrique fournit des représentations p-adiques de $\mathrm{G}_{\mathbf{Q}}$ en abondance (cohomologie étale des variétés algébriques définies sur $\mathbf{Q}$), et l'étude de ces représentations s'est révélée être une aide précieuse pour des tas de questions de théorie des nombres. Par exemple, la démonstration de Wiles du théorème de Fermat s'appuie de manière cruciale sur l'étude des représentations de $\mathrm{G}_{\mathbf{Q}}$ attachées aux courbes elliptiques et aux formes modulaires.

Maintenant, si on fixe un plongement de $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_\ell$, pour tout nombre premier ℓ, on peut voir $\mathrm{G}_{\mathbf{Q}_\ell}$ comme un sous-groupe de $\mathrm{G}_{\mathbf{Q}}$, et les $\mathrm{G}_{\mathbf{Q}_\ell}$ engendrent topologiquement $\mathrm{G}_{\mathbf{Q}}$. La manière dont les $\mathrm{G}_{\mathbf{Q}_\ell}$ se mélangent dans $\mathrm{G}_{\mathbf{Q}}$, est très mystérieuse, mais on peut obtenir énormément d'informations sur une représentation p-adique de $\mathrm{G}_{\mathbf{Q}}$ en regardant sa restriction à $\mathrm{G}_{\mathbf{Q}_\ell}$, pour ℓ premier. Pour des raisons topologiques, c'est la restriction à $\mathrm{G}_{\mathbf{Q}_p}$ qui fournit les renseignements les plus subtils ($\mathbf{GL}_d(\mathscr{O}_E)$ est essentiellement un p-groupe et donc l'image du sous-groupe d'inertie sauvage de $\mathrm{G}_{\mathbf{Q}_\ell}$ par un morphisme continu est d'image finie si $\ell \neq p$, car ce sous-groupe d'inertie sauvage est un ℓ-groupe ; par contre l'image du sous-groupe d'inertie sauvage de $\mathrm{G}_{\mathbf{Q}_p}$ n'a aucune raison d'être finie comme le montre l'exemple du caractère cyclotomique).

Fontaine a introduit une stratégie extrêmement féconde pour classifier les représentations p-adiques de $\mathrm{G}_{\mathbf{Q}_p}$. Celle-ci consiste à construire des anneaux topologiques B, munis d'une action de $\mathrm{G}_{\mathbf{Q}_p}$ et de structures additionnelles respectées par l'action de $\mathrm{G}_{\mathbf{Q}_p}$, et d'étudier le B-module

$B \otimes V$, muni de l'action diagonale de $\mathrm{G}_{\mathbf{Q}_p}$. Une illustration rapide des méthodes de Fontaine se trouve aux n[os] 2.3 et 2.6. L'exemple le plus simple d'invariant que l'on peut obtenir de cette manière est dû à Sen ; il utilise l'anneau $B = \mathbf{C}_p$, et repose de manière cruciale sur les prop. 1.17 et 1.14. Les exercices 6, 2 et 5 donnent une idée des techniques utilisées.

Théorème 1.18. — *Soit K une extension finie de $\mathbf{Q}_p$. Soit V une $\mathbf{Z}_p$-représentation de dimension d de G_K. Alors $\mathbf{C}_p \otimes_{\mathbf{Z}_p} V$ contient un unique sous-K_∞-espace vectoriel $D_{\mathrm{Sen}}(V)$ de dimension d, fixe par H_K, stable par G_K* (agissant à travers Γ_K)*, et engendrant le $\mathbf{C}_p$-espace vectoriel $\mathbf{C}_p \otimes_{\mathbf{Z}_p} V$. De plus, si $x \in D_{\mathrm{Sen}}(V)$, alors $\frac{\gamma-1}{\chi(\gamma)-1}x$ tend vers une limite $\Theta_{\mathrm{Sen}}(x)$ quand γ tend vers 1 dans Γ_K, et $x \mapsto \Theta_{\mathrm{sen}}(x)$ est K_∞-linéaire.*

Définition 1.19. — L'opérateur Θ_{Sen} s'appelle *l'opérateur de Sen* associé à V ; ses valeurs propres sont *les poids de Hodge-Tate* de V, et V *est de Hodge-Tate* si Θ_{Sen} est diagonalisable, et si les poids de Hodge-Tate de V sont des entiers.

Toute cette théorie a pour origine un travail de Tate dans lequel celui-ci conjecture que les représentations de G_K provenant de la géométrie algébrique sont de Hodge-Tate, ce qui a été démontré par Faltings en 1988.

Exemple 1.20. — Soit $k \in \mathbf{Z}$. La puissance k-ième χ^k du caractère cyclotomique définit une $\mathbf{Z}_p$-représentation V_k de dimension 1 de G_K [notée habituellement $\mathbf{Z}_p(k)$] ; on a $\sigma(x) = \chi(\sigma)^k x$ quel que soient $\sigma \in \mathrm{G}_K$ et $x \in V_k$. Comme l'action de G_K se factorise à travers Γ_K, on a $D_{\mathrm{Sen}}(V) = K_\infty \otimes_{\mathbf{Z}_p} V_k$. Un élément x de $D_{\mathrm{Sen}}(V)$ appartient donc à $K_n \otimes_{\mathbf{Z}_p} V_k$ si n est assez grand, et on a $\gamma(x) = \chi(\gamma)^k x$, si γ est proche de 1. On en déduit que Θ_{Sen} est la multiplication par k. La représentation V_k est l'exemple de base d'une représentation de Hodge-Tate de poids k.

2. Quelques anneaux de Fontaine

2.1. L'anneau $\widetilde{\mathbf{E}}^+$. — Rappelons que l'on a défini, si A est un anneau, l'ensemble $\mathbb{R}(A)$ des suites $(x^{(n)})_{n\in\mathbf{N}}$ d'éléments de A telles que l'on ait $(x^{(n+1)})^p = x^{(n)}$ quel que soit $n \in \mathbf{N}$. On a aussi montré que, si A est un p anneau d'anneau résiduel R, alors l'application naturelle de $\mathbb{R}(A)$ dans $\mathbb{R}(R)$, est une bijection, la réciproque étant définie par $x \mapsto \psi_A(x)$, où $\psi_A^{(n)}(x) = \lim_{k\to+\infty}(\hat{x}^{(n+k)})^{p^k}$, et où $\hat{x}^{(n)}$ est un relèvement quelconque de $x^{(n)} \in R$ dans A.

Maintenant, R étant un anneau de caractéristique p, l'application $x \mapsto x^p$ est un morphisme d'anneaux de R dans R, et l'ensemble $\mathbb{R}(R)$ est un sous-anneau de $R^{\mathbf{N}}$. Ceci permet de munir $\mathbb{R}(A)$ d'une structure d'anneau parfait de caractéristique p. La somme et le produit de $x = (x^{(n)})_{n\in\mathbf{N}}$ et $y = (y^{(n)})_{n\in\mathbf{N}}$ étant donnés par les formules

$$(x+y)^{(n)} = \lim_{k\to+\infty}(x^{(n+k)} + y^{(n+k)})^{p^k} \quad \text{et} \quad (xy)^{(n)} = x^{(n)}y^{(n)},$$

la racine p-ième de $x = (x^{(n)})_{n\in\mathbf{N}}$ étant $x^{1/p} = (x^{(n+1)})_{n\in\mathbf{N}}$.

On note $\widetilde{\mathbf{E}}^+$ l'anneau $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$ que l'on peut aussi, d'après ce qui précède, voir comme $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\varpi\mathscr{O}_{\mathbf{C}_p})$, pour n'importe que choix de $\varpi \in \mathscr{O}_{\mathbf{C}_p}$ vérifiant $0 < v_p(\varpi) \leqslant 1$. On remarquera que $\overline{\mathbf{F}}_p$ étant un sous-anneau parfait de $\mathscr{O}_{\mathbf{C}_p}/\varpi\mathscr{O}_{\mathbf{C}_p}$, l'anneau $\widetilde{\mathbf{E}}^+$ contient $\mathbb{R}(\overline{\mathbf{F}}_p)$ qui s'identifie naturellement à $\overline{\mathbf{F}}_p$ par l'application $x = (x^{(n)})_{n\in\mathbf{N}} \mapsto x^{(0)}$.

Si $x = (x^{(n)})_{n\in\mathbf{N}} \in \widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$, on pose $v_{\mathbf{E}}(x) = v_p(x^{(0)})$, ce qui fait que l'on a $v_{\mathbf{E}}(x) = p^n v_p(x^{(n)})$ quel que soit $n \in \mathbf{N}$.

Finalement, si $\sigma \in \mathrm{G}_F$, on fait agir σ sur $\widetilde{\mathbf{E}}^+$, en définissant $\sigma(x)$, si $x = (x^{(n)})_{n\in\mathbf{N}}$ par la formule $\sigma(x) = (\sigma(x^{(n)}))_{n\in\mathbf{N}}$.

Théorème 2.1. — (i) $\widetilde{\mathbf{E}}^+$ *est un anneau de caractéristique* p *qui est parfait et l'application* $v_{\mathbf{E}}$ *en est une valuation pour laquelle il est complet.*

(ii) *L'action de* G_F *sur* $\widetilde{\mathbf{E}}^+$ *est continue, respecte sa structure d'anneau, et commute à l'action de d'endomorphisme de Frobenius* φ *défini par* $\varphi(x) = x^p$.

Démonstration. — (i) On a déjà vu que $\widetilde{\mathbf{E}}^+$ est un anneau parfait de caractéristique p. Si $x = (x^{(n)})_{n\in\mathbf{N}}$ et $(y^{(n)})_{n\in\mathbf{N}}$ sont deux éléments de $\widetilde{\mathbf{E}}^+$, on a

$$v_p((x^{(n)} + y^{(n)})^{p^n}) = p^n v_p(x^{(n)} + y^{(n)}) \geqslant \inf(p^n v_p(x^{(n)}), p^n v_p(y^{(n)})) = \inf(v_{\mathbf{E}}(x), v_{\mathbf{E}}(y)),$$

ce qui, passant à la limite, nous fournit l'inégalité $v_{\mathbf{E}}(x + y) \geqslant \inf(v_{\mathbf{E}}(x), v_{\mathbf{E}}(y))$ et permet de montrer que $v_{\mathbf{E}}$ est une valuation (les autres propriétés à vérifier étant immédiates).

D'autre part, on a $v_{\mathbf{E}}(x-y) \geqslant p^n$ si et seulement si $x^{(0)} = y^{(0)}, \ldots, x^{(n)} = y^{(n)}$ dans $\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$, ce qui montre que la base de voisinages de x pour la topologie induite par $v_{\mathbf{E}}$ constituée des $\{y \mid v_{\mathbf{E}}(x - y) \geqslant p^n\}$ est aussi une base de voisinages de x pour la topologie de $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})$ induite par la topologie produit sur $(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})^{\mathbf{N}}$, chacun des facteurs étant muni de la topologie discrète. On en tire la complétude de $\widetilde{\mathbf{E}}^+$ car un produit d'espaces discrets est complet.

(ii) Le fait que l'action de G_F respecte la structure d'anneau de $\widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})$ est évident. D'autre part, si $\sigma \in \mathrm{G}_F$, on a $v_{\mathbf{E}}(\sigma(x)) = v_{\mathbf{E}}(x)$ ce qui fait que G_F agit par des isométries et donc continûment et le fait que cette action commute à φ est une évidence. Reste à vérifier que, si $x = (x^{(n)})_{n\in\mathbf{N}} \in \widetilde{\mathbf{E}}^+$, alors l'application $\sigma \mapsto \sigma(x)$ est continue. Soient $M > 0$ et n tel que $p^n \geqslant M$. Soit $y \in \mathscr{O}_{\overline{F}}$ tel que $v_p(x^{(n)}-y) \geqslant 1$ et soit K une extension finie galoisienne de F contenant y. Si $\sigma \in \mathrm{G}_F$ et $\tau \in \mathrm{G}_K$, alors $v_p(\sigma\tau(x^{(n)})-\sigma(x^{(n)})) = v_p(\sigma\tau(x^{(n)}-y)-\sigma(x^{(n)}-y)) \geqslant 1$ et donc $v_{\mathbf{E}}(\sigma\tau(x) - \sigma(x)) \geqslant p^n \geqslant M$. Ceci permet de conclure.

Proposition 2.2. — (i) $(\widetilde{\mathbf{E}}^+)^{\varphi=1} = \mathbf{F}_p$.

(ii) *Si* K *est une extension finie de* F, *alors* $(\widetilde{\mathbf{E}}^+)^{\mathrm{G}_K} = k_K$.

Démonstration. — (i) $\varphi(x) = x$ si et seulement si $x^p - x = 0$ et donc si et seulement si $x \in \mathbf{F}_p$ puisque $\widetilde{\mathbf{E}}^+$ est intègre (car muni d'une valuation).

(ii) Par définition de l'action de G_K, on a $(\widetilde{\mathbf{E}}^+)^{\mathrm{G}_K} = \mathbb{R}((\mathscr{O}_{\mathbf{C}_p})^{\mathrm{G}_K})$. Par ailleurs, d'après le theórème d'Ax-Sen-Tate, $\mathbb{R}((\mathscr{O}_{\mathbf{C}_p})^{\mathrm{G}_K}) = \mathbb{R}(\mathscr{O}_K)$. Finalement, $\mathscr{O}_K$ étant un p-anneau (pas strict) d'anneau résiduel k_K, on a $\mathbb{R}(\mathscr{O}_K) = \mathbb{R}(k_K)$, et comme k_K est parfait, $\mathbb{R}(k_K) \cong k_K$.

2.2. Les éléments ε et $\overline{\pi}$. — Soit $\varepsilon = (1, \varepsilon^{(1)}, \ldots, \varepsilon^{(n)}, \ldots) \in \widetilde{\mathbf{E}}^+$, avec $\varepsilon^{(1)} \neq 1$, ce qui fait que $\varepsilon^{(n)}$ est une racine primitive p^n-ième de l'unité. Soit $\overline{\pi} = \varepsilon - 1$ On a

$$v_{\mathbf{E}}(\overline{\pi}) = \lim_{n\to+\infty} p^n v_p(\varepsilon^{(n)} - 1) = \frac{p}{p-1} > 1 > 0.$$

Proposition 2.3. — *Si* $\sigma \in \mathrm{G}_F$, *alors* $\sigma(\varepsilon) = \varepsilon^{\chi(\sigma)}$, *où* χ *est le caractère cyclotomique.*

Démonstration. — Comme on le verra un peu plus tard, on a $\binom{x}{n} \in \mathbf{Z}_p$, si $x \in \mathbf{Z}_p$, ce qui montre que la série $(1+T)^x = \sum_{n=0}^{+\infty} \binom{x}{n} T^n$ converge dans tout corps complet pour une valuation v, dès que $v(T) > 0$. Dans le cas qui nous intéresse, on a $v_p(\varepsilon^{(n)} - 1) > 0$ et $v_{\mathbf{E}}(\varepsilon - 1) > 0$, ce qui donne un sens à $\varepsilon^{\chi(\sigma)}$ et $(\varepsilon^{(n)})^{\chi(\sigma)}$. On a alors, par définition du caractère cyclotomique,

$$\sigma(\varepsilon) = (\sigma(\varepsilon^{(n)}))_{n\in\mathbf{N}} = ((\varepsilon^{(n)})^{\chi(\sigma)})_{n\in\mathbf{N}} = \varepsilon^{\chi(\sigma)}.$$

L'anneau $\widetilde{\mathbf{E}}^+$ étant un anneau valué complet, et $v_{\mathbf{E}}(\overline{\pi}) > 0$, le corps des fractions $\widetilde{\mathbf{E}}$ de $\widetilde{\mathbf{E}}^+$ n'est autre que $\widetilde{\mathbf{E}}^+[\overline{\pi}^{-1}]$. On étend $v_{\mathbf{E}}$ à $\widetilde{\mathbf{E}}$ par $v_{\mathbf{E}}(\overline{\pi}^{-n}x) = v_{\mathbf{E}}(x) - v_{\mathbf{E}}(\overline{\pi})$, ce qui fait de $\widetilde{\mathbf{E}}$ un corps complet pour la valuation (non discrète) $v_{\mathbf{E}}$, et on étend les actions de $\mathrm{G}_{\mathbf{Q}_p}$ et φ de manière évidente à $\widetilde{\mathbf{E}}$.

2.3. L'anneau $\mathbf{B}_{\mathrm{dR}}^+$ des « nombres complexes p-adiques »

On note $\widetilde{\mathbf{A}}^+$ l'anneau des vecteurs de Witt $W(\widetilde{\mathbf{E}}^+)$ à coefficients dans l'anneau parfait $\widetilde{\mathbf{E}}^+$. Tout élément de $\widetilde{\mathbf{A}}^+$ peut s'écrire de manière unique sous la forme $x = \sum_{n=0}^{+\infty} p^n[x_n]$, où $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\widetilde{\mathbf{E}}^+$. D'après les résultats généraux sur les vecteurs de Witt, les actions de $\mathrm{G}_{\mathbf{Q}_p}$ et φ sur $\widetilde{\mathbf{E}}^+$ se relèvent de manière unique en des actions de $\mathrm{G}_{\mathbf{Q}_p}$ et φ sur $\widetilde{\mathbf{A}}^+$. De manière explicite, on a

$$\varphi\Big(\sum_{n=0}^{+\infty} p^n[x_n]\Big) = \sum_{n=0}^{+\infty} p^n[x_n^p] \quad \text{et} \quad \sigma\Big(\sum_{n=0}^{+\infty} p^n[x_n]\Big) = \sum_{n=0}^{+\infty} p^n[\sigma(x_n)], \text{ si } \sigma \in \mathrm{G}_{\mathbf{Q}_p}.$$

On a $\widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}) = \mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$. On note $\overline{\theta} : \widetilde{\mathbf{E}}^+ \to \mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$ l'application qui, à $x = (x_n)_{n\in\mathbf{N}} \in \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p})$ associe $x_0 \in \mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$. Ceci fait de $\overline{\theta}$ un morphisme d'anneaux de $\widetilde{\mathbf{E}}^+$ dans $\mathscr{O}_{\mathbf{C}_p}/p\mathscr{O}_{\mathbf{C}_p}$ qui, de manière évidente, est surjectif et commute à l'action de $\mathrm{G}_{\mathbf{Q}_p}$.

On note $\tilde{\theta} : \widetilde{\mathbf{E}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ l'application qui, à $x = (x^{(n)})_{n\in\mathbf{N}} \in \mathbb{R}(\mathscr{O}_{\mathbf{C}_p})$ associe $x^{(0)} \in \mathscr{O}_{\mathbf{C}_p}$. Ceci fait de $\tilde{\theta}$ une application multiplicative de $\widetilde{\mathbf{E}}^+$ dans $\mathscr{O}_{\mathbf{C}_p}$, dont la réduction modulo p est $\overline{\theta}$. Il résulte de la propriété universelle des vecteurs de Witt, que l'application $\theta : \widetilde{\mathbf{A}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ définie par

$$\theta\Big(\sum_{n=0}^{+\infty} p^n[x_n]\Big) = \sum_{n=0}^{+\infty} p^n x_n^{(0)},$$

est un morphisme d'anneaux.

Il y a deux topologies naturelles que l'on peut mettre sur $\widetilde{\mathbf{A}}^+$. La *topologie forte*, qui n'est autre que la topologie p-adique, fait de l'application $\sum_{n=0}^{+\infty} p^n[x_n] \mapsto (x_n)_{n\in\mathbf{N}}$ un homéomorphisme de $\widetilde{\mathbf{A}}^+$ sur $(\widetilde{\mathbf{E}}^+)^{\mathbf{N}}$, où l'on a muni $\widetilde{\mathbf{E}}^+$ de la topologie discrète. La topologie naturelle sur $\widetilde{\mathbf{A}}^+$ est celle qui fait de $\sum_{n=0}^{+\infty} p^n[x_n] \mapsto (x_n)_{n\in\mathbf{N}}$ un homéomorphisme de $\widetilde{\mathbf{A}}^+$ sur $(\widetilde{\mathbf{E}}^+)^{\mathbf{N}}$, où l'on a muni $\widetilde{\mathbf{E}}^+$ de la topologie définie par $v_{\mathbf{E}}$. Cette topologie, la *topologie faible*, est plus faible que la topologie p-adique, mais $\widetilde{\mathbf{A}}^+$ est encore complet pour cette topologie puisque $\widetilde{\mathbf{E}}^+$ est complet pour $v_{\mathbf{E}}$.

Proposition 2.4. — (i) *Le morphisme $\theta : \widetilde{\mathbf{A}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ est surjectif, et commute avec l'action de $\mathrm{G}_{\mathbf{Q}_p}$.*

(ii) *Le noyau de θ est principal, et un élément $x = \sum_{n=0}^{+\infty} p^n[x_n]$ en est un générateur, si et seulement si $v_{\mathbf{E}}(x_0) = 1$.*

Démonstration. — Le (i) est plus ou moins immédiat ; montrons le (ii). Si $x = \sum_{n=0}^{+\infty} p^n[x_n] \in \widetilde{\mathbf{A}}^+$, on note $\overline{x} = x_0$ son image dans $\widetilde{\mathbf{E}}^+$. Si $x \in \ker\theta$, on a $x_0^{(0)} = -\sum_{n=1}^{+\infty} p^n x_n^{(0)}$, ce qui implique $v_{\mathbf{E}}(\overline{x}) = v_p(x_0^{(0)}) \geqslant 1$. Soit alors $x = \sum_{n=0}^{+\infty} p^n[x_n]$ vérifiant $v_{\mathbf{E}}(\overline{x}) = 1$, et soit $y \in \ker\theta$. D'après ce qui précède, on a $v_{\mathbf{E}}(\overline{y}) \geqslant 1$; il existe donc $a_0 \in \widetilde{\mathbf{E}}^+$ tel que $\overline{y} = a_0\overline{x}$. On peut alors écrire y sous la forme $y = [a_0]x + py_1$, avec $y_1 \in \widetilde{\mathbf{A}}^+$. De plus, $p\theta(y_1) = \theta(y) - \theta([a_0])\theta(x) = 0$, ce qui prouve que $y \in \ker\theta$. On peut donc refaire avec y_1 ce que l'on a fait avec y, ce qui permet de construire, par récurrence, une suite $(a_n)_{n\in\mathbf{N}}$ d'éléments de $\widetilde{\mathbf{A}}^+$, telle que l'on ait, pour tout $n \in \mathbf{N}$, $y = ([a_0] + \cdots + p^n[a_n])x + p^{n+1}y_{n+1}$, avec $y_{n+1} \in \ker\theta$. On a donc $y = \big(\sum_{n=0}^{+\infty} p^n[a_n]\big)x$, ce qui montre que x est un générateur de $\ker\theta$, et permet de conclure.

Exemple 2.5. — Si on pose $\omega = \frac{[\varepsilon]-1}{[\varepsilon^{1/p}]-1} = 1 + [\varepsilon^{1/p}] + \cdots + [\varepsilon^{1/p}]^{p-1}$, on a $\theta(\omega) = 0$ puisque $\theta([\varepsilon]) = 1$ et $\theta([\varepsilon^{1/p}]) = \varepsilon^{(1)} \neq 1$. Par ailleurs, l'image $\overline{\omega}$ de ω dans $\widetilde{\mathbf{E}}^+$ est $\frac{\varepsilon-1}{\varepsilon^{1/p}-1} = (\varepsilon-1)^{1-1/p}$, et on a donc $v_{\mathbf{E}}(\overline{\omega}) = (1-1/p)v_{\mathbf{E}}(\varepsilon-1) = 1$. Ceci montre que ω est un générateur de $\ker\theta$.

Exercice 8. — Soit F une extension non ramifiée de $\mathbf{Q}_p$. Soit K une extension totalement ramifiée de F de degré $e > 1$, soit π_K une uniformisante de K, soit $P \in \mathscr{O}_F[X]$ le polynôme minimal de π_K sur F, et soit $\tilde{\pi}_K \in \widetilde{\mathbf{A}}^+$ vérifiant $\theta(\tilde{\pi}_K) = \pi_K$. Montrer que $P(\tilde{\pi}_K)$ est un générateur de $\ker\theta$.

Exercice 9. — (i) Montrer que la topologie faible est aussi la topologie $(p, \ker\theta)$-adique.

(ii) Montrer que $\mathrm{G}_{\mathbf{Q}_p}$ agit continûment sur $\widetilde{\mathbf{A}}^+$ pour la topologie faible, mais pas pour la topologie p-adique.

On étend θ par $\mathbf{Q}_p$-linéarité en un morphisme d'anneaux de $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$ dans $\mathbf{C}_p$. Le noyau de θ est encore principal engendré par ω, et on note $\mathbf{B}_{\mathrm{dR}}^+$ le séparé complété de $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$ pour la topologie ω-adique. On note v_H la valuation définie par ω sur $\mathbf{B}_{\mathrm{dR}}^+$. Par construction, cette valuation est discrète et $\mathbf{B}_{\mathrm{dR}}^+$ est complet ; le corps résiduel est le même que celui de $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$; c'est donc $\mathbf{C}_p$.

Comme $\ker\theta$ est stable par $\mathrm{G}_{\mathbf{Q}_p}$ l'action de $\mathrm{G}_{\mathbf{Q}_p}$ sur $\widetilde{\mathbf{A}}^+[\frac{1}{p}]$ s'étend par continuité à $\mathbf{B}_{\mathrm{dR}}^+$; par contre, celle de φ ne s'étend pas car $\ker\theta$ n'est pas stable par φ.

Comme $[\varepsilon] - 1 \in \ker\theta$, la série $\log[\varepsilon] = -\sum_{n=1}^{+\infty} \frac{(1-[\varepsilon])^n}{n}$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$. On note t la somme. Si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on a

$$\sigma(t) = \sigma(\log[\varepsilon]) = \log[\sigma(\varepsilon)] = \log[\varepsilon^{\chi(\sigma)}] = \log[\varepsilon]^{\chi(\sigma)} = \chi(\sigma)\log[\varepsilon] = \chi(\sigma)t.$$

Ceci fait de t un analogue p-adique de $2i\pi$ (c'est le « $2i\pi$ de Fontaine »). On a $\theta(t) = 0$, ce qui explique que l'on ne le voit pas dans $\mathbf{C}_p$.

Exercice 10. — Calculer $\theta(\omega^{-1}t)$. En déduire que t est une uniformisante de $\mathbf{B}_{\mathrm{dR}}^+$.

(ii) Soit M la clôture algébrique de $\mathbf{Q}_p$ dans $\mathbf{B}_{\mathrm{dR}}^+$. Montrer que θ induit un isomorphisme de M sur $\overline{\mathbf{Q}}_p$ qui commute à l'action de $\mathrm{G}_{\mathbf{Q}_p}$.

(iii) Montrer que, si K est une extension finie de $\mathbf{Q}_p$, alors $(\mathbf{B}_{\mathrm{dR}}^+)^{\mathrm{G}_K} = K$.

(iv) Montrer que le corps des fractions de $\mathbf{B}_{\mathrm{dR}}^+$ est $\mathbf{B}_{\mathrm{dR}} = \mathbf{B}_{\mathrm{dR}}^+[\frac{1}{t}]$ et que l'on a $\mathbf{B}_{\mathrm{dR}}^{\mathrm{G}_K} = K$, si K est une extension finie de $\mathbf{Q}_p$.

Remarque 2.6. — On montre, en utilisant les résultats de cet exercice, que, si K est une extension finie de $\mathbf{Q}_p$, et si V est une $\mathbf{Z}_p$-représentation de G_K, alors le K espace vectoriel

$\mathbf{D}_{\mathrm{dR}}(V) = (\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Z}_p} V)^{\mathrm{G}_K}$ est de dimension inférieure ou égale au rang de V sur $\mathbf{Z}_p$. On dit que V est *de de Rham* si on a égalité. Fontaine a conjecturé, et Faltings et Tsuji ont démontré, que les représentations de G_K provenant de la géométrie algébrique sont de de Rham. Ceci nous fournit une contrainte très forte pour qu'une représentation provienne de la géométrie, ce qui a des tas d'applications en géométrie arithmétique.

Remarque 2.7. — La topologie naturelle sur $\mathbf{B}_{\mathrm{dR}}^+$ n'est pas la topologie définie par v_H ; celle-ci est beaucoup trop forte pour être utile (elle correspond à la topologie discrète sur $\mathbf{C}_p$...). La topologie naturelle sur $\mathbf{B}_{\mathrm{dR}}^+$ est celle pour laquelle les $p^k\widetilde{\mathbf{A}}^+ + \omega^n\mathbf{B}_{\mathrm{dR}}^+$, avec $k, n \in \mathbf{N}$, forment une base de voisinage de 0. Elle est (beaucoup) plus faible que la topologie induite par v_H.

Exercice 11. — (i) Montrer que l'action de $\mathrm{G}_{\mathbf{Q}_p}$ sur $\mathbf{B}_{\mathrm{dR}}^+$ muni de sa topologie naturelle est continue.

Remarque 2.8. — (i) Comme $\mathbf{B}_{\mathrm{dR}}^+$ est un anneau complet pour la valuation discrète v_H, que t en est une uniformisante, et que le corps résiduel est $\mathbf{C}_p$, il est abstraitement isomorphe à $\mathbf{C}_p[[t]]$, mais ce résultat n'est d'aucune utilité car on peut montrer (ce n'est pas du tout trivial) qu'il n'existe aucun isomorphisme de ce type qui soit compatible à l'action de $\mathrm{G}_{\mathbf{Q}_p}$ ou qui soit continue.

(ii) La topologie naturelle sur $\widetilde{\mathbf{A}}^+$ ou $\mathbf{B}_{\mathrm{dR}}^+$ a l'air un peu compliquée, mais on peut très souvent raisonner comme si on travaillait dans $\mathscr{O}_{\mathbf{C}_p}[[T]]$ ou $\mathbf{C}_p[[T]]$ de la manière suivante. On choisit une section $\mathbf{Z}_p$-linéaire $s : \mathscr{O}_{\mathbf{C}_p} \to \widetilde{\mathbf{A}}^+$ de θ (i.e. $s(ax+by) = as(x)+bs(y)$ si $a, b, \in \mathbf{Z}_p$ et $x, y \in \mathscr{O}_{\mathbf{C}_p}$), que l'on étend par $\mathbf{Q}_p$-linéarité en $s : \mathbf{C}_p \to \widetilde{\mathbf{A}}^+[\frac{1}{p}] \subset \mathbf{B}_{\mathrm{dR}}^+$, et on choisit un générateur ξ de $\ker\theta$ dans $\widetilde{\mathbf{A}}^+$. Alors tout élément de $\widetilde{\mathbf{A}}^+$ (resp. de $\mathbf{B}_{\mathrm{dR}}^+$) peut s'écrire de manière unique (exercice) sous la forme $\sum_{n=0}^{+\infty} s(a_n)\xi^n$ avec $(a_n)_{n\in\mathbf{N}} \in (\mathscr{O}_{\mathbf{C}_p})^{\mathbf{N}}$ (resp. $(a_n)_{n\in\mathbf{N}} \in (\mathbf{C}_p)^{\mathbf{N}}$), et la topologie naturelle sur $\widetilde{\mathbf{A}}^+$ (resp. $\mathbf{B}_{\mathrm{dR}}^+$) correspond à la topologie produit sur $(\mathscr{O}_{\mathbf{C}_p})^{\mathbf{N}}$ (resp. $(\mathbf{C}_p)^{\mathbf{N}}$). Comme s n'est pas multiplicative, il faut faire un peu plus attention que d'habitude, mais on est en général sauvé par le fait $s(a)s(b) \in p^{n+m}\widetilde{\mathbf{A}}^+$ si $a \in p^n\mathscr{O}_{\mathbf{C}_p}$ et $b \in p^m\mathscr{O}_{\mathbf{C}_p}$.

Exercice 12. — (i) Montrer que, si $x \in \widetilde{\mathbf{E}}^+$, et si $v_{\mathbf{E}}(x-1) > 0$, alors la série $\log[x] = -\sum_{n=1}^{+\infty} \frac{(1-[x])^n}{n}$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$.

(ii) Plus généralement, montrer que, si $(a_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{Q}_p$, et si $x \in \mathbf{B}_{\mathrm{dR}}^+$ est tel que la série $\sum_{n=0}^{+\infty} a_n\theta(x)^n$ converge dans $\mathbf{C}_p$, alors $\sum_{n=0}^{+\infty} a_n x^n$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$.

2.4. Le corps des normes de l'extension cyclotomique. — Dans tout ce qui suit, K désigne une extension finie de $\mathbf{Q}_p$, et $F = W(k_K)[\frac{1}{p}]$ (resp. $F' = W(k_{K_\infty})[\frac{1}{p}]$) est l'extension maximale de $\mathbf{Q}_p$ contenue dans K (resp. K_∞).

Lemme 2.9. — *Si $x \in \mathscr{O}_{F_{n+1}}$ et $\sigma \in \mathrm{Gal}(F_{n+1}/F_n)$, alors $v_p(\sigma(x) - x) \geqslant \frac{1}{p-1}$.*

Démonstration. — x peut s'écrire sous la forme $x = \sum_{i=0}^{p-1} x_i(\varepsilon^{(n+1)})^i$, avec $x_i \in \mathscr{O}_{F_n}$ si $0 \leqslant i \leqslant p-1$. Par ailleurs, $\sigma(\varepsilon^{(n+1)}) = \zeta_\sigma\varepsilon^{(n+1)}$, où ζ_σ est une racine p-ième de l'unité, et donc $\sigma(x) - x = \sum_{i=0}^{p-1} x_i(\varepsilon^{(n+1)})^i(\zeta_\sigma^i - 1)$. Le résultat suit de la minoration $v_p(\zeta - 1) \geqslant \frac{1}{p-1}$ si $\zeta^p = 1$.

Notons $\mathfrak{a}$ l'idéal des éléments de valuation $\geqslant \frac{1}{p}$.

Lemme 2.10. — *Si $n \geqslant n_0(K) + 1$ et si $x \in \mathscr{O}_{K_{n+1}}$, alors $\mathrm{N}_{K_{n+1}/K_n}(x) - x^p \in \mathfrak{a}$.*

Démonstration. — Soit $e_1, \dots, e_d$ une base de $\mathscr{O}_{K_n}$ sur $\mathscr{O}_{F_n}$; c'est aussi une base de K_{n+1} sur F_{n+1} car K_{n+1}/K_n et F_{n+1}/F_n sont de degré p. Soit $e_1^*, \dots, e_d^*$ la base de K_n sur F_n duale de $e_1, \dots, e_d$ pour la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{K_n/F_n}(xy)$ qui est aussi la restriction à K_n de la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{K_{n+1}/F_{n+1}}(xy)$. Les e_i^* sont éléments de $\mathfrak{d}_{K_n/F_n}^{-1}$ et donc vérifient $v_p(e_i^*) \geqslant -\frac{1}{p-1} p^{n_0(K)-n} \geqslant -\frac{1}{p(p-1)}$. On peut alors écrire $x \in \mathscr{O}_{K_{n+1}}$ sous la forme $\sum_{i=1}^d x_i e_i^*$, avec $x_i = \mathrm{Tr}_{K_{n+1}/F_{n+1}}(x e_i) \in \mathscr{O}_{F_{n+1}}$. On a $\mathrm{Gal}(K_{n+1}/K_n) = \mathrm{Gal}(F_{n+1}/F_n)$ et, comme $v_p(\sigma(x_i) - x_i) \geqslant \frac{1}{p-1}$ d'après le lemme 2.9, on obtient finalement,

$$v_p(\sigma(x) - x) = v_p\Big(\sum_{i=1}^d (\sigma(x_i) - x_i) e_i^*\Big) \geqslant \frac{1}{p-1} - \frac{1}{p(p-1)} = \frac{1}{p},$$

quel que soit $\sigma \in \mathrm{Gal}(K_{n+1}/K_n)$. Comme $\mathrm{N}_{K_{n+1}/K_n}(x) = \prod_{\sigma \in \mathrm{Gal}(K_{n+1}/K_n)} \sigma(x)$, et comme $\mathrm{Gal}(K_{n+1}/K_n)$ est de cardinal p, cela permet de conclure.

Corollaire 2.11. — *Si $n \geqslant n_0(K) + 1$ et si $x \in \mathscr{O}_{K_{n+1}}/\mathfrak{a}$, alors $x^p \in \mathscr{O}_{K_n}/\mathfrak{a}$ et le morphisme d'anneaux $x \mapsto x^p$ de $\mathscr{O}_{K_{n+1}}/\mathfrak{a}$ dans $\mathscr{O}_{K_n}/\mathfrak{a}$ ainsi défini est surjectif.*

Démonstration. — Soient ω_{n+1} une uniformisante de K_{n+1} et soit $\omega_n = \mathrm{N}_{K_{n+1}/K_n}(\omega_{n+1})$; c'est une uniformisante de K_n. D'après le lemme précédent, on a $\omega_{n+1}^p = \omega_n$ dans $\mathscr{O}_{K_{n+1}}/\mathfrak{a}$. Tout élément de x de $\mathscr{O}_{K_{n+1}}$ peut s'écrire de manière unique sous la forme $x = \sum_{k=0}^{+\infty} \omega_{n+1}^k [a_k]$, où les a_k sont des éléments de $k_{F'}$ et $[a_k] \in \mathscr{O}_{F'}$ est le représentant de Teichmüller de a_k, et on a $x^p = \sum_{k=0}^{+\infty} \omega_n^k [a_k^p]$ modulo p et donc, *a fortiori*, modulo $\mathfrak{a}$. On en déduit l'appartenance de x^p à $\mathscr{O}_{K_n}/\mathfrak{a}$ et, utilisant le fait que $k_{F'}$ est parfait, la surjectivité de $x \mapsto x^p$.

Si K est une extension finie de F, soit

$$\mathbf{E}_K^+ = \{(x_n)_{n \in \mathbf{N}} \in \widetilde{\mathbf{E}}^+,\ x_n \in \mathscr{O}_{K_n}/\mathfrak{a} \text{ si } n \geqslant n_0(K) + 1\}.$$

Ceci fait de $\mathbf{E}_K^+$ un sous-anneau de $\widetilde{\mathbf{E}}^+$ contenant ε et $\overline{\pi}$, ce qui nous permet de définir le sous-anneau $\mathbf{E}_K = \mathbf{E}_K^+[\overline{\pi}^{-1}]$ de $\widetilde{\mathbf{E}}$.

Proposition 2.12. — (i) *Si F est une extension finie non ramifiée de $\mathbf{Q}_p$, alors $\mathbf{E}_F^+ = k_F[[\overline{\pi}]]$ et $\mathbf{E}_F = k_F((\overline{\pi}))$.*

(ii) *Plus généralement, si K est une extension finie de $\mathbf{Q}_p$, alors $\mathbf{E}_K$ est un corps complet pour la valuation discrète $v_{\mathbf{E}}$, d'anneau des entiers $\mathbf{E}_K^+$, et de corps résiduel $k_{F'}$. De plus, si $\overline{\pi}_K = (\overline{\pi}_{K,n})_{n \in \mathbf{N}}$ est une uniformisante de $\mathbf{E}_K^+$, et si $n \geqslant n_0(K) + 1$, alors $\overline{\pi}_{K,n}$ appartient à $\mathscr{O}_{K_n}/\mathfrak{a}$ et tout relèvement $\hat{\pi}_{K,n}$ de $\overline{\pi}_{K,n}$ dans $\mathscr{O}_{K_n}$ est une uniformisante de K_n.*

Démonstration. — Par surjectivité de $x \mapsto x^p$ de $\mathscr{O}_{K_{n+1}}/\mathfrak{a}$ sur $\mathscr{O}_{K_n}/\mathfrak{a}$, on peut trouver une suite $X = (\overline{\omega}_n) \in \mathbf{E}_K^+$, telle que, si $n \geqslant n_0(K) + 1$, $\overline{\omega}_n$ soit l'image d'une uniformisante ω_n de K_n dans $\mathscr{O}_{K_n}/\mathfrak{a}$. Si $i_n = [\frac{e(K_n/F)}{p}]$, on a alors $\mathscr{O}_{K_n}/\mathfrak{a} \cong k_{F'}[X]/X^{i_n}$, et, i_n tendant vers $+\infty$ quand n tend vers $+\infty$, cela montre que $\mathbf{E}_K^+ = \varprojlim \mathscr{O}_{K_n}/\mathfrak{a}$ est isomorphe à $k_{F'}[[X]]$, l'application de $k_{F'}[[X]]$ dans $\mathscr{O}_{K_n}/\mathfrak{a}$ étant donnée par $\sum_{k=0}^{+\infty} a_k X^k \mapsto \sum_{k=0}^{i_n - 1} a_k^{p^{-n}} \overline{\omega}_n^k$. En particulier, si $K = F$, on peut prendre $\omega_n = \varepsilon^{(n)} - 1$, ce qui montre que l'on a $\mathbf{E}_F = k_F((\overline{\pi}))$.

Maintenant, si $\overline{\pi}_K = (\overline{\pi}_{K,n})_{n \in \mathbf{N}}$ est une uniformisante quelconque de $\mathbf{E}_K^+$, on peut écrire $\overline{\pi}_K$ sous la forme $\overline{\pi}_K = \sum_{k=1}^{+\infty} a_k X^k \in k_{F'}[[X]]$, avec $a_1 \neq 0$. Si $n \geqslant n_0(K) + 1$, on a alors $\overline{\pi}_{K,n} = \sum_{k=1}^{+\infty} a_k \overline{\omega}_n^k$, ce qui fait que tout relèvement $\hat{\pi}_{K,n}$ diffère de l'uniformisante $\sum_{k=1}^{+\infty} [a_k] \omega_n^k$

de K_n par un élément de $\mathfrak{a}$, et est une uniformisante de K_n. Ceci termine la démonstration de la proposition.

Remarque 2.13. — On aurait pu, dans la démonstration précédente, remplacer $\mathfrak{a}$ par n'importe quel idéal $\mathfrak{b}$ de $\mathscr{O}_{\mathbf{C}_p}$ contenant $\mathfrak{a}$ et strictement inclus dans $\mathbf{m}_{\mathbf{C}_p}$. On en déduit que, si $\mathfrak{b}$ est un tel idéal,

$$\mathbf{E}_K^+ = \{(x_n)_{n\in\mathbf{N}} \in \mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\mathfrak{b}) = \widetilde{\mathbf{E}}^+,\ x_n \in \mathscr{O}_{K_n}/\mathfrak{b} \text{ si } n \geqslant n_0(K)+1\}.$$

Proposition 2.14. — *Si K est une extension finie de F, alors $\mathbf{E}_K$ est une extension séparable de degré d_{K_∞} de $\mathbf{E}_F$, d'indice d'inertie f_{K_∞} et d'indice de ramification e_{K_∞}. De plus, on a $v_{\mathbf{E}}(\mathfrak{d}_{\mathbf{E}_K/\mathbf{E}_F}) = \lim_{n\to+\infty} p^n v_p(\mathfrak{d}_{K_n/F_n}) \leqslant \frac{1}{p-1}p^{n_0(K)}$.*

Démonstration. — Si $e_{K_\infty}=1$, on a $\mathbf{E}_K = \mathbf{E}_{F'} = k_{F'}((\overline{\pi}))$, et le résultat est évident. Nous supposerons donc dans ce qui suit que $e_{K_\infty}\geqslant 2$. Soit $\overline{\pi}_K = (\overline{\pi}_{K,n})_{n\in\mathbf{N}}$ une uniformisante de $\mathbf{E}_K$ et, si $n\geqslant n_0(K)+1$, soit $\hat{\pi}_{K,n}$ un relèvement de $\overline{\pi}_{K,n}$ dans $\mathscr{O}_{K_n}$. Comme $n\geqslant n_0(K)+1\geqslant n_0(K)$, l'extension K_n/F'_n est totalement ramifiée de degré $e=e_{K_\infty}$; le polynôme minimal P_n de $\hat{\pi}_{K,n}$ sur F'_n est donc un polynôme d'Eisenstein de degré e que l'on peut mettre sous la forme $P_n(X) = X^e + a_{e-1,n}X^{e-1}+\cdots+a_{0,n}$. Soit S l'ensemble des plongements de K_∞ dans $\overline{F}$ au-dessus F'_∞ ; d'après le (iii) du cor. 1.12, c'est aussi l'ensemble des plongements de K_n dans $\overline{F}$ au-dessus F'_n si $n\geqslant n_0(K)$ et on a $P_n(X)=\prod_{\sigma\in S}(X-\sigma(\hat{\pi}_{K,n}))$.

Notons $\overline{a}_{i,n}$ l'image de $a_{i,n}$ dans $\mathscr{O}_{F'_n}/\mathfrak{a}$, et $\overline{P}_n$ le polynôme $X^e+\overline{a}_{e-1,n}X^{e-1}+\cdots+\overline{a}_{0,n}$. On a aussi $\overline{P}_n(X)=\prod_{\sigma\in S}(X-\sigma(\overline{\pi}_{K,n}))$; on en déduit le fait que $a_i=(\overline{a}_{i,n})_{n\geqslant n_0(K)}$ appartient à $\mathbf{E}_{F'}^+$ et $P(X)=X^e+a_{e-1}X^{e-1}+\cdots+a_0=\prod_{\sigma\in S}(X-\sigma(\overline{\pi}_K))\in\mathbf{E}_{F'}^+[X]$. Par ailleurs, comme P_n est un polynôme d'Eisenstein, on a $v_p(a_{0,n})=v_p(\varepsilon^{(n)}-1)$ et donc $v_{\mathbf{E}}(a_0)=v_{\mathbf{E}}(\overline{\pi})$; le polynôme P est donc un polynôme d'Eisenstein, ce qui prouve que c'est le polynôme minimal de $\overline{\pi}_K$ et que $\mathbf{E}_K$ est une extension totalement ramifiée de degré e_{K_∞} de $\mathbf{E}_{F'}$; l'extension $\mathbf{E}_K/\mathbf{E}_F$ est donc une extension d'indice d'inertie $[F':F]=f_{K_\infty}$, d'indice de ramification e_{K_∞} et de degré $f_{K_\infty}e_{K_\infty}=d_{K_\infty}$.

Finalement, on a $v_{\mathbf{E}}(P'(\overline{\pi}_K)) = \lim_{n\to+\infty} p^n v_p(P'_n(\hat{\pi}_{K,n})) = \lim_{n\to+\infty} p^n v_p(\mathfrak{d}_{K_n/F_n})$. On déduit alors de la proposition 1.14 la non nullité de $P'(\overline{\pi}_K)$ qui montre que l'extension $\mathbf{E}_K/\mathbf{E}_F$ est séparable, et l'inégalité $v_{\mathbf{E}}(\mathfrak{d}_{\mathbf{E}_K/\mathbf{E}_F}) = v_{\mathbf{E}}(P'(\overline{\pi}_K)) \leqslant \frac{1}{p-1}p^{n_0(K)}$ que l'on cherchait à établir.

Exercice 13. — Soit $x=(x_n)_{n\in\mathbf{N}}\in\mathbf{E}_K^+$ et, si $n\geqslant n_0(K)+1$, soit $\hat{x}_n\in\mathscr{O}_{K_n}$, un relèvement de x_n.

(i) Montrer que la suite de terme général $\mathrm{N}_{K_{n+k}/K_n}(\hat{x}_{n+k})$ converge dans $\mathscr{O}_{K_n}$ vers un élément $\tilde{x}_n$ qui ne dépend que de x.

(ii) Montrer que, si $n\geqslant n_0(K)+1$, alors $\mathrm{N}_{K_{n+1}/K_n}(\tilde{x}_{n+1})=\tilde{x}_n$.

(iii) On définit $\tilde{x}_n$ pour $n\leqslant n_0(K)$ par la formule $\tilde{x}_n=\mathrm{N}_{K_{n+1}/K_n}(\tilde{x}_{n+1})$. Montrer que $x\mapsto\tilde{x}=(\tilde{x}_n)_{n\in\mathbf{N}}$ induit une bijection de $\mathbf{E}_K^+$ sur la limite projective des $\mathscr{O}_{K_n}$ pour les applications normes (i.e., l'ensemble des suites $(y_n)_{n\in\mathbf{N}}$, vérifiant $y_n\in\mathscr{O}_{K_n}$ et $y_n=\mathrm{N}_{K_{n+1}/K_n}(y_{n+1})$ si $n\in\mathbf{N}$). C'est cette bijection qui vaut le nom de « corps des normes de l'extension K_∞/K » au corps $\mathbf{E}_K$.

2.5. La clôture séparable du corps des normes

Lemme 2.15. — *Si L est une extension galoisienne de K, alors $\mathrm{Gal}(L_\infty/K_\infty)$ agit fidèlement sur $\mathbf{E}_L$.*

Démonstration. — Soit $\overline{\pi}_L = (\overline{\pi}_{L,n})_{n\in\mathbf{N}}$ une uniformisante de $\mathbf{E}_L$. Les conditions suivantes sont équivalentes pour un élément σ de $\mathrm{Gal}(L_\infty/K_\infty)$:

(i) σ agit trivialement sur $\mathbf{E}_L$;

(ii) σ agit trivialement sur le corps résiduel k_{L_∞} de $\mathbf{E}_L$ et sur $\overline{\pi}_L$;

(iii) σ agit trivialement sur $k_{L_n} = k_{L_\infty}$ et sur $\pi_{L,n}$ quel que soit $n \geqslant n_0(K)+1$.

Pour $n \geqslant n_0(K)+1$, un relèvement $\hat{\pi}_{L,n} \in \mathscr{O}_{L_n}$ de $\overline{\pi}_{L,n}$ est une uniformisante de L_n. La condition selon laquelle σ agit trivialement sur $\overline{\pi}_{L,n}$ se traduit aussi par $v_p(\sigma(\hat{\pi}_n) - \hat{\pi}_n) \geqslant \frac{1}{p}$. Par ailleurs, comme $v_p(\mathfrak{d}_{L_n/K_n})$ tend vers 0 quand $n \to +\infty$, il existe N tel que $v_p(\sigma(\hat{\pi}_{L,n}) - \hat{\pi}_{L,n}) \geqslant \frac{1}{p}$ et $\sigma \in \mathrm{Gal}(L_n/K_n)$ impliquent $\sigma(\hat{\pi}_{L,n}) = \hat{\pi}_{L,n}$, si $n \geqslant N$. La discussion précédente montre donc que si σ agit trivialement sur $\mathbf{E}_L$, alors σ agit aussi trivialement sur L_n pour n assez grand et donc $\sigma = 1$, ce qui permet de conclure.

Corollaire 2.16. — *Si L est une extension galoisienne de K, alors $\mathbf{E}_L$ est une extension galoisienne de $\mathbf{E}_K$ dont le groupe de Galois s'identifie canoniquement à* $\mathrm{Gal}(L_\infty/F_\infty)$.

Démonstration. — Si L est une extension galoisienne de K, alors L_∞ est une extension galoisienne de K_∞ de degré $[L_\infty : K_\infty]$. Par ailleurs, d'après la prop. 2.14, $\mathbf{E}_L$ est une extension séparable de $\mathbf{E}_K$ de degré $[L_\infty : K_\infty]$, et le lemme 2.15 montre que

$$|\mathrm{Aut}(\mathbf{E}_L/\mathbf{E}_K)| \geqslant |\mathrm{Gal}(L_\infty/F_\infty)| = [L_\infty : K_\infty] = [\mathbf{E}_L : \mathbf{E}_K],$$

ce qui permet de conclure.

Théorème 2.17. — *Le sous-corps $\mathbf{E} = \cup_{K\subset\overline{F}}\mathbf{E}_K$ est une clôture séparable de $\mathbf{E}_F$ stable par $\mathrm{G}_{\mathbf{Q}_p}$ et, si K est une extension finie de F, alors $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K) = \mathrm{H}_K$; en particulier, $\mathrm{H}_{\mathbf{Q}_p}$ agit continûment sur $\mathbf{E}$ muni de la topologie discrète.*

Démonstration. — Comme $(\mathbf{E}_K)^\sigma = \mathbf{E}_{K^\sigma}$ si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, la seule chose qui ne soit pas une conséquence directe (via la théorie de Galois des extensions infinies) de la proposition précédente est le fait que $\mathbf{E}$ est séparablement clos. Soit donc F une extension finie non ramifiée de $\mathbf{Q}_p$, et soit $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbf{E}_F[X]$ un polynôme séparable ; il s'agit de montrer que P a d racines dans $\mathbf{E}$. Quitte à remplacer $P(X)$ par $\overline{\pi}^{dr}P(\overline{\pi}^{-r}X)$, où $r \in \mathbf{N}$ est assez grand, on peut supposer que les a_i sont des éléments de $\mathbf{E}_F^+$.

Si $a_i = (a_{i,n})_{n\in\mathbf{N}}$, soit $P_n = X^d + \hat{a}_{d-1,n}X^{d-1} + \cdots + \hat{a}_{0,n} \in \mathscr{O}_{F_n}[X]$, où $\hat{a}_{i,n}$ est un relèvement de $a_{i,n}$ dans $\mathscr{O}_{F_n}$ et soit $K^{(n)}$ l'extension de F_n engendrée par les racines $\alpha_{1,n}, \ldots, \alpha_{d,n}$ de P_n. Nous aurons besoin du lemme suivant :

Lemme 2.18. — *Il existe $n(P)$ tel que, si $n \geqslant n(P)$, alors*

(i) P_n est séparable et $v_p(\alpha_{i,n} - \alpha_{j,n}) \leqslant \frac{1}{2(p+1)}$

(ii) $K^{(n+1)}$ contient $K^{(n)}$ et il existe une permutation σ_n de $\{1, \ldots, d\}$ telle que $v_p(\alpha_{i,n} - \alpha^p_{\sigma_n(i),n+1}) > \frac{1}{2(p+1)}$.

Démonstration. — Soit $\Delta = (\Delta_n)_{n\in\mathbf{N}} \in \mathbf{E}_F^+$ le discrimant de P et, si $n \in \mathbf{N}$, soit $\Delta(P_n) \in \mathscr{O}_{F_n}$ le discriminant de P_n ; on a $\Delta \neq 0$ par hypothèse et, par construction, $\Delta(P_n)$ est un relèvement de Δ_n dans $\mathscr{O}_{F_n}$. En particulier, si n est assez grand, on a $v_p(\Delta_n) = p^{-n}v_{\mathbf{E}}(\Delta)$, et il existe $n(P)$ tel que l'on ait $v_p(\Delta(P_n)) = v_p(\Delta_n) \leqslant \frac{1}{2p(p+1)}$ si $n \geqslant n(P)$. On en déduit le (i).

Maintenant, on a $v_p(\hat{a}_{i,n+1}^p - \hat{a}_{i,n}) \geqslant \frac{1}{p}$ quels que soient $0 \leqslant i \leqslant d-1$ et $n \geqslant 1$; on en déduit les inégalités

$$v_p(P_n(\alpha_{i,n+1}^p) - (P_{n+1}(\alpha_{i,n+1}))^p) \geqslant \frac{1}{p} \quad \text{et} \quad v_p(P_n'(\alpha_{i,n+1}^p) - (P_{n+1}'(\alpha_{i,n+1}))^p) \geqslant \frac{1}{p}.$$

Comme on a de plus $P_{n+1}(\alpha_{i,n+1}) = 0$ et $v_p(P_{n+1}'(\alpha_{i,n+1})) \leqslant v_p(\Delta(P_{n+1})) \leqslant \frac{1}{2p(p+1)}$, si $n \geqslant n(P)$, on obtient

$$v_p(P_n(\alpha_{i,n+1}^p)) \geqslant \frac{1}{p} \quad \text{et} \quad v_p(P_n'(\alpha_{i,n+1}^p)) \leqslant \frac{1}{2p(p+1)} < \frac{1}{2}v_p(P_n(\alpha_{i,n+1}^p)).$$

Le lemme de Hensel permet alors de montrer qu'il existe une unique racine $\alpha_{j,n}$ de P_n appartenant à $K^{(n+1)}$ telle que l'on ait $v_p(\alpha_{j,n} - \alpha_{i,n+1}^p) > \frac{1}{2(p+1)}$; on en déduit le lemme.

Revenons à la démonstration du théorème. La réunion $K^{(\infty)}$ des $K^{(n)}$, $n \geqslant n(P)$ est, d'après le (ii) du lemme précédent, une extension de degré au plus $d!$ de F_∞ ; il existe donc une extension finie K de F telle que l'on ait $K^{(n)} \subset K_n$ quel que soit $n \geqslant n(P)$. Quitte à renuméroter les $\alpha_{i,n}$, on peut supposer que toutes les permutations σ_n apparaissant dans le lemme précédent sont l'identité. Maintenant, soit $\mathfrak{b} = \{x \in \mathbf{C}_p,\ v_p(x) \geqslant \frac{1}{2(p+1)}\}$. La suite $(\alpha_{i,n})$ nous définit un élément $\alpha_i = (\alpha_{i,n})_{n\in\mathbf{N}}$ de $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\mathfrak{b})$ appartenant à $\mathbf{E}_K^+$ puisque $\alpha_{i,n} \in K_n$ si n est assez grand, et qui est un zéro de P par construction. Finalement, comme $v_p(\alpha_{i,n} - \alpha_{j,n}) \leqslant \frac{1}{2p(p+1)}$ si $i \neq j$, on a $\alpha_i \neq \alpha_j$ si $i \neq j$, ce qui permet de conclure.

Remarque 2.19. — (i) Le corps $\widetilde{\mathbf{E}}$ étant parfait, il contient la clôture radicielle $\mathbf{E}^{\mathrm{rad}}$ de $\mathbf{E}$ qui est une clôture algébrique de $\mathbf{E}_{\mathbf{Q}_p}$ puisque $\mathbf{E}$ est une clôture séparable de $\mathbf{E}_{\mathbf{Q}_p}$.

(ii) Il contient de même, si K est une extension finie de $\mathbf{Q}_p$, la a clôture radicielle $\mathbf{E}_K^{\mathrm{rad}}$ de $\mathbf{E}_K$. Comme il est de plus complet pour la valuation $v_{\mathbf{E}}$, il contient aussi le complété $\widetilde{\mathbf{E}}_K$ de $\mathbf{E}_K^{\mathrm{rad}}$.

Exercice 14. — Montrer que l'anneau des entiers $\widetilde{\mathbf{E}}_K^+$ de $\widetilde{\mathbf{E}}_K$ est le sous ensemble de $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\mathfrak{a})$ des suites $x = (x_n)_{n\in\mathbf{N}}$ vérifiant $x_n \in \mathscr{O}_{K_\infty}/\mathfrak{a}$ quel que soit $n \in \mathbf{N}$.

Lemme 2.20. — (i) $\mathbf{E}^{\mathrm{rad}}$ *est dense dans* $\widetilde{\mathbf{E}}$.

(ii) $\mathbf{E}$ *est dense dans* $\widetilde{\mathbf{E}}$.

Démonstration. — Soit $x = (x_n)_{n\in\mathbf{N}} \in \widetilde{\mathbf{E}}^+ = \mathbb{R}(\mathscr{O}_C/\mathfrak{a})$. Si $m \in \mathbf{N}$, il existe K, extension finie de F, telle que $x_m \in \mathscr{O}_K/\mathfrak{a}$. D'après le lemme 2.11, il existe alors $y = (y_n)_{n\geqslant n(K)}$ appartenant à $\mathbf{E}_K^+$ (identifié à la limite projective des $\mathscr{O}_{K_n}/\mathfrak{a}$) tel que l'on ait $y_{n_0(K)+1} = x_m$. Soit alors $z = y^{p^{m-n_0(K)-1}}$; c'est un élément de $\mathbf{E}_K^{\mathrm{rad}}$ et on a $z_m = x_m$ et donc $v_{\mathbf{E}}(x-z) \geqslant p^m v_p(\mathfrak{a}) = p^{m-1}$, ce qui permet de démontrer le (i).

Pour démontrer le (ii), il suffit, compte tenu du (i), de montrer que l'on peut approcher tout élément de $\mathbf{E}^{\mathrm{rad}}$ par des éléments de $\mathbf{E}$. Soit donc $x \in \mathbf{E}^{\mathrm{rad}}$; il existe $r \in \mathbf{N}$ tel que $x^{p^r} \in \mathbf{E}$. Soit $\pi \in \mathbf{E}^+$ vérifiant $v_{\mathbf{E}}(\pi) > 0$ et, si $n \in \mathbf{N}$, soit x_n une solution de l'équation $X^{p^r} - \pi^{np^r}X = x^{p^r}$. Le polynôme $X^{p^r} - \pi^{np^r}X - x^{p^r}$ étant à coefficients dans $\mathbf{E}$ et séparable, et $\mathbf{E}$ étant séparablement clos, on a $x_n \in \mathbf{E}$. D'autre part, si n est assez grand, la théorie des polygones de Newton montre que l'on a $v_{\mathbf{E}}(x_n) = v_{\mathbf{E}}(x)$ et l'égalité $(x_n - x)^{p^r} = \pi^{np^r}x_n$ montre que l'on a $v_{\mathbf{E}}(x - x_n) = nv_{\mathbf{E}}(\pi) + \frac{1}{p^r}v_{\mathbf{E}}(x)$ et donc que $v_{\mathbf{E}}(x - x_n)$ tend vers $+\infty$ quand n tend vers $+\infty$. Ceci permet de conclure.

Théorème 2.21. — (i) $\widetilde{\mathbf{E}}$ *est algébriquement clos.*

(ii) *Si K est une extension finie de F, alors $\widetilde{\mathbf{E}}^{\mathrm{H}_K} = \widetilde{\mathbf{E}}_K$.*

Démonstration. — $\widetilde{\mathbf{E}}$ est un corps complet contenant $\mathbf{E}^{\mathrm{rad}}$ comme sous-corps dense ; c'est donc le complété de $\mathbf{E}^{\mathrm{rad}}$ qui est un corps algébriquement clos ; il en est donc de même de $\widetilde{\mathbf{E}}$. Maintenant, d'après le théorème d'Ax-Sen-Tate, $\widetilde{\mathbf{E}}^{\mathrm{H}_K}$ est le complété du sous-corps de $\mathbf{E}^{\mathrm{rad}}$ fixe par H_K. Comme $\mathbf{E}$ est séparablement clos et $\mathbf{E}^{\mathrm{H}_K} = \mathbf{E}_K$, le sous-corps de $\mathbf{E}^{\mathrm{rad}}$ fixe par H_K est la clôture radicielle de $\mathbf{E}_K$ et son complété est $\widetilde{\mathbf{E}}_K$ par définition, ce qui permet de conclure.

Exercice 15. — (i) Montrer que, si K est une extension finie de $\mathbf{Q}_p$, alors $\mathbf{E}_K$ est une extension radicielle de degré p de $\varphi(\mathbf{E}_K)$ et $1, \varepsilon, \ldots, \varepsilon^{p-1}$ est une base de $\mathbf{E}_K$ sur $\varphi(\mathbf{E}_K)$. (On commencera par supposer $K/\mathbf{Q}_p$ non ramifiée.)

(ii) Montrer que $\mathbf{E}$ est une extension radicielle de degré p de $\varphi(\mathbf{E})$ et $1, \varepsilon, \ldots, \varepsilon^{p-1}$ est une base de $\mathbf{E}$ sur $\varphi(\mathbf{E})$.

(iii) On définit $\psi : \mathbf{E} \to \mathbf{E}$ par la formule

$$\psi(\varphi(a_0) + \varphi(a_1)\varepsilon + \cdots + \varphi(a_{p-1})\varepsilon^{p-1}) = a_0.$$

Montrer que ψ est un inverse à gauche de φ (i.e. $\psi \circ \varphi = \mathrm{id}$) qui commute à l'action de G_F, et que, si K est une extension finie de F, alors $\psi(\mathbf{E}_K) \subset \mathbf{E}_K$.

2.6. L'anneau A et les (φ, Γ)-modules

Soit $\widetilde{\mathbf{A}}$ l'anneau des vecteurs de Witt à coefficients dans $\widetilde{\mathbf{E}}$. On munit $\widetilde{\mathbf{A}}$ de la topologie faible faisant de $\sum_{n=0}^{+\infty} p^n[x_n] \mapsto (x_n)_{n\in\mathbf{N}}$ un homéomorphisme de $\widetilde{\mathbf{A}}$ sur $(\widetilde{\mathbf{E}})^{\mathbf{N}}$. L'action naturelle de φ et $\mathrm{G}_{\mathbf{Q}_p}$ est alors continue pour cette topologie.

Soit $\pi = [\varepsilon] - 1$. L'adhérence $\mathbf{A}_{\mathbf{Q}_p}$ de $\mathbf{Z}_p[\pi, \pi^{-1}]$ dans $\widetilde{\mathbf{A}}$ est isomorphe à l'anneau des entiers de $\mathbf{Q}_p\{\{T\}\}$, l'isomorphisme envoyant T sur π, et $\mathbf{A}_{\mathbf{Q}_p}$ est stable par φ et $\mathrm{G}_{\mathbf{Q}_p}$ agissant à travers $\Gamma_{\mathbf{Q}_p}$, et on a

$$\varphi(\pi) = (1+\pi)^p - 1 \quad \text{et} \quad \sigma(\pi) = (1+\pi)^{\chi(\sigma)} - 1, \text{ si } \sigma \in \Gamma_{\mathbf{Q}_p}.$$

L'anneau $\mathbf{A}_{\mathbf{Q}_p}$ est un p-anneau strict d'anneau résiduel $\mathbf{E}_{\mathbf{Q}_p}$.

On note $\mathbf{A}$ l'adhérence, pour la topologie p-adique, de l'anneau des entiers de l'extension maximale non ramifiée de $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[\frac{1}{p}]$ dans $\widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}[\frac{1}{p}]$. Cet anneau vérifie les propriétés suivantes.

- $\mathbf{A}$ est un p-anneau strict d'anneau résiduel $\mathbf{E}$.
- $\mathbf{A}$ est stable par φ et $\mathrm{G}_{\mathbf{Q}_p}$.
- Si K est une extension finie de $\mathbf{Q}_p$, alors $\mathbf{A}_K = \mathbf{A}^{\mathrm{H}_K}$ est un p-anneau strict d'anneau résiduel $\mathbf{E}_K$.

Exercice 16. — (i) Démontrer toutes les affirmations ci-dessus concernant la construction de $\mathbf{A}$ et ses propriétés.

(ii) Démontrer, en utilisant les propriétés de $\mathbf{A}$ énoncées ci-dessus, que $\varphi - 1 : \mathbf{A} \to \mathbf{A}$ est surjective, et que $\mathbf{A}^{\varphi=1} = \mathbf{Z}_p$.

Si K est une extension finie de $\mathbf{Q}_p$, et si V est un $\mathbf{Z}_p$-module libre de rang d muni d'une action continue de G_K, on pose $\mathbf{D}(V) = (\mathbf{A} \otimes_{\mathbf{Z}_p} V)^{\mathrm{H}_K}$, où l'on a muni $\mathbf{A} \otimes_{\mathbf{Z}_p} V$ de l'action diagonale de G_K. Comme on n'a pris que les invariants sous l'action de H_K, on récupère un module sur

$\mathbf{A}^{\mathrm{H}_K} = \mathbf{A}_K$ muni d'une action résiduelle de Γ_K. Par ailleurs, on peut munir $\mathbf{A} \otimes_{\mathbf{Z}_p} V$ de l'action de $\varphi \otimes \mathrm{id}$, et comme cette action commute à celle de G_K, cela muni $\mathbf{D}(V)$ d'une action de φ commutant à celle de Γ_K. En résumé, $\mathbf{D}(V)$ est *un* (φ, Γ)*-module sur* $\mathbf{A}_K$.

Le résultat suivant est le point de départ de la classification, découverte par Fontaine, des représentations p-adiques de G_K en termes de (φ, Γ)-modules.

Théorème 2.22. — *Si V est comme ci-dessus, alors $\mathbf{D}(V)$ est un $\mathbf{A}_K$-module libre de rang d, et $V = (\mathbf{A} \otimes_{\mathbf{A}_K} \mathbf{D}(V))^{\varphi=1}$ en tant que représentation de G_K, où l'on a muni $\mathbf{A} \otimes_{\mathbf{A}_K} \mathbf{D}(V)$ de l'action diagonale de G_K, G_K agissant à travers Γ_K sur $\mathbf{D}(V)$, et de l'action diagonale de φ.*

L'intérêt de cette classification est que, Γ_K étant procyclique (au moins si $p \geqslant 3$), un (φ, Γ)-module D est complètement décrit par l'action de φ et celle d'un générateur γ de Γ_K. Si $e_1, \dots, e_d$ est une base de D sur $\mathbf{A}_K$, on peut considérer la matrice A (resp. B) de $(\varphi(e_1), \dots \varphi(e_d))$ (resp. de $(\gamma(e_1), \dots \gamma(e_d))$) dans la base $e_1, \dots, e_d$. Alors A et B sont deux éléments de $\mathbf{GL}_d(\mathbf{A}_K)$ vérifiant la relation $A\varphi(B) = B\varphi(A)$ traduisant le fait que φ et γ commutent, mais que les actions de φ et γ sur $\mathbf{A}_K$ ne sont pas triviales. On est donc ramené à étudier les couples (A, B) d'éléments de $\mathbf{GL}_d(\mathbf{A}_K)$ vérifiant les conditions ci-dessus, ce qui est plus simple, *a priori*, que de décrire une représentation de G_K. De fait, cette classification des représentations p-adiques de G_K en termes de (φ, Γ)-modules est l'un des outils les plus puissants dont on dispose à l'heure actuelle pour l'étude des représentations p-adiques de G_K et de $\mathrm{G}_{\mathbf{Q}}$.

Pierre Colmez