REPRÉSENTATIONS GALOISIENNES ET (φ, Γ)-MODULES, NOTES DU COURS DE M2

par

Pierre Colmez

Table des matières

1. Anneaux de Fontaine

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

1.1.1. L'extension cyclotomique d'une extension non ramifiée de $\mathbf{Q}_p$. — Soient F un corps de caractéristique $\neq p$, $\overline{F}$ une clôture algébrique de F, et $\mathrm{G}_F = \mathrm{Aut}(\overline{F}/F)$. 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.*

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 $F_n = \mathbf{Q}_p(\varepsilon^{(n)})$, 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 $\mathbf{Q}_p$, 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* $\mathrm{Gal}(F_n/\mathbf{Q}_p)$ *sur* $(\mathbf{Z}/p^n\mathbf{Z})^*$.

(iii) *F_∞ est une extension galoisienne de $\mathbf{Q}_p$, et χ induit un isomorphisme de $\Gamma_{\mathbf{Q}_p} =$* $\mathrm{Gal}(F_\infty/\mathbf{Q}_p)$ *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 $\mathbf{Q}_p$. 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 $\mathbf{Q}_p$. De plus, $\mathrm{Gal}(F_n/\mathbf{Q}_p)$ 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.

1.1.2. 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 $\Gamma_{\mathbf{Q}_p}$ sur F_∞ s'étend par continuité à $\widehat{F}_\infty$, et l'objet de ce n° est d'étudier cette action.

Lemme 1.2. — *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.

Proposition 1.3. — (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 $k \in \mathbf{Z}$, alors « $v_p(x) \geqslant kv_p(\pi_n)$ » $\Leftrightarrow$ « $v_p(\mathrm{R}_n(x)) \geqslant kv_p(\pi_n)$ ».*

(iii) R_n *s'étend par continuité à* $\widehat{F}_\infty$, *et on a* $v_p(\mathrm{R}_n(x)) > v_p(x) - v_p(\pi_n)$.

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.

Dans le (ii), 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

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

On en déduit la formule $\mathrm{R}_n(x)$. Ceci permet de montrer que, si $v_p(x) \geqslant 0$, alors $v_p(\mathrm{R}_n(x)) \geqslant 0$. 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.

Par ailleurs, d'après le (ii), on a $v_p(\mathrm{R}_n(x)) > v_p(x) - v_p(\pi_n)$, si $x \in F_\infty$, ce qui prouve que l'application F_n-linéaire R_n est uniformément continue, et donc s'étend par continuité à $\widehat{F}_\infty$ en une application vérifiant encore $v_p(\mathrm{R}_n(x)) > v_p(x) - v_p(\pi_n)$, pour tout $x \in \widehat{F}_\infty$.

Remarque 1.4. — (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. 1.3, 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 $x \in \widehat{F}_\infty$.

1.1.3. L'extension cyclotomique d'une extension finie de $\mathbf{Q}_p$. — Soit K une extension finie de $\mathbf{Q}_p$. 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 $\Gamma_K = \mathrm{G}_K/\mathrm{H}_K$.

On note $\mathrm{G}_{\mathbf{Q}_p}$ le groupe de galois absolu $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ de $\mathbf{Q}_p$. Ce groupe admet une filtration par les *sous-groupes de ramification* $\mathrm{G}_{\mathbf{Q}_p}^t$, pour $t \geqslant -1$. Ces sous-groupes sont distingués dans $\mathrm{G}_{\mathbf{Q}_p}$ et vérifient les propriétés suivantes :

- $\mathrm{G}_{\mathbf{Q}_p}^s \subset \mathrm{G}_{\mathbf{Q}_p}^t$, si $s \geqslant t$ (la filtration est décroissante).
- $\mathrm{G}_{\mathbf{Q}_p}^t = \mathrm{G}_{\mathbf{Q}_p}$, si $t = -1$.
- $\mathrm{G}_{\mathbf{Q}_p}^t$ est le sous-groupe d'inertie de $\mathrm{G}_{\mathbf{Q}_p}$, si $t \in]-1, 0]$.
- Le sous-groupe d'inertie sauvage de $\mathrm{G}_{\mathbf{Q}_p}$ est la réunion des $\mathrm{G}_{\mathbf{Q}_p}^t$, pour $t > 0$.

Si $s \geqslant 0$, on note $\overline{\mathbf{Q}}_p^{(s)}$ l'intersection des $\overline{\mathbf{Q}}_p^{\mathrm{G}_{\mathbf{Q}_p}^t}$, pour $t > s-1$. Si $K \subset \overline{\mathbf{Q}}_p$ est une extension de $\mathbf{Q}_p$, on note $K^{(s)}$ le sous-corps $K \cap \overline{\mathbf{Q}}_p^{(s)}$ de K.

• $\overline{\mathbf{Q}}_p^{(0)}$ est l'extension maximale non ramifiée $\mathbf{Q}_p^{\mathrm{nr}}$ de $\mathbf{Q}_p$; si $[K:\mathbf{Q}_p]<+\infty$, alors $K^{(0)}$ est de la forme $\mathbf{Q}_p(\boldsymbol{\mu}_{p^n-1})$, où $n=[K^{(0)}:\mathbf{Q}_p]$.

• $K^{(1)}$ est l'extension maximale modérément ramifiée de $\mathbf{Q}_p$ contenue dans K ; si $[K:\mathbf{Q}_p]<+\infty$, alors $K^{(1)}$ est de la forme $K^{(0)}(\pi^{1/e})$, où $e=[K^{(1)}:K^{(0)}]$ et $\pi\in K^{(0)}$ vérifie $v_p(\pi)=1$.

Les groupes de ramification sont reliés à la différente. On rappelle que si $K\subset L$ sont deux extensions finies de $\mathbf{Q}_p$, l'ensemble des $y\in L$ tels que $\mathrm{Tr}_{L/K}yz\in\mathscr{O}_K$, pour tout $z\in\mathscr{O}_K$, est un idéal fractionnaire de L dont l'inverse $\mathfrak{d}_{L/K}$ est appelé la *différente* de L sur K ; cet idéal est déterminé par sa valuation p-adique (i.e. la valuation de n'importe quel générateur). Les principales propriétés de la différentes sont résumées dans la proposition suivante.

Proposition 1.5. — (i) *Il existe $x\in\mathscr{O}_L$ tel que $\mathscr{O}_L=\mathscr{O}_K[x]$, et si $P\in K[X]$ est le polynôme minimal de x, alors $v_p(\mathfrak{d}_{L/K})=v_p(P'(x))$.*
(ii) $v_p(\mathfrak{d}_{L/K})=v_p(\mathfrak{d}_{L/\mathbf{Q}_p})-v_p(\mathfrak{d}_{K/\mathbf{Q}_p})$.
(iii) $v_p(\mathfrak{d}_{K/\mathbf{Q}_p})=\int_0^{+\infty}\big(1-\frac{1}{[K_n:K_n^{(s)}]}\big)\,ds$.

Exemple 1.6. — (i) $\mathscr{O}_{F_n}=\mathbf{Z}_p[\varepsilon^{(n)}]$, le polynôme minimal de $\varepsilon^{(n)}$ est $P_n(X)=\frac{X^{p^n}-1}{X^{p^{n-1}}-1}$, et on a $P_n'(\varepsilon^{(n)})=p^n\frac{(\varepsilon^{(n)})^{p^n-1}}{\varepsilon^{(1)}-1}$. On en déduit que $v_p(\mathfrak{d}_{F_n/\mathbf{Q}_p})=n-\frac{1}{p-1}$.
(ii) En utilisant le (iii) de la formule précédente, combiné avec la théorie de Galois pour déterminer les sous-corps de F_n, on en déduit que $F_n^{(s)}=F_{[s]}$, si $s\leqslant n$ et $F_n^{(s)}=F_n$, si $s\geqslant n$.

Proposition 1.7. — *La suite $(p^nv_p(\mathfrak{d}_{K_n/F_n}))_{n\in\mathbf{N}}$ est bornée ; en particulier $v_p(\mathfrak{d}_{K_n/F_n})\to 0$.*

Démonstration. — On part des formules

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

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

$$p^nv_p(\mathfrak{d}_{K_n/F_n})=\frac{p}{p-1}\int_0^{+\infty}[F_n^{(s)}:\mathbf{Q}_p]\Big(1-\frac{1}{[K_n:F_nK_n^{(s)}]}\Big)\,ds.$$

Maintenant, il existe $n(K)$ tel que $K_n^{(s)}\supset K^{(s)}=K$ et donc $[K_n:F_nK_n^{(s)}]=1$, si $s\geqslant n(K)$, ce qui nous fournit la formule

$$p^nv_p(\mathfrak{d}_{K_n/F_n})=\frac{p}{p-1}\int_0^{n(K)}[F_n^{(s)}:\mathbf{Q}_p]\Big(1-\frac{1}{[K_n:F_nK_n^{(s)}]}\Big)\,ds.$$

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

$$\int_0^{n(K)}[F_n^{(s)}:\mathbf{Q}_p]\,ds=\int_0^{n(K)}[F_{[s]}:\mathbf{Q}_p]\,ds=1+(p-1)+\cdots+(p-1)p^{n(K)-2}=p^{n(K)-1}.$$

1.2. Anneaux de caractéristique p

1.2.1. 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 $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p)$ ou, plus généralement, comme $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\varpi)$, pour n'importe que choix de $\varpi \in \mathscr{O}_{\mathbf{C}_p}$ vérifiant $0 < v_p(\varpi) \leqslant 1$. On note $(x_n)_{n\in\mathbf{N}}$ l'écriture de $x = (x^{(n)})_{n\in\mathbf{N}}$ comme élément de $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/p)$; autrement dit, $x^{(n)}$ est la réduction modulo p de $x^{(n)}$. On remarquera que $\overline{\mathbf{F}}_p$ étant un sous-anneau parfait de $\mathscr{O}_{\mathbf{C}_p}/\varpi$, 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 $v_{\mathbf{E}}(x) = p^n v_p(x^{(n)})$ quel que soit $n \in \mathbf{N}$, et que $v_{\mathbf{E}}(x) = p^n v_p(x_n)$, pour tout n assez grand, si $x \neq 0$.

Finalement, si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, 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 1.8. — (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 $\mathrm{G}_{\mathbf{Q}_p}$ 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 $\mathrm{G}_{\mathbf{Q}_p}$ 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 $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$, on a $v_{\mathbf{E}}(\sigma(x)) = v_{\mathbf{E}}(x)$ ce qui fait que $\mathrm{G}_{\mathbf{Q}_p}$ 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 $\sigma\in\mathrm{G}_{\mathbf{Q}_p}$ 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 1.9. — (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, $\mathbb{R}(k_K)\cong k_K$.

1.2.2. Les éléments ε et $\overline{\pi}$, le corps $\widetilde{\mathbf{E}}$. — Soit $\varepsilon=(1,\varepsilon^{(1)},\dots,\varepsilon^{(n)},\dots)\in\widetilde{\mathbf{E}}^+$, 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

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

Proposition 1.10. — *Si $\sigma\in\mathrm{G}_{\mathbf{Q}_p}$, alors $\sigma(\varepsilon)=\varepsilon^{\chi(\sigma)}$, où χ est le caractère cyclotomique.*

Démonstration. — 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 $\widetilde{\mathbf{E}}$.

Remarque 1.11. — Comme $v_{\mathbf{E}}(\varphi(x))=pv_{\mathbf{E}}(x)$, on peut caractériser $\widetilde{\mathbf{E}}^+$ (resp. l'idéal maximal $\widetilde{\mathbf{E}}^{++}$ de $\widetilde{\mathbf{E}}$) comme l'ensemble des $x\in\widetilde{\mathbf{E}}$ tels que la suite $(\varphi^n(x))_{n\in\mathbf{N}}$ soit bornée (resp. tende vers 0) dans $\widetilde{\mathbf{E}}$.

Théorème 1.12. — $\widetilde{\mathbf{E}}=\widetilde{\mathbf{E}}^+[\overline{\pi}^{-1}]$ *est algébriquement clos.*

Démonstration. — Comme $\widetilde{\mathbf{E}}$ est parfait, il suffit de prouver qu'il est séparablement clos. Soit $P=X^d+a_{d-1}X^{d-1}+\cdots+a_0\in\widetilde{\mathbf{E}}[X]$ un polynôme séparable ; il s'agit de montrer que P a d racines dans $\widetilde{\mathbf{E}}$. 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 $\widetilde{\mathbf{E}}^+$.

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

Lemme 1.13. — *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) *il existe une permutation σ_n de $\{1,\dots,d\}$ telle que* $v_p(\alpha_{i,n}-\alpha^p_{\sigma_n(i),n+1})>\frac{1}{2(p+1)}$.

Démonstration. — Soit $\Delta=(\Delta_n)_{n\in\mathbf{N}}\in\widetilde{\mathbf{E}}^+$ le discrimant de P et, si $n\in\mathbf{N}$, soit $\Delta(P_n)\in\mathscr{O}_{\mathbf{C}_p}$ 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 $\mathscr{O}_{\mathbf{C}_p}$. 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 $v_p(\Delta(P_n))=v_p(\Delta_n)\leqslant\frac{1}{2(p+1)}$ si $n\geqslant n(P)$. On en déduit le (i).

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

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

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

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

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

Revenons à la démonstration du théorème. 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 $\mathbb{R}(\mathscr{O}_{\mathbf{C}_p}/\mathfrak{b})$ qui est un zéro de P par construction. Enfin, comme $v_p(\alpha_{i,n}-\alpha_{j,n})\leqslant\frac{1}{2(p+1)}$ si $i\neq j$, on a $\alpha_i\neq\alpha_j$ si $i\neq j$, ce qui permet de conclure.

Proposition 1.14. — $\widetilde{\mathbf{E}}^{\mathrm{H}_{\mathbf{Q}_p}}=\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$.

Démonstration. — Comme $\overline{\pi}$ est fixe par $\mathrm{H}_{\mathbf{Q}_p}$, il suffit de démontrer que $(\widetilde{\mathbf{E}}^+)^{\mathrm{H}_{\mathbf{Q}_p}}=\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^+$, et l'inclusion $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^+\subset(\widetilde{\mathbf{E}}^+)^{\mathrm{H}_{\mathbf{Q}_p}}$ étant immédiate, il suffit de prouver l'autre inclusion. Soit donc $x=(x_n)_{n\in\mathbf{N}}=(x^{(n)})_{n\in\mathbf{N}}$ appartenant à $(\widetilde{\mathbf{E}}^+)^{\mathrm{H}_{\mathbf{Q}_p}}$. Alors $x^{(n)}$ est fixe par $\mathrm{H}_{\mathbf{Q}_p}$, pour tout $n\in\mathbf{N}$, et il résulte du th. d'Ax-Sen-Tate que $x^{(n)}\in\mathscr{O}_{\widehat{F}_\infty}$. On peut donc écrire x_n sous la forme $\sum_{i=0}^{(p-1)p^{k_n}-1}a_{i,n}\pi_{k_n}^i$, où les $a_{i,n}$ sont des éléments de $\mathbf{F}_p$, ce qui permet d'associer à x la suite des $\tilde{x}_n=\sum_{i=0}^{(p-1)p^{k_n}-1}a_{i,n}\overline{\pi}^{p^{n-k_n}}\in\varphi^{-n}(\mathbf{E}_{\mathbf{Q}_p}^+)\subset\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^+$. Par ailleurs la condition $x_{n+1}^p=x_n$ se traduit par la congruence $\tilde{x}_{n+1}\equiv\tilde{x}_n\bmod\overline{\pi}^{(p-1)p^{n-1}}$; on en déduit que $x\mapsto(\tilde{x}_n)_{n\in\mathbf{N}}$ est un isomorphisme de $(\widetilde{\mathbf{E}}^+)^{\mathrm{H}_{\mathbf{Q}_p}}$ sur $\varprojlim\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^+/\overline{\pi}^{(p-1)p^{n-1}}$, et comme cette limite projective n'est autre que $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^+$, par définition de $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}^+$, cela permet de conclure.

1.2.3. Le corps $\mathbf{E}$. — Soit $\mathbf{E}$ la clôture séparable de $\mathbf{E}_{\mathbf{Q}_p}$ dans $\widetilde{\mathbf{E}}$.

Théorème 1.15. — (i) $\mathbf{E}$ *est dense dans* $\widetilde{\mathbf{E}}$ (et donc $\widetilde{\mathbf{E}}$ est le complété de $\mathbf{E}$ pour $v_{\mathbf{E}}$).

(ii) $\mathbf{E}$ *est stable par* $\mathrm{G}_{\mathbf{Q}_p}$ *et* $\mathrm{H}_{\mathbf{Q}_p}$ *s'identifie à* $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$.

Démonstration. — Comme $\mathbf{E}$ est dense dans $\mathbf{E}^{\mathrm{rad}}$, il suffit de prouver que $\mathbf{E}^{\mathrm{rad}}$ est dense dans $\widetilde{\mathbf{E}}$, et il suffit de prouver le même énoncé pour les anneaux d'entiers. On est ramené à prouver que si $x=(x_n)_{n\in\mathbf{N}}\in\widetilde{\mathbf{E}}^+$ et si $N\in\mathbf{N}$, il existe $y=(y_n)_{n\in\mathbf{N}}\in(\mathbf{E}^{\mathrm{rad}})^+$ tel que $v_{\mathbf{E}}(x-y)\geqslant p^N$, et quitte à remplacer x et y par $x^{p^{-N-1}}$ et $y^{p^{-N-1}}$, il suffit de prouver que l'on peut trouver $y\in(\mathbf{E}^{\mathrm{rad}})^+$ tel que $v_p(x_0-y_0)\geqslant\frac{1}{p}$.

Soit K une extension finie de $\mathbf{Q}_p$ telle que $x_0 \in \mathscr{O}_K/p$, soit n assez grand pour que $v_p(\mathfrak{d}_{K_n/F_n}) < \frac{1}{p}$, et soit ω tel que $\mathscr{O}_{K_n} = \mathbf{Z}_p[\omega]$, et donc $x_0 = Q(\omega)$, avec $Q \in \mathbf{F}_p[X]$. On note P_n le polynôme minimal de ω sur F_n ; on a $v_p(P'_n(\omega)) = v_p(\mathfrak{d}_{K_n/F_n}) < \frac{1}{p}$. On écrit $P_n(X)$ sous la forme

$$P_n(X) = X^d + A_{d-1}(\pi_n)X^{d-1} + \cdots + A_0(\pi_n), \quad \text{avec } A_{d-1}, \dots, A_0 \in \mathbf{Z}_p[X],$$

et on définit $P(X) \in \mathbf{E}^+_{\mathbf{Q}_p}[X]$ par $P(X) = X^d + A_{d-1}(\overline{\pi})X^{d-1} + \cdots + A_0(\overline{\pi})$. Le polynôme P est séparable car si $u = (u_n)_{n\in\mathbf{N}} \in \widetilde{\mathbf{E}}^+$ est une racine de P, alors $v_p(P_n(\hat{u}_n)) \geqslant 1$, et la condition $v_p(P_n(\omega)) < \frac{1}{p}$ implique qu'il existe un conjugué de ω vérifiant $v_p(\sigma(\omega) - \hat{u}_n) > 1 - \frac{1}{p}$ (factoriser P_n) ; on a alors $v_p(P'_n(\hat{u}_n)) = v_p(P'_n(\omega_n)) < 1$, et donc $P'(u) \neq 0$. On déduit de ce qui précède que $u \in \mathbf{E}^+$ et que, quitte à remplacer u par un conjugué, $v_p(u_n - \omega) > 1 - \frac{1}{p}$. On a alors $v_p(Q(u_n) - x_0) > 1 - \frac{1}{p}$, ce qui prouve que l'on peut prendre $y = Q(u)^{p^{-n}}$ qui est aussi égal à $Q(u^{p^{-n}})$. Ceci démontre le (i).

Maintenant, $\mathbf{E}_{\mathbf{Q}_p}$ est stable par $\mathrm{G}_{\mathbf{Q}_p}$ et fixe par $\mathrm{H}_{\mathbf{Q}_p}$; il en résulte que $\mathbf{E}$ est stable par $\mathrm{G}_{\mathbf{Q}_p}$ et que l'action de $\mathrm{G}_{\mathbf{Q}_p}$ sur $\mathbf{E}$ induit un morphisme de groupes de $\mathrm{H}_{\mathbf{Q}_p}$ dans $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$. Ce morphisme est injectif car un élément du noyau agit trivialement sur $\widetilde{\mathbf{E}}$ par densité de $\mathbf{E}$ dans $\widetilde{\mathbf{E}}$, et donc aussi sur $\mathbf{C}_p$ qui contient $\overline{\mathbf{Q}}_p$. Par ailleurs, l'image de $\mathrm{H}_{\mathbf{Q}_p}$ est fermée dans $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$ puisque $\mathrm{H}_{\mathbf{Q}_p}$ est compact. Il résulte donc du théorème d'Ax-Sen-Tate que $\widetilde{\mathbf{E}}^{\mathrm{H}_{\mathbf{Q}_p}}$ est le complété de la clôture radicielle de $\mathbf{E}^{\mathrm{H}_{\mathbf{Q}_p}}$, et comme on a vérifié que $\widetilde{\mathbf{E}}^{\mathrm{H}_{\mathbf{Q}_p}}$ est le complété $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ de la clôture radicielle de $\mathbf{E}_{\mathbf{Q}_p}$, on a $\mathbf{E}^{\mathrm{H}_{\mathbf{Q}_p}} = \mathbf{E}_{\mathbf{Q}_p}$, et on déduit de la correspondance de Galois que $\mathrm{H}_{\mathbf{Q}_p} = \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p})$. Ceci permet de conclure.

Remarque 1.16. — On a $\mathrm{G}_{\mathbf{Q}_p}/\mathrm{H}_{\mathbf{Q}_p} = \Gamma \cong \mathbf{Z}_p^*$, ce qui fournit un lien très étroit entre le groupe de Galois absolu du corps local $\mathbf{Q}_p$ qui est de caractéristique 0 et celui de $\mathbf{E}_{\mathbf{Q}_p}$ qui est de caractéristique p.

Si $[K : \mathbf{Q}_p] < +\infty$, on pose $\mathbf{E}_K = \mathbf{E}^{\mathrm{H}_K}$ et $\widetilde{\mathbf{E}}_K = \widetilde{\mathbf{E}}^{\mathrm{H}_K}$. Si $K = \mathbf{Q}_p$, on retombe sur les objets précédemment définis (par construction pour $\mathbf{E}_{\mathbf{Q}_p}$ et d'après la démonstration du th. 1.15 pour $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$). Il résulte de la correspondance de Galois et du théorème d'Ax-Sen-Tate que :

Proposition 1.17. — (i) $\widetilde{\mathbf{E}}_K$ *est le complété de la clôture radicielle de* $\mathbf{E}_K$.

(ii) $\mathbf{E}_K$ (*resp.* $\widetilde{\mathbf{E}}_K$) *est une extension séparable de* $\mathbf{E}_{\mathbf{Q}_p}$ (*resp.* $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$) *de degré* $[\mathrm{H}_{\mathbf{Q}_p} : \mathrm{H}_K] = [K_\infty : F_\infty]$, *et si* $K/\mathbf{Q}_p$ *est galoisienne, alors* $\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}$ *et* $\widetilde{\mathbf{E}}_K/\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ *sont galoisiennes de groupe de Galois* $\mathrm{H}_{\mathbf{Q}_p}/\mathrm{H}_K = \mathrm{Gal}(K_\infty/F_\infty)$.

1.3. Le corps $\widetilde{\mathbf{B}}$ et certains de ses sous-anneaux

1.3.1. Les anneaux $\widetilde{\mathbf{A}}^+$ *et* $\widetilde{\mathbf{A}}$ *et leurs topologies.* — Soient $\widetilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+)$ et $\widetilde{\mathbf{A}} = W(\widetilde{\mathbf{E}})$. Par construction, on a

$$\widetilde{\mathbf{A}}/p\widetilde{\mathbf{A}} = \widetilde{\mathbf{E}} \quad \text{et} \quad \widetilde{\mathbf{A}}^+/p\widetilde{\mathbf{A}}^+ = \widetilde{\mathbf{E}}^+$$

et tout élément de $\widetilde{\mathbf{A}}^+$ (resp. $\widetilde{\mathbf{A}}$) s'écrit de manière unique sous la forme $\sum_{k=0}^{+\infty} p^k[x_k]$, où les x_k sont des éléments de $\widetilde{\mathbf{E}}^+$ (resp. $\widetilde{\mathbf{E}}$).

Ces anneaux sont naturellement munis de deux topologies : la topologie forte et la topologie faible. La *topologie forte* consiste à munir $\widetilde{\mathbf{A}}$ (resp. $\widetilde{\mathbf{A}}^+$) de la topologie d'anneau la moins fine rendant continue la projection $\widetilde{\mathbf{A}} \to \widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{A}}^+ \to \widetilde{\mathbf{E}}^+$), où l'on a muni $\widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{E}}^+$) de la topologie discrète. La topologie forte sur $\widetilde{\mathbf{A}}$ ou $\widetilde{\mathbf{A}}^+$ n'est donc rien d'autre que la topologie p-adique.

La *topologie faible* sur $\widetilde{\mathbf{A}}$ (resp. $\widetilde{\mathbf{A}}^+$) est la topologie d'anneau la moins fine rendant continue la projection $\widetilde{\mathbf{A}} \to \widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{A}}^+ \to \widetilde{\mathbf{E}}^+$), où l'on a muni $\widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{E}}^+$) de la topologie induite par la valuation $v_{\mathbf{E}}$. Une base de voisinages de 0 pour cette topologie est constituée des $p^k\widetilde{\mathbf{A}}+[\tilde{p}]^n\widetilde{\mathbf{A}}^+$ (resp. $p^k\widetilde{\mathbf{A}}^+ + [\tilde{p}]^n\widetilde{\mathbf{A}}^+$), où k,n décrivent $\mathbf{N}$.

Remarquons que la restriction de la topologie forte (resp. faible) sur $\widetilde{\mathbf{A}}$ à $\widetilde{\mathbf{A}}^+$ est la topologie forte (resp. faible) sur $\widetilde{\mathbf{A}}^+$. La topologie faible peut aussi se décrire de la manière suivante. Si $x = \sum_{i=0}^{+\infty} p^i[x_i] \in \widetilde{\mathbf{A}}$ et $k \in \mathbf{Z}$, soit $w_k(x) = \inf_{i\leqslant k} v_{\mathbf{E}}(x_i)$. On a $x \in p^{k+1}\widetilde{\mathbf{A}} + [\tilde{p}]^n\widetilde{\mathbf{A}}^+$ si et seulement si $w_k(x) \geqslant n$ et, d'autre part, la fonction w_k vérifie les propriétés suivantes qui sont immédiates.

(i) $w_k(x) = +\infty$ si et seulement si $x \in p^{k+1}\widetilde{\mathbf{A}}$,

(ii) $w_k(x+y) \geqslant \inf(w_k(x), w_k(y))$ avec égalité si $w_k(x) \neq w_k(y)$.

(iii) $w_k(xy) \geqslant \inf_{i+j\leqslant k}(w_i(x) + w_j(y))$.

(iv) $w_k(\varphi(x)) = pw_k(x)$.

(v) $w_k(\sigma(x)) = w_k(x)$ si $\sigma \in \mathrm{G}_{\mathbf{Q}_p}$.

Lemme 1.18. — *L'application qui à $x \in \widetilde{\mathbf{E}}$ associe $[x] \in \widetilde{\mathbf{A}}$ est continue pour les topologies faible et forte.*

Démonstration. — Le résultat est trivial si on munit $\widetilde{\mathbf{A}}$ et $\widetilde{\mathbf{E}}$ des topologies fortes (la topologie forte sur $\widetilde{\mathbf{E}}$ étant la topologie discrète). D'autre part, d'après les formules explicites donnant l'addition des vecteurs de Witt, il existe des polynômes $Q_k \in \mathbf{Z}[X,Y]$ tels que l'on ait

$$[x+y]-[x] = \sum_{k=0}^{+\infty} p^k\Big[Q_k\big(x^{p^{-k}}, y^{p^{-k}}\big)\Big]$$

et Q_k est divisible par Y puisque $[x+y]-[x] = 0$ si $y=0$. On en déduit le fait que, si $v_{\mathbf{E}}(y) \geqslant np^{k-1}$, alors $[x+y]-[x] \in p^k\widetilde{\mathbf{A}} + [\tilde{p}]^n\widetilde{\mathbf{A}}^+$. Ceci permet de conclure.

Proposition 1.19. — (i) *L'application $(x_k)_{k\in\mathbf{N}} \mapsto \sum_{k=0}^{+\infty} p^k[x_k]$ est un homéomorphisme de $(\widetilde{\mathbf{E}})^{\mathbf{N}}$ (resp. $(\widetilde{\mathbf{E}}^+)^{\mathbf{N}}$) sur $\widetilde{\mathbf{A}}$ (resp. $\widetilde{\mathbf{A}}^+$) pour les topologies faible et forte.*

(ii) *$\widetilde{\mathbf{A}}$ et $\widetilde{\mathbf{A}}^+$ sont séparés et complets pour les topologies forte et faible.*

Démonstration. — La demonstration est la même dans tous les cas. L'application $(x_k)_{k\in\mathbf{N}} \mapsto \sum_{k=0}^{+\infty} p^k[x_k]$ est continue comme limite uniforme d'applications continues et, dans l'autre sens, on récupère les x_k à partir de x via l'algorithme suivant : $x_k = \overline{a}_k$, où $a_0 = x$ et $a_{k+1} = p^{-1}(a_k - [x_k])$. Comme d'autre part, « $px \in p^{k+1}\widetilde{\mathbf{A}} + [\tilde{p}]^n\widetilde{\mathbf{A}}^+$ » implique « $x \in p^k\widetilde{\mathbf{A}} + [\tilde{p}]^n\widetilde{\mathbf{A}}^+$, on en déduit la continuité des applications $x \mapsto x_k$ en utilisant de manière répétée celles de $x \mapsto \overline{x}$ et $x \mapsto [x]$. Ceci termine la démonstration du (i).

Le (ii) s'en déduit via l'énoncé correspondant pour $\widetilde{\mathbf{E}}^+$ et $\widetilde{\mathbf{E}}$.

Soient $\widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}[\frac{1}{p}]$ et $\widetilde{\mathbf{B}}^+ = \widetilde{\mathbf{A}}^+[\frac{1}{p}]$. Tout élément de $\widetilde{\mathbf{B}}$ (resp. $\widetilde{\mathbf{B}}^+$) s'écrit de manière unique sous la forme $\sum_{k\in\mathbf{Z}} p^k[x_k]$, où $(x_k)_{k\in\mathbf{Z}}$ est une suite d'éléments de $\widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{E}}^+$) nuls pour $k \ll 0$.

On peut munir ces anneaux de la topologie forte (resp. faible) consistant à munir $\widetilde{\mathbf{B}} = \cup_{k\in\mathbf{N}} p^{-k}\widetilde{\mathbf{A}}$ et $\widetilde{\mathbf{B}}^+ = \cup_{k\in\mathbf{N}} p^{-k}\widetilde{\mathbf{A}}^+$ de la toplogie de la limite inductive, où l'on a muni $p^{-k}\widetilde{\mathbf{A}} \cong \widetilde{\mathbf{A}}$

et $p^{-k}\widetilde{\mathbf{A}}^+ \cong \widetilde{\mathbf{A}}^+$ de la topologie forte (resp. faible), ce qui fait de $\widetilde{\mathbf{B}}$ et $\widetilde{\mathbf{B}}^+$ des $\mathbf{Q}_p$-espaces de Banach dont les boules unités sont $\widetilde{\mathbf{A}}$ et $\widetilde{\mathbf{A}}^+$ (resp. des $\mathbf{Q}_p$-espaces vectoriels topologiques localement convexes et complets).

Proposition 1.20. — *$\widetilde{\mathbf{B}}$ est un corps.*

Démonstration. — $\widetilde{\mathbf{A}}$ est un p-anneau strict dont l'anneau résiduel $\widetilde{\mathbf{E}}$ est un corps.

Par fonctorialité des vecteurs de Witt, on peut relever (de manière unique) les actions de $\mathrm{G}_{\mathbf{Q}_p}$ et φ sur $\widetilde{\mathbf{E}}$ et $\widetilde{\mathbf{E}}^+$, ce qui permet de munir les anneaux $\widetilde{\mathbf{A}}$, $\widetilde{\mathbf{B}}$, $\widetilde{\mathbf{A}}^+$ et $\widetilde{\mathbf{B}}^+$ d'une action de $\mathrm{G}_{\mathbf{Q}_p}$ et d'une action du Frobenius φ commutant entre elles. De manière explicite,

$$\varphi\Big(\sum p^k[x_k]\Big) = \sum p^k[x_k^p] \quad \text{et} \quad \sigma\Big(\sum p^k[x_k]\Big) = \sum p^k[\sigma(x_k)] \text{ si } \sigma \in \mathrm{G}_{\mathbf{Q}_p}.$$

Proposition 1.21. — *φ agit continûment sur $\widetilde{\mathbf{A}}$, $\widetilde{\mathbf{B}}$, $\widetilde{\mathbf{A}}^+$ et $\widetilde{\mathbf{B}}^+$ munis des topologies forte ou faible et l'on a*

$$\widetilde{\mathbf{A}}^{\varphi=1} = (\widetilde{\mathbf{A}}^+)^{\varphi=1} = \mathbf{Z}_p \quad \text{et} \quad \widetilde{\mathbf{B}}^{\varphi=1} = (\widetilde{\mathbf{B}}^+)^{\varphi=1} = \mathbf{Q}_p.$$

Démonstration. — La continuité de l'action de φ est immédiate et un élément $x = \sum_{k=0}^{+\infty} p^k[x_k]$ est invariant par φ si et seulement si on a $x_k^p = x_k$ et donc $x_k \in \mathbf{F}_p$ pour tout k, c'est-à-dire si et seulement si $x \in W(\mathbf{F}_p) = \mathbf{Z}_p$.

Remarque 1.22. — Ni $\mathrm{H}_{\mathbf{Q}_p}$ ni, a fortiori, $\mathrm{G}_{\mathbf{Q}_p}$ n'agissent discrètement sur $\widetilde{\mathbf{E}}$ ou $\widetilde{\mathbf{E}}^+$, ce qui implique que ni $\mathrm{H}_{\mathbf{Q}_p}$ ni $\mathrm{G}_{\mathbf{Q}_p}$ n'agissent continûment sur $\widetilde{\mathbf{A}}$, $\widetilde{\mathbf{B}}$, $\widetilde{\mathbf{A}}^+$ ou $\widetilde{\mathbf{B}}^+$ si on les munit de la topologie forte. Par contraste on a le résultat suivant.

Proposition 1.23. — *$\mathrm{G}_{\mathbf{Q}_p}$ agit continûment sur $\widetilde{\mathbf{A}}$, $\widetilde{\mathbf{B}}$, $\widetilde{\mathbf{A}}^+$ et $\widetilde{\mathbf{B}}^+$ munis de la topologie faible.*

Démonstration. — C'est une conséquence des homéomorphismes de $\widetilde{\mathbf{A}}^+$ sur $(\widetilde{\mathbf{E}}^+)^{\mathbf{N}}$ et $\widetilde{\mathbf{A}}$ sur $(\widetilde{\mathbf{E}})^{\mathbf{N}}$ et de la continuité de l'action de $\mathrm{G}_{\mathbf{Q}_p}$ sur $\widetilde{\mathbf{E}}^+$ et $\widetilde{\mathbf{E}}$.

Si $[K:F] < +\infty$, soient $\widetilde{\mathbf{A}}_K = W(\widetilde{\mathbf{E}}_K)$, $\widetilde{\mathbf{B}}_K[\frac{1}{p}]$, $\widetilde{\mathbf{A}}_K^+ = W(\widetilde{\mathbf{E}}_K^+)$, $\widetilde{\mathbf{B}}_K^+ = \widetilde{\mathbf{A}}_K^+[\frac{1}{p}]$. Par construction, on a

$$\widetilde{\mathbf{A}}_K/p\widetilde{\mathbf{A}}_K = \widetilde{\mathbf{E}}_K \quad \text{et} \quad \widetilde{\mathbf{A}}_K^+/p\widetilde{\mathbf{A}}_K^+ = \widetilde{\mathbf{E}}_K^+.$$

Les anneaux $\widetilde{\mathbf{A}}_K$, $\widetilde{\mathbf{B}}_K$, $\widetilde{\mathbf{A}}_K^+$ et $\widetilde{\mathbf{B}}_K^+$ sont des sous-anneaux de $\widetilde{\mathbf{A}}$, $\widetilde{\mathbf{B}}$, $\widetilde{\mathbf{A}}^+$ et $\widetilde{\mathbf{B}}^+$ respectivement, fermés pour les topologies forte ou faible. D'autre part, on a :

Proposition 1.24. — *Si K est une extension finie de F, alors*

$$\widetilde{\mathbf{A}}^{\mathrm{H}_K} = \widetilde{\mathbf{A}}_K, \quad (\widetilde{\mathbf{A}}^+)^{\mathrm{H}_K} = \widetilde{\mathbf{A}}_K^+, \quad \widetilde{\mathbf{B}}^{\mathrm{H}_K} = \widetilde{\mathbf{B}}_K \quad \text{et} \quad (\widetilde{\mathbf{B}}^+)^{\mathrm{H}_K} = \widetilde{\mathbf{B}}_K^+.$$

Démonstration. — C'est une conséquence immédiate du fait que $\widetilde{\mathbf{E}}^{\mathrm{H}_K} = \widetilde{\mathbf{E}}_K$ et $(\widetilde{\mathbf{E}}^+)^{\mathrm{H}_K} = \widetilde{\mathbf{E}}_K^+$.

Corollaire 1.25. — *Si K est une extension finie de F, alors $\widetilde{\mathbf{B}}_K$ est un corps.*

1.3.2. L'élément π. — Soit $\pi = [\varepsilon] - 1$. Comme l'action de φ et $\mathrm{G}_{\mathbf{Q}_p}$ sur π sont donnée par les formules

$$\varphi(\pi) = (1+\pi)^p - 1 \quad \text{et} \quad g(\pi) = (1+\pi)^{\chi(g)} - 1,$$

l'anneau $\mathbf{A}^+_{\mathbf{Q}_p} = \mathbf{Z}_p[[\pi]]$ est stable par φ et $\mathrm{G}_{\mathbf{Q}_p}$.

Soit $\mathbf{A}_{\mathbf{Q}_p} = \mathbf{Z}_p[[\pi]]\{\frac{1}{\pi}\}$ l'adhérence de $\mathbf{Z}_p[[\pi]][\frac{1}{\pi}]$ dans $\widetilde{\mathbf{A}}$ pour la topologie forte (ou faible, cela revient au même car $\mathbf{Z}_p[[\pi]]$ est complet pour les deux). C'est l'anneau des séries de Laurent de la forme $\sum_{k \in \mathbf{Z}} a_k \pi^k$, où $a_k \in \mathbf{Z}_p$ et $\lim_{k \to -\infty} v_p(a_k) = +\infty$. Soit $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[\frac{1}{p}]$.

Proposition 1.26. — *$\mathbf{B}_{\mathbf{Q}_p}$ est un sous-corps de $\widetilde{\mathbf{B}}$ stable par $\mathrm{G}_{\mathbf{Q}_p}$ et φ.*

Démonstration. — $\mathbf{A}_{\mathbf{Q}_p}$ est un p-anneau strict dont l'anneau résiduel $\mathbf{A}_{\mathbf{Q}_p}/p\mathbf{A}_{\mathbf{Q}_p}$ égal à $\mathbf{F}_p(\overline{\pi})$, est un corps ; ceci permet de prouver que $\mathbf{B}_{\mathbf{Q}_p}$ est un corps. La stablité de $\mathbf{B}_{\mathbf{Q}_p}$ sous l'action de φ et de $\mathrm{G}_{\mathbf{Q}_p}$ résulte, quant à elle, des formules ci-dessus.

1.3.3. Les anneaux $\mathbf{A}$, $\mathbf{B}$, $\mathbf{A}_K$ et $\mathbf{B}_K$. — Si $[K : F] < +\infty$, l'extension $\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}$ est finie et séparable, et comme $\widetilde{\mathbf{B}}$ a comme corps résiduel $\widetilde{\mathbf{E}}$ qui contient $\mathbf{E}_K$, il existe une unique extension non ramifiée $\mathbf{B}_K$ de $\mathbf{B}_{\mathbf{Q}_p}$ de corps résiduel $\mathbf{E}_K$ contenue dans $\widetilde{\mathbf{B}}$. On note $\mathbf{A}_K$ l'anneau de ses entiers.

Remarque 1.27. — Soient $\overline{x} \in \mathbf{E}^+_K$ un élément primitif de l'extension séparable $\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}$, $\overline{P} \in \mathbf{E}^+_{\mathbf{Q}_p}[X]$ le polynôme minimal de $\overline{x}$ sur $\mathbf{E}_{\mathbf{Q}_p}$ et $P \in \mathbf{A}^+_{\mathbf{Q}_p}[X]$ un polynôme unitaire dont la réduction modulo p est $\overline{P}$. D'après le lemme de Hensel, le polynôme P a une unique racine x dans $\widetilde{\mathbf{A}}$ dont la réduction modulo p est $\overline{x}$ et $\mathbf{B}_K = \mathbf{B}_{\mathbf{Q}_p}[x] \cong \mathbf{B}_{\mathbf{Q}_p}[X]/P$ et $\mathbf{A}_K = \mathbf{A}_{\mathbf{Q}_p}[x] \cong \mathbf{A}_{\mathbf{Q}_p}[X]/P$.

Si K est une extension non ramifiée de F, on a $\mathbf{A}_K = \mathscr{O}_K \otimes_{\mathbf{Z}_p} \mathbf{A}_{\mathbf{Q}_p}$. Dans le cas général, on a le résultat (immédiat) suivant.

Proposition 1.28. — *Soient K une extension finie de $\mathbf{Q}_p$ et F l'extension non ramifiée maximale de $\mathbf{Q}_p$ contenue dans K_∞. Si $\overline{\pi}_K$ est une uniformisante de $\mathbf{E}_K$ et π_K est un élément de $\mathbf{A}_K$ dont la réduction modulo p est $\overline{\pi}_K$, alors $\mathbf{A}_K$ est un $\mathbf{A}_F$-module libre dont $(1, \pi_K, \ldots, \pi_K^{e_K - 1})$ est une base.*

Proposition 1.29. — *Soient K une extension finie de $\mathbf{Q}_p$ et F l'extension non ramifiée maximale de $\mathbf{Q}_p$ contenue dans K_∞. Si $\overline{\pi}_K$ est une uniformisante de $\mathbf{E}_K$ et π_K est un élément de $\mathbf{A}_K$ dont la réduction modulo p est $\overline{\pi}_K$, alors tout élément de $\mathbf{A}_K$ peut s'écrire de manière unique sous la forme $\sum_{k \in \mathbf{Z}} a_k \pi_K^k$, où $(a_k)_{k \in \mathbf{Z}}$ est une suite d'éléments de $\mathscr{O}_F$ tendant vers 0 quand k tend vers $-\infty$.*

Démonstration. — On peut expliciter l'écriture d'un élément x de $\mathbf{A}_K$ comme série de Laurent en π_K de la manière suivante. Soit $s : \mathbf{E}_K \to \mathbf{A}_K$ la section de la réduction $x \mapsto \overline{x}$ modulo p donnée par la formule

$$s\Big(\sum_{k \in \mathbf{Z}} a_k \overline{\pi}_K^k\Big) = \sum_{k \in \mathbf{Z}} [a_k] \pi_K^k.$$

Si $x \in \mathbf{A}_K$, on définit par récurrence une suite $(a_n)_{n \in \mathbf{N}}$ d'éléments de $\mathbf{A}_K$ en posant $x_0 = x$ et $x_{n+1} = p^{-1}(x_n - s(\overline{x}_n))$. On a alors $s(x) = \sum_{n=0}^{+\infty} p^n s(\overline{x}_n)$.

Comme $\mathbf{E} = \cup_{[K:F]<+\infty}\mathbf{E}_K$ est la clôture séparable de $\mathbf{E}_{\mathbf{Q}_p}$, l'extension maximale non ramifiée $\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{nr}}$ de $\mathbf{B}_{\mathbf{Q}_p}$ dans $\widetilde{\mathbf{B}}$ est aussi la réunion des $\mathbf{B}_K$, où K parcourt les extensions finies de F. On note $\mathbf{B}$ l'adhérence de $\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{nr}}$ dans $\widetilde{\mathbf{B}}$ pour la topologie forte ; son anneau des entiers $\mathbf{A}$ est donc le complété de l'anneau $\cup_{[K:F]<+\infty}\mathbf{A}_K$ des entiers de $\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{nr}}$ pour la topologie p-adique.

Proposition 1.30. — (i) *Si K est une extension finie de $\mathbf{Q}_p$, $\mathbf{A}_K$ et $\mathbf{B}_K$ sont stables par φ.*

(ii) *Les sous-anneaux $\mathbf{B}$, $\mathbf{A}$ et de $\widetilde{\mathbf{B}}$ sont stables sous l'action de $\mathrm{G}_{\mathbf{Q}_p}$ et φ.*

(iii) $\mathrm{H}_{\mathbf{Q}_p}$ *agit continuement sur $\mathbf{B}$ muni de la topologie forte.*

(iv) *Si K est une extension finie de F, on a $\mathbf{B}^{\mathrm{H}_K} = \mathbf{B}_K$ et $\mathbf{A}^{\mathrm{H}_K} = \mathbf{A}_K$.*

Démonstration. — (i) Si $\overline{x} \in \mathbf{E}_K^+$ est un élément primitif de l'extension séparable $\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}$, il en est de même de $\overline{x}^p$. Maintenant, si $x \in \mathbf{A}_K$ a pour réduction $\overline{x}$ modulo p et si $P \in \mathbf{A}_{\mathbf{Q}_p}[X]$ est le polynôme minimal de x sur $\mathbf{B}_{\mathbf{Q}_p}$, le polynôme minimal de $\varphi(x)$ sur $\mathbf{B}_{\mathbf{Q}_p}$ est le polynome $\varphi(P) \in \mathbf{A}_{\mathbf{Q}_p}[X]$ dont la réduction modulo p est le polynôme minimal de $\overline{x}^p$. Il résulte alors de la rem. 1.27 que l'on a $\mathbf{B}_K = \mathbf{B}_{\mathbf{Q}_p}[\varphi(x)]$, ce qui montre que $\mathbf{B}_K$ (et donc aussi $\mathbf{A}_K$) est stable par φ.

(ii) La stabilité de $\mathbf{A}$ et $\mathbf{B}$ par φ suit, par complétion, de celle de $\mathbf{A}_K$ et $\mathbf{B}_K$ pour toute extension finie K de F. D'autre part, comme $g \in \mathrm{G}_{\mathbf{Q}_p}$ est un isomorphisme de $\mathbf{B}_{\mathbf{Q}_p}$, l'unicité de $\mathbf{B}_K$ montre que g induit un isomorphisme de $\mathbf{B}_K$ sur $\mathbf{B}_{g(K)}$, ce qui montre que $\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{nr}}$ est stable par $\mathrm{G}_{\mathbf{Q}_p}$; il en est donc de même de $\mathbf{B}$ et $\mathbf{A}$ par complétion.

(iii) On a $\mathrm{Gal}(\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{nr}}/\mathbf{B}_{\mathbf{Q}_p}) = \mathrm{Gal}(\mathbf{E}/\mathbf{E}_{\mathbf{Q}_p}) = \mathrm{H}_{\mathbf{Q}_p}$, ce qui montre que $\mathrm{H}_{\mathbf{Q}_p}$ agit continûment sur $\mathbf{E} = \mathbf{A}/p\mathbf{A}$ muni de la topologie discrète et donc continûment sur $\mathbf{A}$ (et sur $\mathbf{B}$) muni de la topologie forte (p-adique).

(iv) Si K est une extension finie de F, on a $\mathbf{E}^{\mathrm{H}_K} = \mathbf{E}_K$ et donc $(\mathbf{B}_{\mathbf{Q}_p}^{\mathrm{nr}})^{\mathrm{H}_K} = \mathbf{B}_K$, ce qui permet de déduire l'identité $\mathbf{B}^{\mathrm{H}_K}$ du théorème d'Ax-Sen-Tate.

Remarque 1.31. — Par construction, $\mathbf{A}$ et $\mathbf{B}$ sont complets pour la topologie forte. Par contre, comme $\mathbf{E}$ est dense dans $\widetilde{\mathbf{E}}$ et $\mathbf{A}/p\mathbf{A} = \mathbf{E}$, on montre que $\mathbf{A}$ (resp. $\mathbf{B}$) est dense dans $\widetilde{\mathbf{A}}$ (resp. $\widetilde{\mathbf{B}}$) pour la topologie faible.

1.3.4. L'opérateur ψ. —

Corollaire 1.32. — (i) $1, [\varepsilon], \dots, [\varepsilon^{p-1}]$ *est une base de $\mathbf{A}$ sur $\varphi(\mathbf{A})$.*

(ii) $\mathbf{B}$ *est une extension de degré p de $\varphi(\mathbf{B})$ et $1, [\varepsilon], \dots, [\varepsilon^{p-1}]$ est une base de $\mathbf{B}$ sur $\varphi(\mathbf{B})$.*

Démonstration. — Il s'agit de montrer que l'application $(x_0, \dots, x_{p-1}) \mapsto \varphi(x_0) + \varphi(x_1)[\varepsilon] + \dots + \varphi(x_{p-1})[\varepsilon^{p-1}]$ est un isomorphisme de $\mathbf{A}^p$ sur $\mathbf{A}$ et comme les deux membres sont séparés et complets pour la topologie p-adique et sans p-torsion, il suffit de vérifier le résultat modulo p, ce qui suit du lemme précédent.

Le (ii) est une conséquence immédiate du (i).

Soit $\psi : \mathbf{B} \to \mathbf{B}$ défini par $\psi(x) = p^{-1}\varphi^{-1}(\mathrm{Tr}_{\mathbf{B}/\varphi(\mathbf{B})}(x))$.

Proposition 1.33. — (i) *Si $x = \varphi(x_0) + \varphi(x_1)[\varepsilon] + \dots + \varphi(x_{p-1})[\varepsilon^{p-1}]$, alors $\psi(x) = x_0$.*

(ii) $\psi(\mathbf{A}) \subset \mathbf{A}$.

(iii) $\psi \circ \varphi = \mathrm{id}$ (autrement dit, ψ est un inverse à gauche de φ).

(iv) ψ *commute à l'action de* $\mathrm{G}_{\mathbf{Q}_p}$.

Démonstration. — On a $\psi(1)=1$ puisque $\mathbf{B}/\varphi(\mathbf{B})=p$. D'autre part, comme $[\varepsilon^i]^p=\varphi([\varepsilon^i])$, le polynôme minimal de $[\varepsilon^i]$ sur $\varphi(\mathbf{B})$ est $X^p-\varphi([\varepsilon^i])$ si $1\leqslant i\leqslant p-1$ et sa trace est donc nulle. On en déduit le (i) et les (ii) et (iii) qui en sont des conséquences directes. Le (iv), quant à lui est une conséquence du fait que φ (et donc aussi $\mathrm{Tr}_{\mathbf{B}/\varphi(\mathbf{B})}$) commute à $\mathrm{G}_{\mathbf{Q}_p}$.

1.3.5. Les anneaux $\mathbf{A}^+$, $\mathbf{B}^+$, $\mathbf{A}^+_K$ et $\mathbf{B}^+_K$. — Soient $\mathbf{A}^+=\widetilde{\mathbf{A}}^+\cap\mathbf{A}$ et $\mathbf{B}^+=\widetilde{\mathbf{B}}^+\cap\mathbf{B}=\mathbf{A}^+[\frac{1}{p}]$.

Lemme 1.34. — *Si $x\in\mathbf{A}\cap(\widetilde{\mathbf{A}}^++p^k\widetilde{\mathbf{A}})$, il existe $y\in p^k\mathbf{A}$ tel que $x-y\in\widetilde{\mathbf{A}}^+\cap p^{k+1}\widetilde{\mathbf{A}}$.*

Démonstration. — Par hypothèse, on peut écrire x sous la forme $a+p^kb$ avec $a\in\widetilde{\mathbf{A}}^+$ et $b\in\widetilde{\mathbf{A}}$. Soit $\overline{b}\in\widetilde{\mathbf{E}}$ la réduction de b modulo p. Comme $\mathbf{E}$ est dense dans $\widetilde{\mathbf{E}}$ (th. 1.15), il existe $\overline{z}\in\mathbf{E}$ tel que $v_{\mathbf{E}}(\overline{z}-\overline{b})\geqslant 0$, ce qui implique que si $z\in\mathbf{A}$ est n'importe quel relèvement de $\overline{z}$, alors $z-b\in\widetilde{\mathbf{A}}^++p\widetilde{\mathbf{A}}$. On peut alors prendre $y=p^kz$.

Proposition 1.35. — $\mathbf{A}^+/p\mathbf{A}^+=\mathbf{E}^+$.

Démonstration. — On a $\mathbf{A}\cap p\widetilde{\mathbf{A}}=p\mathbf{A}$ et $\widetilde{\mathbf{A}}^+\cap p\widetilde{\mathbf{A}}=p\widetilde{\mathbf{A}}^+$, ce qui montre que $\mathbf{A}^+\cap p\widetilde{\mathbf{A}}=p\mathbf{A}^+$ d'une part et d'autre part que l'injection de $\mathbf{A}^+/p\mathbf{A}^+$ dans $\widetilde{\mathbf{A}}/p\widetilde{\mathbf{A}}$ se factorise par $\mathbf{A}/p\mathbf{A}=\mathbf{E}$ et $\widetilde{\mathbf{A}}^+/p\widetilde{\mathbf{A}}^+=\widetilde{\mathbf{E}}^+$. On en déduit le fait que l'injection de $\mathbf{A}^+$ dans $\widetilde{\mathbf{A}}$ induit une injection de $\mathbf{A}^+/p\mathbf{A}^+$ dans $(\mathbf{A}/p\mathbf{A})\cap\widetilde{\mathbf{E}}^+=\mathbf{E}^+$. Il reste à prouver que cette application est surjective.

Soit $\overline{x}\in\mathbf{E}^+$ et $x\in\mathbf{A}$ un relèvement quelconque de $\overline{x}$. Utilisant le lemme précédent, on construit par récurrence des suites $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\geqslant 1}$ d'éléments de $\mathbf{A}$ vérifiant les conditions suivantes

(i) $x_0=x\in\widetilde{\mathbf{A}}^++p\widetilde{\mathbf{A}}$;
(ii) $y_n\in p^n\mathbf{A}$ et $x_n-y_n\in\widetilde{\mathbf{A}}^++p^{n+1}\widetilde{\mathbf{A}}$;
(iii) $x_{n+1}=x_n-y_n\in\widetilde{\mathbf{A}}^++p^{n+1}\widetilde{\mathbf{A}}$.

La suite de terme général x_n a une limite z dans $\mathbf{A}$ qui appartient à $\widetilde{\mathbf{A}}^+$ et donc est élément de $\mathbf{A}^+$. De plus, l'image de z modulo $\mathbf{A}^+\cap p\widetilde{\mathbf{A}}=p\mathbf{A}^+$ est égale à $\overline{x}$ par construction. On en déduit le résultat.

On définit $\mathbf{A}^+_K$ et $\mathbf{B}^+_K$ en prenant, comme d'habitude, les invariants sous H_K. Contrairement à d'habitude, on n'a pas forcément $\mathbf{A}^+_K/p\mathbf{A}^+_K=\mathbf{E}^+_K$.

Proposition 1.36. — *$\mathbf{A}^+_K/p\mathbf{A}^+_K$ s'injecte dans $\mathbf{E}^+_K$ et ne lui est égal que si $\mathbf{E}_K/\mathbf{E}_{\mathbf{Q}_p}$ est non ramifiée ou, ce qui revient au même, si K_∞/F_∞ est non ramifiée.*

2. L'équivalence de catégories de Fontaine

2.1. Rudiments de cohomologie galoisienne. — Soient G un groupe topologique et X un groupe topologique muni d'une action continue de G respectant la structure de groupe, c'est-à-dire une application continue $(\sigma,x)\to\sigma(x)$ de $G\times X$ dans X vérifiant :

- $\sigma\tau(x)=\sigma(\tau(x))$ quels que soient $\sigma,\tau\in G$ et $x\in X$
- $\sigma(xy)=\sigma(x)\sigma(y)$ quels que soient $\sigma\in G$ et $x,y\in X$.

On appelle *cocycle continu* sur G à valeurs dans X une application continue $\sigma\to c_\sigma$ vérifiant la relation (dite de cocycle)

$$c_{\sigma\tau}=c_\sigma\sigma(c_\tau)\quad\text{quels que soient }\sigma,\tau\in G.$$

L'exemple de cocycle continu le plus simple est le *cocycle trivial* défini par $c_\sigma = 1$ quel que soit $\sigma \in G$.

Si $\sigma \to c_\sigma$ est un cocycle continu sur G et $a \in X$, alors $\sigma \to c'_\sigma = a^{-1}c_\sigma\sigma(a)$ est un cocyle continu sur G comme le montre la relation

$$c'_{\sigma\tau} = a^{-1}c_{\sigma\tau}\sigma\tau(a) = a^{-1}c_\sigma\sigma(c_\tau)\sigma\tau(a) = a^{-1}c_\sigma\sigma(a)\sigma(a^{-1}c_\tau\tau(a)) = c'_\sigma\sigma(c'_\tau).$$

On dit que deux cocycles continus $\sigma \to c_\sigma$ et $\sigma \to c'_\sigma$ sont *cohomologues* s'il existe $a \in X$ tel que l'on ait $c'_\sigma = a^{-1}c_\sigma\sigma(a)$. Un cocycle $\sigma \to c_\sigma$ est donc cohomologue au cocycle trivial s'il existe $a \in X$ tel que l'on ait $c_\sigma = a^{-1}\sigma(a)$ quel que soit $\sigma \in G$ (un tel cocylcle est un *cobord*).

La relation de cohomologie est de manière évidente une relation d'équivalence et on note $H^1(G, X)$ l'ensemble des classes d'équivalences.

Si H est un sous-groupe de G, et $\sigma \to c_\sigma$ est un cocycle continu sur G, la restriction de c à H est clairement un cocycle continu sur G. De plus, si $\sigma \to c_\sigma$ et $\sigma \to c'_\sigma$ sont cohomologues sur G, ils le sont a fortiori sur H (on peut prendre le même a) ; on en déduit une application naturelle *de restriction* :

$$\mathrm{res} : H^1(G, X) \longrightarrow H^1(H, X).$$

Maintenant, si H est un sous-groupe distingué fermé de G et si $\sigma \to c_\sigma$ est un cocycle continu de G/H dans X^H, on peut obtenir "par inflation" un cocycle continu $\inf(c)$ sur G en posant $\inf(c)_\sigma = c_{\pi(\sigma)}$, où π désigne la projection de G sur G/H. D'autre part, si $\sigma \to c_\sigma$ et $\sigma \to c'_\sigma$ sont cohomologues sur G/H, ils le sont sur G (on peut prendre le même a) ; on en déduit une application naturelle *d'inflation* :

$$\inf : H^1(G/H, X^H) \longrightarrow H^1(G, X).$$

Proposition 2.1. — *La suite (dite "d'inflation-restriction")*

$$1 \to H^1(G/H, X^H) \xrightarrow{\inf} H^1(G, X) \xrightarrow{\mathrm{res}} H^1(H, X)$$

est exacte.

Remarque 2.2. — Comme on n'a pas supposé X commutatif, les ensembles considérés ne sont pas des groupes et dire que la suite ci-dessus est exacte signifie premièrement que l'application d'inflation de $H^1(G/H, X^H)$ dans $H^1(G, X)$ est injective et que si $\sigma \to c_\sigma$ est un cocycle sur G dont la restriction à H est cohomologue au cocycle trivial, alors il est cohomologue à un cocycle qui provient par inflation d'un cocycle sur G/H.

Démonstration. — Commençons par l'injectivité de l'inflation. Si $\sigma \to c_\sigma$ est un cocycle sur G provenant par inflation d'un cocycle sur G/H, on a $c_\sigma = 1$ si $\sigma \in H$ et donc, si $\sigma \to c_\sigma$ et $\sigma \to c'_\sigma$ sont deux cocycles sur H à valeurs dans X^H dont les inflations sont cohomologues, il existe $x \in X$ tel que l'on ait $c'_\sigma = a^{-1}c_\sigma\sigma(a)$ quel que soit $\sigma \in G$, ce qui devient $\sigma(a) = a$ si $\sigma \in H$ et prouve que $a \in X^H$ et que $\sigma \to c_\sigma$ et $\sigma \to c_\sigma$ ont même image dans $H^1(G/H, X^H)$.

Maintenant, si $\sigma \to c_\sigma$ est un cocycle sur G dont la restriction à H est cohomologue au cocycle trivial, il existe a tel que $c'_\sigma = a^{-1}c_\sigma\sigma(a) = 1$ si $\sigma \in H$. Mais alors si $\tau \in G$ et $\sigma \in H$, on a

$$\begin{aligned} c'_{\tau\sigma} &= c'_\tau\tau(c'_\sigma) = c'_\tau \\ c'_{\sigma\tau} &= c'_{\tau(\tau^{-1}\sigma\tau)} = c'_\tau \\ c'_{\sigma\tau} &= c'_\sigma\sigma(c'_\tau) = \sigma(c'_\tau), \end{aligned}$$

ce qui prouve que c' est à valeurs dans X^H et constant modulo H et donc est l'inflation d'un cocycle sur G/H. Ceci termine la démonstration de la proposition.

Théorème 2.3. — (Hilbert 90) *Soit L/F une extension galoisienne finie de groupe de Galois G. Si on fait agir G sur $\mathrm{GL}_d(L)$ de la manière évidente, alors $H^1(G, \mathrm{GL}_d(L)) = \{1\}$.*

Démonstration. — Soit $\sigma \to U_\sigma$ un cocycle et $M \in \mathrm{M}_d(L)$ quelconque. Considérons la « série de Poincaré »

$$P_M = \sum_{\tau\in G} U_\tau\tau(M).$$

Si $\sigma \in G$, alors

$$U_\sigma\sigma(P_M) = U_\sigma \sum_{\tau\in G} \sigma(U_\tau)\sigma\tau(M) = \sum_{\tau\in G} U_{\sigma\tau}\sigma\tau(M) = P_M$$

et pour démontrer que U_σ est cohomologue au cocycle trivial, il suffit de prouver que l'on peut trouver M de telle sorte que P_M soit inversible.

Si $x \in L^d$, soit $P(x) = \sum_{\tau\in G} U_\tau\tau(x)$. Les $P(x)$ engendrent L^d (vu en tant que L-espace vectoriel) car si ℓ est une forme linéaire sur L^d telle que $\ell(P(x)) = 0$ quel que soit $x \in L^d$, alors, prenant x de la forme λy, avec $\lambda \in L$, on obtient

$$\sum_{\tau\in G} \tau(\lambda)\ell(U_\tau(\tau(x))) = 0$$

quels que soient $y \in L^d$ et $\lambda \in L$. D'après le lemme d'indépendance linéaire des caractères (on peut voit τ comme un caractère de L^*), ceci implique $\ell(U_\tau(\tau(x))) = 0$ quels que soient $\tau \in G$ et $y \in L^d$ et donc $\ell = 0$ car U_τ et τ sont inversibles.

Soient alors $x_1, \dots, x_d \in L^d$ tels que $P(x_1), \dots, P(x_d)$ forment une base de L^d sur L et soit M la matrice de l'endomorphisme de L^d envoyant le i-ème vecteur e_i de la base canonique de L^d sur x_i. Par construction, on a $P_M(e_i) = P(x_i)$, ce qui implique que P_M est inversible et permet de conclure.

Remarque 2.4. — Si L est infini, on peut se contenter de considérer les matrices M diagonales et poser, si $\alpha \in L$, $P_\alpha = \sum_{\tau\in G} \tau(\alpha)U_\tau$. Le même calcul que précédemment montre que l'on a $U_\sigma\sigma(P_\alpha) = P_\alpha$ et le problème est de montrer que l'on peut trouver α de telle sorte que P_α soit inversible. Or $\det(\sum_{\tau\in G} X_\tau U_\tau)$ vu comme polynôme en les variables X_τ n'est pas identiquement nul puisque les U_τ sont inversibles et on peut utiliser le théorème d'Artin d'indépendance algébrique des automorphismes d'un corps infini pour conclure.

Proposition 2.5. — *Sous les mêmes hypothèses que le théorème précédent, on a*

(i) $H^1(G, L^*) = \{1\}$

(ii) $H^1(G, L) = \{1\}$.

Démonstration. — Le (i) correspond au cas $d=1$ du théorème précédent. Passons au (ii). Soit $\sigma \to c_\sigma$ un cocycle sur G à valeurs dans L [la loi de groupe sur L étant écrite additivement, la relation de cocycle devient $c_{\sigma\tau} = c_\sigma + \sigma(c_\tau)$]. Soit $U_\sigma = \left(\begin{smallmatrix} 1 & c_\sigma \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(L)$. On a

$$U_{\sigma\tau} = \left(\begin{smallmatrix} 1 & c_{\sigma\tau} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & c_\sigma+\sigma(c_\tau) \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & c_\sigma \\ 0 & 1 \end{smallmatrix}\right)\sigma\big(\left(\begin{smallmatrix} 1 & c_\tau \\ 0 & 1 \end{smallmatrix}\right)\big) = U_\sigma\sigma(U_\tau)$$

et $\sigma \to U_\sigma$ est un cocycle sur G à valeurs dans $\mathrm{GL}_2(L)$. Comme $H^1(G, \mathrm{GL}_2(L)) = \{1\}$ d'après le théorème de Hilbert 90, il existe $A = \left(\begin{smallmatrix} a_1 & a_2 \\ b_1 & b_2 \end{smallmatrix}\right) \in \mathrm{GL}_2(L)$ telle que l'on ait $A = U_\sigma\sigma(A)$ quel que soit $\sigma \in G$. On obtient donc

$$\left(\begin{smallmatrix} a_1 & a_2 \\ b_1 & b_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & c_{\sigma\tau} \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \sigma(a_1) & \sigma(a_2) \\ \sigma(b_1) & \sigma(b_2) \end{smallmatrix}\right) = \left(\begin{smallmatrix} \sigma(a_1)+c_\sigma\sigma(b_1) & \sigma(a_2)+c_\sigma\sigma(b_2) \\ \sigma(b_1) & \sigma(b_2) \end{smallmatrix}\right)$$

et comme il existe $i \in \{1,2\}$ tel que $b_i \neq 0$ puisque A est inversible, on obtient $\frac{a_i}{b_i} = \sigma\big(\frac{a_i}{b_i}\big) + c_\sigma$, ce qui prouve que $\sigma \to c_\sigma$ est cohomologue au cocycle trivial.

Corollaire 2.6. — *Soit L une extension galoisienne (pas nécessairement finie) de F et $G = \mathrm{Gal}(L/F)$. L'action naturelle de G sur L, L^* et $\mathrm{GL}_d(L)$ est continue si on munit ces trois groupes de la topologie discrète et*
(i) $H^1(G, L) = \{1\}$
(ii) $H^1(G, L^*) = \{1\}$
(iii) $H^1(G, \mathrm{GL}_d(L)) = \{1\}$.

Démonstration. — Soit $X \in \{L,\ L^*,\ \mathrm{GL}_d(L)\}$ et $x \in X$. Comme x est définie sur une extension finie K de F, l'action de G sur X est constante modulo $\mathrm{Gal}(L/K)$ et donc localement constante (i.e continue pour la topologie discrète). D'autre part, si $\sigma \to c_\sigma$ est un cocycle sur G continu pour la topologie discrète, il existe une extension galoisienne finie K de F telle que l'on ait $c_\sigma = 1$ si $\sigma \in \mathrm{Gal}(L/K)$. Il résulte de la suite d'inflation restriction que $\sigma \to c_\sigma$ provient par inflation d'un cocycle sur $\mathrm{Gal}(K/F)$ à valeurs dans $X^{\mathrm{Gal}(L/K)} = K$ (resp. K^*, resp. $\mathrm{GL}_d(K)$) et est donc cohomologue au cocycle trivial d'après le théorème 2.3 ou la proposition 2.5.

2.2. Anneaux G_K-réguliers et représentations B-admissibles. — Soit K une extension finie de $\mathbf{Q}_p$. Notre problème est de comprendre le groupe G_K via l'étude de ses représentations p-adiques. Pour mettre un peu d'ordre dans les représentations p-adiques de G_K, l'idée de Fontaine est de construire des anneaux B munis d'actions de G_K et de structures additionnelles respectées par l'action de G_K. Chacun de ces anneaux permet de découper dans l'ensemble des représentations p-adiques de G_K celles qui sont B-admissible (i.e. qui deviennent triviales quand on étend les scalaires à B). Si V est une représentation B-admissible de G_K, le B^{G_K}-module $(B \otimes V)^{\mathrm{G}_K}$ est libre de rang $\dim_{\mathbf{Q}_p} V$ et est muni de toutes les structures additionnelles de B respectées par l'action de G_K. Ceci permet d'associer aux représentations de G_K des invariants plus maniables (en général des objets provenant de l'algèbre linéaire) et, si l'anneau B est assez fin (i.e a suffisamment de structures respectées par G_K) de classifier les représentations B-admissibles en termes de ces invariants. Cette approche a l'avantage de ramener l'étude de toutes les représentations B-admissibles à celle de l'anneau B.

Définition 2.7. — Soit G un groupe topologique. Un anneau topologique B est appelé un *G-anneau* s'il est muni d'une action continue de G respectant sa structure d'anneau, c'est-à-dire que l'on a une application continue $(\sigma, x) \to \sigma(x)$ de $G \times B$ dans B vérifiant :
- $\sigma\tau(x) = \sigma(\tau(x))$, quels que soient $\sigma, \tau \in G$ et $x \in B$.

• $\sigma(x+y)=\sigma(x)+\sigma(y)$ et $\sigma(xy)=\sigma(x)\sigma(y)$, quels que soient $\sigma\in G$ et $x,y\in B$.

Remarque 2.8. — Si B est un G-anneau et A est un sous-anneau de B stable par G, alors A est un G-anneau.

Définition 2.9. — Soient G un groupe topologique et B un G-anneau. On appelle *B-représentation* de G un B-module libre W de dimension finie muni d'une action semi-linéaire continue de G, c'est-à-dire que l'on a une application continue $(\sigma,w)\to\sigma(w)$ de $G\times W$ dans W vérifiant :

• $\sigma\tau(w)=\sigma(\tau(w))$, quels que soient $\sigma,\tau\in G$ et $w\in W$.
• $\sigma(w_1+w_2)=\sigma(w_1)+\sigma(w_2)$, quels que soient $\sigma\in G$ et $w_1,w_2\in W$.
• $\sigma(bw)=\sigma(b)\sigma(w)$, quels que soient $\sigma\in G$, $b\in B$ et $w\in W$.

Remarque 2.10. — Si on choisit une base $e_1,\dots,e_d$ de W sur B et que l'on note $U_\sigma=(u_{i,j}^\sigma)$ la matrice des vecteurs $\sigma(e_1),\dots,\sigma(e_d)$ dans la base $e_1,\dots,e_d$ (i.e. $\sigma(e_j)=\sum_{i=1}^d u_{i,j}^\sigma e_i$), les conditions ci-dessus se traduisent par la relation de cocycle $U_{\sigma\tau}=U_\sigma\sigma(U_\tau)$, pour tous $\sigma,\tau\in G$. En particulier, en prenant $\tau=\sigma^{-1}$, on en déduit le fait que U_σ est inversible et que $\sigma\to U_\sigma$ est un cocycle à valeurs dans $\mathrm{GL}_d(B)$. D'autre part, si on choisit une autre base $f_1,\dots,f_d$ de W sur B et que l'on note $M=(m_{i,j})$ la matrice de passage et U'_σ la matrice de $\sigma(f_1),\dots,\sigma(f_d)$ dans la base $f_1,\dots,f_d$, on a $U'_\sigma=M^{-1}U_\sigma\sigma(M)$, ce qui montre que les cocycles associés à deux bases différentes sont cohomologues. Ceci permet d'associer à toute B-représentation de G de dimension d un élément de $H^1(G,\mathrm{GL}_d(B))$.

Définition 2.11. — (i) On dit qu'une B-représentation de dimension d de G est *B-admissible* si la classe de cohomologie dans $H^1(G,\mathrm{GL}_d(B))$ qui lui est associée est triviale.

(ii) Plus généralement, si A est un sous-anneau de B stable par G, et si W *une A-représentation de* G, on munit $B\otimes_A W$ d'une structure de B-représentation donnée par $\sigma(b\otimes w)=\sigma(b)\otimes\sigma(w)$, et on dit que W *est B-admissible si la B-représentation $B\otimes_A W$ est B-admissible.*

Théorème 2.12. — *Soit K une extension finie de $\mathbf{Q}_p$. Une $\mathbf{Q}_p$-représentation de G_K est $\overline{\mathbf{Q}}_p$-admissible si et seulement si G_K agit à travers un quotient fini.*

Démonstration. — Soit $d=\dim_{\mathbf{Q}_p}V$ et soit $e_1,\dots,e_d$ une base de V sur $\mathbf{Q}_p$. Si V est $\overline{\mathbf{Q}}_p$ admissible, on peut trouver une base $v_1,\dots,v_d$ de $\overline{\mathbf{Q}}_p\otimes V$ sur $\overline{\mathbf{Q}}_p$ stable par G_K. Si on décompose e_i dans la base $v_1,\dots,v_d$ sous la forme $e_i=\sum_{j=1}^d a_{i,j}v_j$ avec $a_{i,j}\in\overline{\mathbf{Q}}_p$ et que l'on considère une extension galoisienne finie de K contenant les $a_{i,j}$ pour $1\leqslant i,j\leqslant d$, il est clair que l'action de G_K sur les e_i (et donc sur V tout entier par linéarité) se factorise à travers $\mathrm{Gal}(L/K)$.

Réciproquement, l'hypothèse selon laquelle l'action de G_K se factorise à travers un quotient finie est équivalente au fait que ce cocycle est continu si on munit $\mathrm{GL}_d(\overline{\mathbf{Q}}_p)$ de la topologie discrète et le résultat suit de ce que $H^1(\mathrm{G}_K,\mathrm{GL}_d(\overline{\mathbf{Q}}_p))=\{1\}$, d'après le corollaire 2.6.

Remarque 2.13. — Soit $e_1,\dots,e_d$ une base de W sur A. Notons comme d'habitude $U_\sigma=(u_{i,j}^\sigma)$ la matrice des vecteurs $\sigma(e_1),\dots,\sigma(e_d)$ dans la base $e_1,\dots,e_d$. Si W est B-admissible, c'est, par définition, qu'il existe $M=(m_{i,j})\in\mathrm{GL}_d(B)$ telle que l'on ait $M^{-1}U_\sigma\sigma(M)=1$ quel que soit

$\sigma \in G$, ce qui fait que si l'on pose $v_k = \sum_{j=1}^d m_{j,k}e_j$, on a

$$\sigma(v_k) = \sum_{j=1}^d \sigma(m_{j,k}\sigma(e_j) = \sum_{i=1}^d \Big(\sum_{j=1}^d u_{i,j}^\sigma \sigma(m_{j,k})\Big)e_i = v_k$$

et les vecteurs $v_1, \dots, v_d$ forment une base de $B \otimes_A W$ sur B (puisque M est inversible) formée de vecteurs invariants par G.

On en déduit le fait que $D_B(W) = (B \otimes_A W)^G$ est le B^G-module libre engendré par $v_1, \dots, v_d$ et que l'application naturelle $\alpha_B : B \otimes_{B^G} D_B(W) \to B \otimes_A W$ est un isomorphisme commutant à l'action de G.

Définition 2.14. — (i) On dit qu'un G-anneau topologique est *G-pseudo-régulier* s'il est intègre et si $B^G = \mathrm{Frac}(B)^G$. Remarquons que ceci implique que B^G est un corps.

(ii) Soient B un G-anneau G-pseudo-régulier et A un sous-anneau de B stable par G. On dit que B est *(G, A)-régulier* si la condition « $x \neq 0$ et $\sigma(x) = a_\sigma x$, avec $a_\sigma \in A^*$, pour tout $\sigma \in G$ » implique $x \in B^*$. On dit que B est *G-régulier* s'il est (G, B)-régulier.

Remarque 2.15. — Un G-anneau qui est un corps est automatiquement G-régulier.

Proposition 2.16. — *Soient $A \subset B$ des G-anneaux et W une A-représentation de G.*

(i) *Si B est G-pseudo-régulier, l'application $\alpha_B : B \otimes_{B^G} D_B(W) \longrightarrow B \otimes_A W$ est injective et $\dim_{B^G}(D_B(W)) \leqslant \dim_A W$.*

(ii) *Si B est (G, A)-régulier, les trois conditions suivantes sont équivalentes :*

(a) *W est B-admissible*

(b) *$\dim_{B^G}(D_B(W)) = \dim_A W$.*

(c) *$\alpha_B : B \otimes_{B^G} D_B(W) \longrightarrow B \otimes_A W$ est un isomorphisme.*

Démonstration. — (i) Soient $v_1, \dots, v_n$ des éléments de $D_B(W)$ formant une famille libre sur B^G. Montrons qu'ils forment encore une famille libre sur B. Supposons le contraire et soit $\sum_{i=1}^n b_i v_i = 0$ une combinaison linéaire minimale entre les v_i. Quitte à étendre les scalaires à $\mathrm{Frac}(B)$, on peut tout diviser par b_1 et donc supposer que $b_1 = 1$. Appliquant alors $\sigma \in G$ à la combinaison linéaire et utilisant le fait que les v_i sont fixes par G, on obtient

$$\sum_{i=2}^n (\sigma(b_i) - b_i)v_i = 0,$$

ce qui, compte-tenu de la minimalité de la combinaison linéaire initiale, implique $b_i \in \mathrm{Frac}(B)^G = B^G$ et est en contradiction avec le fait que les v_i sont libres sur B^G. L'injectivité de α_B et l'inégalité $\dim_{B^G}(D_B(W)) \leqslant \dim_A W$ s'en déduisent.

(ii) On a déjà vu (remarque 2.13) que (a) implique (b) et (c). D'autre part (c) implique (b) de manière évidente si on considère les dimensions sur B des espaces de départ et d'arrivée de α_B. Il ne reste donc qu'à vérifier que (b) implique (a). Soit $d = \dim_A W$. Il s'agit de montrer qu'une base $v_1, \dots, v_d$ de $D_B(W)$ sur B^G est aussi une base de $B \otimes_A W$ sur B. Soit $e_1, \dots, e_d$ une base de W sur A et $v_j = \sum_{i=1}^d b_{i,j}e_i$ la décomposition de v_j dans la base $e_1, \dots, e_d$ de $B \otimes_A W$. Soit Δ le déterminant de la matrice $(b_{i,j})$. Comme B est G-pseudo-régulier et que les v_j sont libres sur B^G, Δ est un élément de B non nul d'après le (i). D'autre part, le fait que les v_j sont fixes par G se traduit par la formule $\Delta = \sigma(\Delta) \det \sigma$, où $\det \sigma \in A^*$ est le déterminant de la matrice des $\sigma(e_i)$ dans la base des e_i et comme on a supposé que B est (G,A)-régulier, ceci implique $\Delta\in B^*$ et la matrice $(b_{i,j})$ est inversible, ce qui permet de conclure.

2.3. Représentations galoisiennes et φ-modules. — Soient κ un corps de caractéristique p tel que $[\kappa:\kappa^p]<+\infty$, κ^{s} sa clôture séparable, $G=\mathrm{Gal}(\kappa^{\mathrm{s}}/\kappa)$, A^{s} un p-anneau strict d'anneau résiduel κ^{s} (et donc A^{s} est de valuation discrète, puisque κ^{s} est un corps), muni d'une action continue de G compatible avec celle sur κ^{s} par réduction modulo p, et d'un frobenius φ commutant à l'action de G et induisant $x\mapsto x^p$ sur κ^{s} par réduction modulo p (donc $(A^{\mathrm{s}})^{\varphi=1}=\mathbf{Z}_p$). On pose $A=(A^{\mathrm{s}})^G$; alors A est stable par φ et est un p-anneau strict d'anneau résiduel κ. Les exemples que nous avons en vue sont :

- $\kappa=\mathbf{F}_p$, $\kappa^{\mathrm{s}}=\overline{\mathbf{F}}_p$, $G=\widehat{\mathbf{Z}}$, $A^{\mathrm{s}}=W(\overline{\mathbf{F}}_p)$ et $A=\mathbf{Z}_p$,
- $\kappa=\mathbf{E}_{\mathbf{Q}_p}$, $\kappa^{\mathrm{s}}=\mathbf{E}$, $G=\mathrm{H}_{\mathbf{Q}_p}$, $A^{\mathrm{s}}=\mathbf{A}$ et $A=\mathbf{A}_{\mathbf{Q}_p}$,
- plus généralement, si $[K:\mathbf{Q}_p]<+\infty$, $\kappa=\mathbf{E}_K$, $\kappa^{\mathrm{s}}=\mathbf{E}$, $G=\mathrm{H}_K$, $A^{\mathrm{s}}=\mathbf{A}$ et $A=\mathbf{A}_K$.

Soit $\mathrm{Rep}_{\mathrm{tors}}G$ la catégorie des $\mathbf{Z}_p$-modules de longueur finie munis d'une action linéaire continue de G. Si $V\in\mathrm{Rep}_{\mathrm{tors}}G$, soit $D(V)=(A^{\mathrm{s}}\otimes V)^G$, où $\sigma\in G$ agit par $\sigma\cdot(a\otimes v)=\sigma(a)\otimes\sigma(v)$; c'est un A-module puisque $(A^{\mathrm{s}})^G=A$.

Proposition 2.17. — (i) *Si $V\in\mathrm{Rep}_{\mathrm{tors}}G$, l'application naturelle $A^{\mathrm{s}}\otimes_A D(V)\to A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V$ est un isomorphisme.*

(ii) $H^1(G,A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V)=0$.

(iii) *Si $0\to V'\to V\to V''\to 0$ est une suite exacte dans $\mathrm{Rep}_{\mathrm{tors}}G$, la suite*
$$0\to D(V')\to D(V)\to D(V'')\to 0$$
est exacte

Démonstration. — Si V est tué par p, on a $A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V=\kappa^{\mathrm{s}}\otimes_{\mathbf{F}_p}V$ et $A^{\mathrm{s}}\otimes_A D(V)=\kappa^{\mathrm{s}}\otimes_\kappa V$; le (i) est donc une conséquence de la trivialité de $H^1(G,\mathrm{GL}_d(\kappa^{\mathrm{s}}))$ et de $(\kappa^{\mathrm{s}})^G=\kappa$, et le (ii) est alors une conséquence du (i) et de la trivialité de $H^1(G,\kappa^{\mathrm{s}})$.

D'autre part, si $0\to V'\to V\to V''\to 0$ est exacte, et si V' et V'' vérifient les (i) et (ii), la suite exacte de cohomologie
$$0\to D(V')\to D(V)\to D(V'')\to H^1(G,A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V')\to H^1(G,A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V)\to H^1(G,A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V'')$$
montre que $H^1(G,A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V)=0$ et que la suite $0\to D(V')\to D(V)\to D(V'')\to 0$ est exacte. De plus, dans le diagramme commutatif
$$\begin{tikzcd}
0 \arrow[r] & A^{\mathrm{s}}\otimes_A D(V') \arrow[r]\arrow[d,"\iota'"] & A^{\mathrm{s}}\otimes_A D(V) \arrow[r]\arrow[d,"\iota"] & A^{\mathrm{s}}\otimes_A D(V'') \arrow[r]\arrow[d,"\iota''"] & 0\\
0 \arrow[r] & A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V' \arrow[r] & A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V \arrow[r] & A^{\mathrm{s}}\otimes_{\mathbf{Z}_p}V'' \arrow[r] & 0
\end{tikzcd}$$
les lignes sont exactes car A^{s} est plat sur $\mathbf{Z}_p$ et A (car sans p-torsion) et ι' et ι'' sont des isomorphismes par hypothèse ; il en est donc de même de ι. On en déduit le résultat par récurrence sur la longueur de V.

Remarque 2.18. — Le A-module $D(V)$ est de longueur finie et est muni d'une action d'un frobenius φ induite par celle de $\varphi\otimes 1$ sur $A^{\mathrm{s}}\otimes V$ (qui commute à celle de G). Cette action est semi-linéaire par rapport à l'action de φ sur A. De plus, $\varphi(\kappa^{\mathrm{s}})$ engendre κ^{s} en tant que κ espace vecoriel (grâce à l'hypothèse $[\kappa : \kappa^p] < +\infty$), et donc $\varphi(A^{\mathrm{s}})$ engendre A^{s} en tant que A-module. Il résulte donc du (i) de la proposition que $\varphi(D(V))$ engendre $D(V)$ en tant que A-module. En d'autres termes, $D(V)$ est un objet de la catégorie $\Phi^{\mathrm{et}}_{\mathrm{tors}}(A)$ des *φ-modules étales* de torsion sur A.

Lemme 2.19. — *Si $B \in \mathrm{GL}_d(\kappa^{\mathrm{s}})$, l'ensemble V des solutions $v \in (\kappa^{\mathrm{s}})^d$ de l'équation $\varphi(v) = Bv$ est un $\mathbf{F}_p$-espace vectoriel de dimension d dont une base sur $\mathbf{F}_p$ est aussi une base de $(\kappa^{\mathrm{s}})^d$ sur κ^{s}.*

Démonstration. — Si $B = (b_{i,j})_{1\leqslant i,j\leqslant d}$, on cherche les d-uplets $(x_1, \dots, x_d) \in (\kappa^{\mathrm{s}})^d$ tels que l'on ait

$$x_i^p = \sum_{j=1}^d b_{i,j}x_j \quad \text{si } 1 \leqslant i \leqslant d.$$

Ces d-uplets forment de manière évidente un sous-$\mathbf{F}_p$-espace vectoriel V de $(\kappa^{\mathrm{s}})^d$. D'autre part, si $\Lambda = \kappa^{\mathrm{s}}[X_1, \dots, X_d]/(X_i^p - \sum_{j=1}^d b_{i,j}X_j)_{1\leqslant i\leqslant d}$, V est en bijection avec les morphismes de κ^{s}-algèbres de Λ dans κ^{s}. Maintenant, Λ est de dimension p^d sur κ^{s} de base les $X_1^{k_1} \cdots X_d^{k_d}$, avec $0 \leqslant k_i \leqslant p-1$ si $1 \leqslant i \leqslant d$, et on est ramené à prouver que $\Lambda \cong (\kappa^{\mathrm{s}})^{p^d}$ en tant que κ^{s}-algèbre. Soit $\overline{\kappa}$ la clôture algébrique de κ (c'est aussi la clôture radicielle de κ^{s}). Alors $\overline{\kappa} \otimes_{\kappa^{\mathrm{s}}} \Lambda \cong \prod_j \overline{\kappa}[X]/X^{a_j}$, où les a_j sont des entiers dont la somme vaut p^d. Si un des a_j est $\geqslant 2$, l'algèbre $\overline{\kappa} \otimes_{\kappa^{\mathrm{s}}} \Lambda$ a un quotient isomorphe à $\overline{\kappa}[X]/X^2$; il existe donc une solution $(x_1, \dots, x_d)$ du système ci-dessus qui se relève en une solution $(\tilde{x}_1, \dots, \tilde{x}_d)$, où $\tilde{x}_i = x_i + y_iX$ est l'image de X_i par le morphisme surjectif $\overline{\kappa} \otimes_{\kappa^{\mathrm{s}}} \Lambda \to \overline{\kappa}[X]/X^2$. Or on a $\tilde{x}_i^p = x_i^p$ dans $\overline{\kappa}[X]/X^{a_j}$; le fait que $(x_1, \dots, x_d)$ et $(\tilde{x}_1, \dots, \tilde{x}_d)$ soient solutions du système se traduit par $\sum_{j=1}^d b_{i,j}y_j = 0$, pour tout $1 \leqslant i \leqslant d$, et l'inversibilité de B implique que les y_j sont tous nuls. Ceci implique que l'image du morphisme $\overline{\kappa} \otimes_{\kappa^{\mathrm{s}}} \Lambda \to \overline{\kappa}[X]/X^2$ est incluse dans $\overline{\kappa}$, en contradiction avec sa surjectivité. Il en résulte que les a_j sont tous égaux à 1 et qu'il y a p^d morphismes distincts de Λ dans $\overline{\kappa}$. Or $\overline{\kappa}$ est la réunion des $(\kappa^{\mathrm{s}})^{p^{-n}}$ et l'inversibilité de B montre que l'appartenance des x_i à $(\kappa^{\mathrm{s}})^{p^{-n}}$ implique leur appartenance à $(\kappa^{\mathrm{s}})^{p^{1-n}}$, si $n \geqslant 1$. Il en résulte que tout morphisme de Λ dans $\overline{\kappa}$ est à valeurs dans κ^{s}, que V est de cardinal p^d et donc de dimension d sur $\mathbf{F}_p$.

Pour conclure, il suffit donc de démontrer que si $v_1, \dots, v_d$ sont des éléments de V qui sont liés sur κ^{s}, alors ils le sont déjà sur $\mathbf{F}_p$. Soit donc $\alpha_1v_1 + \cdots + \alpha_rv_r$ une relation minimale entre les v_i. Quitte à tout diviser par α_1, on peut supposer $\alpha_1 = 1$. Appliquant $B^{-1}\varphi$ à la relation, on obtient une nouvelle relation, à savoir, $\varphi(\alpha_1)v_1 + \cdots + \varphi(\alpha_r)v_r$. Comme on avait supposé la relation initiale minimale et que $\varphi(\alpha_1) = \alpha_1 = 1$, tous les coefficients de la relation $(\varphi(\alpha_2)-\alpha_2)v_2+\cdots+(\varphi(\alpha_r)-\alpha_r)v_r = 0$ sont nuls, ce qui implique que $\varphi(\alpha_i) = \alpha_i$ (i.e $\alpha_i \in \mathbf{F}_p$), quel que soit $1 \leqslant i \leqslant d$. Ceci permet de conclure.

Si D est un objet de $\Phi^{\mathrm{et}}_{\mathrm{tors}}(A)$, soit $V(D) = (A^{\mathrm{s}} \otimes D)^{\varphi=1}$, où φ agit par $\varphi \otimes \varphi$; c'est un $\mathbf{Z}_p$-module puisque $(A^{\mathrm{s}})^{\varphi=1} = \mathbf{Z}_p$.

Proposition 2.20. — (i) *Si D est un φ-module étale sur A, l'application naturelle $A^{\mathrm{s}} \otimes_{\mathbf{Z}_p} V(D) \to A^{\mathrm{s}} \otimes_A D$ est un isomorphisme.*

(ii) *L'application $1-\varphi : A^{\mathrm{s}} \otimes_A D \to A^{\mathrm{s}} \otimes_A D$ est surjective*

(iii) *Si $0 \to D' \to D \to D'' \to 0$ est une suite exacte de φ-modules étales sur A, alors la suite*

$$0 \to V(D') \to V(D) \to V(D'') \to 0$$

est exacte

Démonstration. — Si D est tué par p, on a $A^{\mathrm{s}}\otimes_A D=\kappa^{\mathrm{s}}\otimes_\kappa D$ et $A^{\mathrm{s}}\otimes_{\mathbf{Z}_p} V(D)=\kappa^{\mathrm{s}}\otimes_{\mathbf{F}_p} V(D)$. Si on choisit une base de D sur κ, la matrice de φ dans cette base appartient à $\mathrm{GL}_d(\kappa)\subset\mathrm{GL}_d(\kappa^{\mathrm{s}})$ et le (i) a été traité dans le lemme 2.19. Le (ii) quant à lui est alors une conséquence du (i) et de la surjectivité de $1-\varphi:\kappa^{\mathrm{s}}\to\kappa^{\mathrm{s}}$ (c'est juste $x\mapsto x-x^p$ et κ^{s} est séparablement clos).

D'autre part, si $0\to D'\to D\to D''\to 0$ est une suite exacte de φ-modules étales sur A et si D' et D'' vérifient les (i) et (ii), le lemme du serpent

$$0\to V(D')\to V(D)\to V(D'')\to A^{\mathrm{s}}\otimes_A D'/(1-\varphi)\to A^{\mathrm{s}}\otimes_A D/(1-\varphi)\to A^{\mathrm{s}}\otimes_A D''/(1-\varphi)$$

montre que $1-\varphi$ est surjectif sur $A^{\mathrm{s}}\otimes_A D$ et que la suite $0\to V(D')\to V(D)\to V(D'')\to 0$ est exacte. De plus, dans le diagramme commutatif

$$\begin{tikzcd}
0 \arrow[r] & A^{\mathrm{s}}\otimes_{\mathbf{Z}_p} V(D') \arrow[r] \arrow[d, "\iota'"] & A^{\mathrm{s}}\otimes_{\mathbf{Z}_p} V(D) \arrow[r] \arrow[d, "\iota"] & A^{\mathrm{s}}\otimes_{\mathbf{Z}_p} V(D'') \arrow[r] \arrow[d, "\iota''"] & 0 \\
0 \arrow[r] & A^{\mathrm{s}}\otimes_A D' \arrow[r] & A^{\mathrm{s}}\otimes_A D \arrow[r] & A^{\mathrm{s}}\otimes_A D'' \arrow[r] & 0
\end{tikzcd}$$

les lignes sont exactes car A^{s} est plat sur $\mathbf{Z}_p$ et A (car sans p-torsion) et ι' et ι'' sont des isomorphismes par hypothèse ; il en est donc de même de ι. On en déduit le résultat par récurrence sur la longueur de D.

Remarque 2.21. — Le $\mathbf{Z}_p$-module $V(D)$ est de longueur finie et est muni d'une action linéaire continue de G déduite de l'action $\sigma\otimes 1$ sur $A^{\mathrm{s}}\otimes_A D$ (qui commute à l'action de φ. Autrement dit, $V(D)$ est un objet de $\mathrm{Rep}_{\mathrm{tors}}G$. On déduit alors du (i) des prop. 2.17 et 2.20 que les foncteurs $D\mapsto V(D)$ et $V\mapsto D(V)$ sont inverses l'un de l'autre ; de plus, ces foncteurs sont exacts d'après les (iii) des prop. 2.17 et 2.20 ; ils induisent donc un équivalence de catégorie $\mathrm{Rep}_{\mathrm{tors}}G\cong\Phi^{\mathrm{et}}_{\mathrm{tors}}(A)$.

2.4. Représentations galoisiennes et (φ,Γ)-modules

2.4.1. Représentations p-adiques de $\mathrm{G}_{\mathbf{Q}_p}$. — Notons :

- $\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}$ la catégorie des $\mathscr{O}_L$-modules de longueur finie, munis d'une action linéaire continue de $\mathrm{G}_{\mathbf{Q}_p}$,
- $\mathrm{Rep}_{\mathscr{O}_L}\mathrm{G}_{\mathbf{Q}_p}$ la catégorie des $\mathscr{O}_L$-modules libres de rang fini, munis d'une action linéaire continue de $\mathrm{G}_{\mathbf{Q}_p}$,
- $\mathrm{Rep}_L\mathrm{G}_{\mathbf{Q}_p}$ la catégorie des L-espaces vectoriels de dimension finie, munis d'une action linéaire continue de $\mathrm{G}_{\mathbf{Q}_p}$.

Si V est un objet de $\mathrm{Rep}_{\mathscr{O}_L}\mathrm{G}_{\mathbf{Q}_p}$, alors V/p^kV est un objet de $\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}$ pour tout k, et V est la limite projective des V/p^kV. Si V est un objet de $\mathrm{Rep}_L\mathrm{G}_{\mathbf{Q}_p}$, alors V possède des $\mathscr{O}_L$-réseaux stables par $\mathrm{G}_{\mathbf{Q}_p}$ (par compacité de $\mathrm{G}_{\mathbf{Q}_p}$), et si V_0 est un de ces réseaux, on a $V=L\otimes_{\mathscr{O}_L}V_0$.

Proposition 2.22. — *Toute $\mathbf{Q}_p$-représentation d'un groupe compact G admet un $\mathbf{Z}_p$-réseau stable par G.*

Soit $e_1,\dots,e_d$ une base de V sur $\mathbf{Q}_p$ et soit $\Lambda=\mathbf{Z}_pe_1\oplus\cdots\oplus\mathbf{Z}_pe_d$. Si $\sigma\in G$, soit $U_\sigma=(a_{i,j,\sigma})_{1\leqslant i,j\leqslant d}$ la matrice de σ dans la base $e_1,\dots,e_d$ (c'est-à-dire $\sigma(e_i)=\sum_{j=1}^d a_{j,i}e_j$). L'application $\sigma\to U_\sigma$ étant continue et G étant compact, il existe $n\in\mathbf{N}$ tel que $a_{i,j,\sigma}\in p^{-n}\mathbf{Z}_p$ quel que soient $1\leqslant i,j\leqslant d$ et $\sigma\in G$. On a donc $\sigma(\Lambda)\subset p^{-n}\Lambda$, pour tout $\sigma\in G$, ce qui implique que

$T = \sum_{\sigma\in G}\sigma(\Lambda)$ est un réseau de V ; comme il est stable par G par construction, cela permet de conclure.

Dans la suite,

• une *$\mathscr{O}_L$-représentation de* $\mathrm{G}_{\mathbf{Q}_p}$ désigne un objet de $\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}$ ou de $\mathrm{Rep}_{\mathscr{O}_L}\mathrm{G}_{\mathbf{Q}_p}$,

• une *représentation p-adique de* $\mathrm{G}_{\mathbf{Q}_p}$ désigne un objet de $\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}$, de $\mathrm{Rep}_{\mathscr{O}_L}\mathrm{G}_{\mathbf{Q}_p}$ ou de $\mathrm{Rep}_L\mathrm{G}_{\mathbf{Q}_p}$.

Théorème 2.23. — (Fontaine)

(i) *Si D est un (φ,Γ)-module étale, alors* $\mathbf{V}(D) = ((\mathscr{O}_L\otimes_{\mathbf{Z}_p}\mathbf{A})\otimes_{\mathscr{O}_{\mathscr{E}}} D)^{\varphi=1}$, *est une $\mathscr{O}_L$ (resp. L)-représentation p-adique de* $\mathrm{G}_{\mathbf{Q}_p}$.

(ii) *Si V est une représentation p-adique de* $\mathrm{G}_{\mathbf{Q}_p}$, *alors* $\mathbf{D}(V) = (\mathbf{A}\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}}$ *est un (φ,Γ)-module étale.*

(iii) *Les foncteurs* $\mathbf{V}$ *et* $\mathbf{D}$ *sont exacts, inverses l'un de l'autre, et induisent des équivalences de catégories :*

$$\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}\cong\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}},\quad \mathrm{Rep}_{\mathscr{O}_L}\mathrm{G}_{\mathbf{Q}_p}\cong\Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})\quad\text{et}\quad \mathrm{Rep}_L\mathrm{G}_{\mathbf{Q}_p}\cong\Phi\Gamma^{\mathrm{et}}(\mathscr{E}).$$

Démonstration. — Dans le cas d'objets de torsion, cela résulte de la rem. 2.21 (si le corps des coefficients L est $\mathbf{Q}_p$) ; l'action de Γ sur $\mathbf{D}(V)$ venant du fait que l'on n'a pris les points fixes que sous l'action de H et donc qu'il reste une action résiduelle de $\mathrm{G}_{\mathbf{Q}_p}/\mathrm{H}$; dans l'autre sens, on obtient, sur $\mathbf{V}(D)$, une action de $\mathrm{G}_{\mathbf{Q}_p}$ et pas seulement de H, car D est muni d'une action de $\mathrm{G}_{\mathbf{Q}_p}$ agissant à travers son quotient Γ, et que $\mathbf{A}$ est muni d'une action de $\mathrm{G}_{\mathbf{Q}_p}$. Le cas de coefficients généraux s'obtient en remarquant qu'une $\mathscr{O}_L$-représentation de $\mathrm{G}_{\mathbf{Q}_p}$ est une $\mathbf{Z}_p$-représentation de $\mathrm{G}_{\mathbf{Q}_p}$ munie d'une action de $\mathscr{O}_L$, qui est $\mathbf{Z}_p$-linéaire et commute à celle de G, ce qui munit $\mathbf{D}(V)$ d'une action $\mathbf{Z}_p$-linéaire de $\mathscr{O}_L$ qui commute à celles de φ et Γ ; l'argument est le même pour munir $\mathbf{V}(D)$ d'une action de $\mathscr{O}_L$ si D l'est.

Le cas des $\mathscr{O}_L$-modules sans torsion s'en déduit par passage à la limite projective ; le cas des L-espaces vectoriels en inversant p.

Remarque 2.24. — (i) Le résultat ci-dessus s'étend aux représentations de G_K, où $[K:\mathbf{Q}_p]<+\infty$, en remplaçant les (φ,Γ)-modules sur $\mathscr{O}_{\mathscr{E}}$ ou $\mathscr{E}$ par des (φ,Γ)-modules sur $\mathscr{O}_L\otimes_{\mathbf{Z}_p}\mathbf{A}_K$ ou $\mathscr{O}_L\otimes_{\mathbf{Z}_p}\mathbf{B}_K$.

(ii) 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 $\mathrm{G}_{\mathbf{Q}}$.

On rappelle que χ désigne le caractère cyclotomique. On définit le *dual de Tate* $\check{V}$ d'une représentation p-adique V de $\mathrm{G}_{\mathbf{Q}_p}$ par :

• $\check{V}=\mathrm{Hom}(V,(L/\mathscr{O}_L)\otimes\chi)$, si $V\in\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}$,

• $\check{V} = \mathrm{Hom}(V, \mathscr{O}_L \otimes \chi)$, si $V \in \mathrm{Rep}_{\mathscr{O}_L} \mathrm{G}_{\mathbf{Q}_p}$,
• $\check{V} = \mathrm{Hom}(V, L \otimes \chi)$, si $V \in \mathrm{Rep}_L \mathrm{G}_{\mathbf{Q}_p}$.

Si D est un (φ,Γ)-module étale, et si V est la représentation p-adique de $\mathrm{G}_{\mathbf{Q}_p}$ qui lui correspond, alors la représentation correspondant à $\check{D}$ est $\check{V}$.

2.4.2. Représentations abéliennes de $\mathrm{G}_{\mathbf{Q}_p}$. — D'après la théorie locale du corps de classe, l'extension maximale abélienne $\mathbf{Q}_p^{\mathrm{ab}}$ de $\mathbf{Q}_p$ est la composée de $\mathbf{Q}_p^{\mathrm{nr}}$ et de F_∞. De plus, $\mathbf{Q}_p^{\mathrm{nr}}$ est obtenu en rajoutant à $\mathbf{Q}_p$ les racines de l'unité d'ordre premier à p. L'abélianisé $\mathrm{G}_{\mathbf{Q}_p}^{\mathrm{ab}}$ de $\mathrm{G}_{\mathbf{Q}_p}$ est donc isomorphe au produit des groupes de Galois $\mathrm{Gal}(F_\infty/\mathbf{Q}_p) = \Gamma \cong \mathbf{Z}_p^*$ et $\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{nr}}/\mathbf{Q}_p) = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) = \varphi^{\widehat{\mathbf{Z}}}$; il est donc isomorphe au complété profini $(\mathbf{Q}_p^*)^\wedge$ de $\mathbf{Q}_p^*$. Si $a \in \mathbf{Q}_p \subset (\mathbf{Q}_p^*)^\wedge$, on note σ_a l'élément de $\mathrm{G}_{\mathbf{Q}_p}^{\mathrm{ab}}$ qui lui correspond. Son action est décrite explicitement par les formules suivantes :

• si $a \in \mathbf{Z}_p^*$, alors $\sigma_a(\zeta) = \zeta^a$, si $\zeta \in \boldsymbol{\mu}_{p^\infty}$ et $\sigma_a(\zeta) = \zeta$ si ζ est d'ordre premier à p,
• $\sigma_p(\zeta) = \zeta$, si $\zeta \in \boldsymbol{\mu}_{p^\infty}$ et $\sigma_p(\zeta) = \zeta^p$ si ζ est d'ordre premier à p.

On dit qu'une représentation de $\mathrm{G}_{\mathbf{Q}_p}$ est *abélienne* si elle se factorise par $\mathrm{G}_{\mathbf{Q}_p}^{\mathrm{ab}}$. Comme le quotient de $\mathrm{G}_{\mathbf{Q}_p}^{\mathrm{ab}}$ par $\mathrm{H}_{\mathbf{Q}_p}$ est $\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{nr}}/\mathbf{Q}_p) = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$, on déduit de la rem. 2.21 la version suivante de l'équivalence de catégories de Fontaine.

Proposition 2.25. — *Le foncteur $V \mapsto (W(\overline{\mathbf{F}}_p) \otimes_{\mathbf{Z}_p} V)^{\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)}$ induit une équivalence de catégories entre représentations abéliennes de $\mathrm{G}_{\mathbf{Q}_p}$ et (φ,Γ)-modules étales sur $\mathscr{O}_L$ (ou sur L, si V est une L-représentation).*

2.4.3. Le foncteur $D \mapsto D^{\mathrm{nr}}$ et l'équivalence de catégories de Fontaine. — Soit $\mathrm{H}'_{\mathbf{Q}_p} \subset \mathrm{H}_{\mathbf{Q}_p}$ le groupe de Galois absolu de $\mathbf{Q}_p^{\mathrm{ab}}$. On a donc $\mathrm{G}_{\mathbf{Q}_p}/\mathrm{H}'_{\mathbf{Q}_p} = \mathrm{G}_{\mathbf{Q}_p}^{\mathrm{ab}}$ et $\mathrm{H}_{\mathbf{Q}_p}/\mathrm{H}'_{\mathbf{Q}_p} = \mathrm{Gal}(\mathbf{Q}_p^{\mathrm{nr}}/\mathbf{Q}_p) = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$.

Si V est une représentation p-adique de $\mathrm{G}_{\mathbf{Q}_p}$, soit $\mathbf{D}^{\mathrm{nr}}(V) = (W(\overline{\mathbf{F}}_p) \otimes V)^{\mathrm{H}_{\mathbf{Q}_p}}$.

Lemme 2.26. — *Si V est une représentation de $\mathrm{G}_{\mathbf{Q}_p}$, alors $\mathbf{D}^{\mathrm{nr}}(V) = \mathbf{D}^{\mathrm{nr}}(V^{\mathrm{H}'_{\mathbf{Q}_p}})$.*

Démonstration. — Soient $V_1 = V^{\mathrm{H}'_{\mathbf{Q}_p}}$ et $V_2 = V/V_1$. Il suffit de prouver que $(W(\overline{\mathbf{F}}_p) \otimes V)^{\mathrm{H}'_{\mathbf{Q}_p}} = W(\overline{\mathbf{F}}_p) \otimes V_1$. Supposons le contraire, et soit $X \subset W(\overline{\mathbf{F}}_p) \otimes V_2$ l'ensemble des éléments tués par p dans l'image de $(W(\overline{\mathbf{F}}_p) \otimes V)^{\mathrm{H}'_{\mathbf{Q}_p}}$. Alors X est un $\overline{\mathbf{F}}_p$-espace vectoriel qui est stable par $\mathrm{H}_{\mathbf{Q}_p}/\mathrm{H}'_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$, et qui est non nul sous notre hypothèse. Il résulte du th. de Hilbert 90 que X est de la forme $\overline{\mathbf{F}}_p \otimes V_2'$, où V_2' est fixe par $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ et donc inclus dans V_2. Soit alors $v \in V_2'$. Comme $\mathrm{H}'_{\mathbf{Q}_p}$ agit trivialement sur $W(\overline{\mathbf{F}}_p) \otimes V_1$, cela implique que $\sigma(\tilde{v}) - \tilde{v}$ ne dépend pas du choix de relèvement de v dans $W(\overline{\mathbf{F}}_p) \otimes V$. Or, par hypothèse, v admet relèvement fixe par $\mathrm{H}'_{\mathbf{Q}_p}$, et donc tout relèvement de v est fixe par $\mathrm{H}'_{\mathbf{Q}_p}$. Comme on peut choisir un tel relèvement dans V, on obtient une contradiction avec la définition de V_1, ce qui permet de conclure.

Dans tout ce qui suit, D est un (φ,Γ)-module étale et $V = \mathbf{V}(D)$ est la représentation p-adique de $\mathrm{G}_{\mathbf{Q}_p}$ qui lui correspond via l'équivalence de catégories de Fontaine, de telle sorte que $D = (\mathbf{A} \otimes_{\mathbf{Z}_p} V)^{\mathrm{H}}$.

Proposition 2.27. — $D^{\mathrm{nr}} = \mathbf{D}^{\mathrm{nr}}(V)$.

Démonstration. — Si x appartient à $\cap_{n\in\mathbf{N}}\varphi^n(\mathbf{E})$, il en est de même de ses conjugués sous l'action de H, et le polynôme minimal de x sur $\mathbf{E}_{\mathbf{Q}_p} = \mathbf{F}_p((T))$ est à coefficients dans $\cap_{n\in\mathbf{N}}\varphi^n(\mathbf{E}_{\mathbf{Q}_p}) = \mathbf{F}_p$. On en déduit que $\cap_{n\in\mathbf{N}}\varphi^n(\mathbf{E}) = \overline{\mathbf{F}}_p$, que $\cap_{n\in\mathbf{N}}\varphi^n(\mathbf{A}) = W(\overline{\mathbf{F}}_p)$, et que

$$D^{\mathrm{nr}} = \cap_{n\in\mathbf{N}}\varphi^n(D) \subset \big(\cap_{n\in\mathbf{N}}\,\varphi^n(\mathbf{A})\big)\otimes_{\mathbf{Z}_p} V = W(\overline{\mathbf{F}}_p)\otimes_{\mathbf{Z}_p} V.$$

Il en résulte que

$$D^{\mathrm{nr}} = (W(\overline{\mathbf{F}}_p)\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}} = \mathbf{D}^{\mathrm{nr}}(V).$$

Remarque 2.28. — Comme $\mathbf{D}^{\mathrm{nr}}(V) = \mathbf{D}^{\mathrm{nr}}(V^{\mathrm{H}'})$, on voit que D^{nr} est de dimension sur $\mathscr{O}_L$ inférieure ou égale à celle de $V^{\mathrm{H}'}$, et donc en particulier à celle de V, ce qui permet de retrouver le résultat selon lequel il est de dimension inférieure ou égale à celle de D sur $\mathscr{O}_{\mathscr{E}}$.

2.4.4. Les foncteurs $D\mapsto D^+$, $D\mapsto D^{++}$, etc. et l'équivalence de catégories de Fontaine

Remarque 2.29. — Les modules D^{nr}, D^{++} et D^+ peuvent se décrire via les anneaux de Fontaine. La description de D^{nr} fait l'objet de la prop. 2.27 ; nous allons donner une description de D^+ et D^{++}.

• On note $\widetilde{\mathbf{A}}^{++}$ l'idéal $W(\widetilde{\mathbf{E}}^{++})$ de $\widetilde{\mathbf{A}}^+$, ce qui fait de $\widetilde{\mathbf{A}}^+$ (resp. $\widetilde{\mathbf{A}}^{++}$) l'ensemble des $x\in\widetilde{\mathbf{A}}$ tels que $(\varphi^n(x))_{n\in\mathbf{N}}$ soit bornée (resp. $\varphi^n(x)\to 0$). Comme $\widetilde{\mathbf{E}}^+ = \overline{\mathbf{F}}_p\oplus\widetilde{\mathbf{E}}^{++}$, on a $\widetilde{\mathbf{A}}^+ = W(\overline{\mathbf{F}}_p)\oplus\widetilde{\mathbf{A}}^{++}$.

• Enfin, on pose $\mathbf{A}^{++} = \mathbf{A}\cap\widetilde{\mathbf{A}}^{++}$ (on rappelle que $\mathbf{A}^+ = \mathbf{A}\cap\widetilde{\mathbf{A}}^+$), ce qui fait de $\mathbf{A}^+$ (resp. $\mathbf{A}^{++}$) l'ensemble des $x\in\mathbf{A}$ tels que $(\varphi^n(x))_{n\in\mathbf{N}}$ soit bornée (resp. $\varphi^n(x)\to 0$). On a $\mathbf{A}^+ = W(\overline{\mathbf{F}}_p)\oplus\mathbf{A}^{++}$.

On en déduit que, si on définit $\mathbf{D}^+(V)$ et $\mathbf{D}^{++}(V)$ par :

$$\mathbf{D}^+(V) = (\mathbf{A}^+\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}}\quad\text{et}\quad \mathbf{D}^{++}(V) = (\mathbf{A}^{++}\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}},$$

alors $D^+ = \mathbf{D}^+(V)$ et $D^{++} = \mathbf{D}^{++}(V)$.

Remarque 2.30. — (i) Le module $\widetilde{D}$ peut se décrire aussi via les anneaux de Fontaine : si $V = \mathbf{V}(D)$ de telle sorte que $D = (\mathbf{A}\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}}$, alors

$$\widetilde{D} = \widetilde{\mathbf{D}}(V),\quad \text{avec } \widetilde{\mathbf{D}}(V) = (\widetilde{\mathbf{A}}\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}}.$$

En effet, on a

$$(\widetilde{\mathbf{A}}\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}} = (\widetilde{\mathbf{A}}\otimes_{\mathbf{A}}(\mathbf{A}\otimes_{\mathbf{Z}_p} V))^{\mathrm{H}} = \widetilde{\mathbf{A}}^{\mathrm{H}}\otimes_{\mathbf{A}_{\mathbf{Q}_p}} D = (\mathscr{O}_L\otimes_{\mathbf{Z}_p}\widetilde{\mathbf{A}}^{\mathrm{H}})\otimes_{\mathscr{O}_{\mathscr{E}}} D = \widetilde{D}.$$

(ii) Si D est un (φ,Γ)-module étale sur $\widetilde{\mathscr{O}}_{\mathscr{E}}$, alors $\widetilde{\mathbf{V}}(D) = ((\mathscr{O}_L\otimes_{\mathbf{Z}_p}\widetilde{\mathbf{A}})\otimes D)^{\varphi=1}$ est une représentation de $\mathrm{G}_{\mathbf{Q}_p}$, et $\widetilde{\mathbf{E}}$ étant algébriquement clos, le foncteur $D\mapsto\widetilde{\mathbf{V}}(D)$ est un inverse du foncteur $V\mapsto\widetilde{\mathbf{D}}(V)$.

(iii) Il résulte de la discussion précédente et de l'équivalence de catégories de Fontaine que $D = \mathbf{D}(\widetilde{\mathbf{V}}(\widetilde{D}))$, et donc que $D\mapsto\widetilde{D}$ induit des équivalences de catégories :

$$\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}\cong\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}(\widetilde{\mathscr{O}}_{\mathscr{E}}),\quad \Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})\cong\Phi\Gamma^{\mathrm{et}}(\widetilde{\mathscr{O}}_{\mathscr{E}})\quad\text{et}\quad \Phi\Gamma^{\mathrm{et}}(\mathscr{E})\cong\Phi\Gamma^{\mathrm{et}}(\widetilde{\mathscr{E}}).$$

Remarque 2.31. — (i) Les modules $\widetilde{D}^{++}$ et $\widetilde{D}^+$ peuvent se décrire aussi via les anneaux de Fontaine : si on définit $\widetilde{\mathbf{D}}^+(V)$ et $\widetilde{\mathbf{D}}^{++}(V)$ par

$$\widetilde{\mathbf{D}}^+(V) = (\widetilde{\mathbf{A}}^+\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}},\quad\text{et}\quad \widetilde{\mathbf{D}}^{++}(V) = (\widetilde{\mathbf{A}}^{++}\otimes_{\mathbf{Z}_p} V)^{\mathrm{H}},$$

alors $\widetilde{D}^+ = \widetilde{\mathbf{D}}^+(V)$ et $\widetilde{D}^{++} = \widetilde{\mathbf{D}}^{++}(V)$. En particulier, le $\widetilde{\mathscr{O}}_{\mathscr{E}}^+$-module $\widetilde{D}^+/\widetilde{D}^{++}$ est de type fini, tué par $\widetilde{\mathscr{O}}_{\mathscr{E}}^{++}$; il est égal à D^{nr}.

(ii) On peut retrouver V, et donc aussi D, à partir de $\widetilde{D}^+$. En effet d'après la prop. 2.37, on a $\widetilde{\mathbf{A}}^{++}\otimes_{\mathbf{Z}_p} V = \widetilde{\mathbf{A}}^{++}\otimes_{\widetilde{\mathbf{A}}^+_{\mathbf{Q}_p}} \widetilde{D}^{++}$, si V est de torsion On en déduit d'une part, que $\widetilde{D}^{++}$ est presque de type fini sur $\widetilde{\mathscr{O}}_{\mathscr{E}}^+$, et donc est un (φ,Γ)-module sur $\widetilde{\mathscr{O}}_{\mathscr{E}}^+$, et d'autre part, que $\widetilde{\mathbf{A}}\otimes_{\widetilde{\mathbf{A}}^+_{\mathbf{Q}_p}} \widetilde{D}^+ = \widetilde{\mathbf{A}}\otimes_{\mathbf{Z}_p} V$, et donc que $V = \widetilde{\mathbf{V}}(\widetilde{D}^+)$ et $\widetilde{D} = \widetilde{\mathscr{O}}_{\mathscr{E}}\otimes_{\widetilde{\mathscr{O}}_{\mathscr{E}}^+}\widetilde{D}^{++}$. Comme $\widetilde{D}^+/\widetilde{D}^{++}$ est tué par $\widetilde{\mathscr{O}}_{\mathscr{E}}^{++}$, on déduit que ce qui précède que $\widetilde{D}^+$ est presque de type fini sur $\widetilde{\mathscr{O}}_{\mathscr{E}}^+$, et que $V = \widetilde{\mathbf{V}}(\widetilde{D}^+)$ et $\widetilde{D} = \widetilde{\mathscr{O}}_{\mathscr{E}}\otimes_{\widetilde{\mathscr{O}}_{\mathscr{E}}^+}\widetilde{D}^+$. Ces formules restent valables pour un élément de $\Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})$ ou de $\Phi\Gamma^{\mathrm{et}}(\mathscr{E})$ par limite projective et tensorisation par L.

(iii) Il résulte aussi de la prop. 2.37 que le foncteur $D\mapsto \widetilde{D}^{++}$ est exact comme composé des deux foncteurs exacts $D\mapsto V$ et $V\mapsto \widetilde{\mathbf{D}}^{++}(V)$. On en déduit que $\widetilde{D}\mapsto\widetilde{D}^{++}$ induit des équivalences de catégories

$$\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}(\widetilde{\mathscr{O}}_{\mathscr{E}})\cong\Phi\Gamma^{0^+}_{\mathrm{tors}}(\widetilde{\mathscr{O}}_{\mathscr{E}}^+),\quad \Phi\Gamma^{\mathrm{et}}(\widetilde{\mathscr{O}}_{\mathscr{E}})\cong\Phi\Gamma^{0^+}(\widetilde{\mathscr{O}}_{\mathscr{E}}^+)\quad\text{et}\quad \Phi\Gamma^{\mathrm{et}}(\widetilde{\mathscr{E}})\cong\Phi\Gamma^{0^+}(\widetilde{\mathscr{E}}^+),$$

où le 0^+ en exposant signifie que φ est étale (i.e. de pente 0), mais est topologiquement nilpotent. Le foncteur inverse est juste le foncteur $D\mapsto\widetilde{\mathscr{O}}_{\mathscr{E}}\otimes_{\widetilde{\mathscr{O}}_{\mathscr{E}}^+} D$.

(iv) Par contre, le foncteur $D\mapsto\widetilde{D}^+$ n'est pas exact puisque $D\mapsto D^{\mathrm{nr}}$ ne l'est pas.

(v) Le sous-anneau $\mathscr{O}_{\mathscr{E}}\cdot\widetilde{\mathscr{O}}_{\mathscr{E}}^+$ de $\widetilde{\mathscr{O}}_{\mathscr{E}}$ est dense dans $\widetilde{\mathscr{O}}_{\mathscr{E}}$ (appliquer le lemme **??** à $\mathscr{O}_{\mathscr{E}}$). On en déduit que $\mathscr{O}_{\mathscr{E}}\otimes_{\mathscr{O}_{\mathscr{E}}^+}\widetilde{D}^+$ est dense dans $\widetilde{D}$.

2.4.5. Le foncteur $V\mapsto\widetilde{\mathbf{D}}^{++}(V)$. — Soient $L\supset K$ deux extensions finies de $\mathbf{Q}_p$ et A un anneau muni d'une action de $\mathrm{H}_{\mathbf{Q}_p}$. Si $x\in A$ est fixe par H_L, définissons $\mathrm{T}_{L/K}(x)$ par la formule

$$\mathrm{T}_{L/K}(x)=\sum_{\sigma\in\mathrm{H}_K/\mathrm{H}_L}\sigma(x).$$

En particulier, si $A=\overline{\mathbf{Q}}_p$, alors $\mathrm{T}_{L/K}$ est l'application $\mathrm{Tr}_{L_\infty/K_\infty}: L_\infty\to K_\infty$.

Lemme 2.32. — (i) *Si K est une extension finie de $\mathbf{Q}_p$, la restriction de $v_{\mathbf{E}}$ à $\widetilde{\mathbf{E}}_K$ n'est pas discrète.*

(ii) *Si $L\supset K$ sont deux extensions finies de $\mathbf{Q}_p$, alors $\widetilde{\mathbf{E}}_L/\widetilde{\mathbf{E}}_K$ est une extension séparable de degré $[L_\infty : K_\infty]$.*

(iii) *Si $L\supset K$ sont deux extensions finies de $\mathbf{Q}_p$, alors, quel que soit $\delta>0$, il existe $\alpha\in\widetilde{\mathbf{E}}_L$ vérifiant $v_{\mathbf{E}}(\alpha)\geqslant-\delta$ et $\mathrm{T}_{L/K}(\alpha)=1$.*

Démonstration. — Le (i) suide ce que $\mathbf{E}_K$ contient $\overline{\pi}^{p^{-n}}$ quel que soit $n\in\mathbf{N}$. Le (ii) a déjà été démontré, et il résulte du (ii) que l'application $\mathrm{T}_{L/K}$ coïncide avec la trace de $\widetilde{\mathbf{E}}_L$ sur $\widetilde{\mathbf{E}}_K$ et donc n'est pas identiquement nulle. Elle est donc surjective et il existe $x\in\widetilde{\mathbf{E}}_L$ vérifiant $\mathrm{T}_{L/K}(x)=1$ et quitte à remplacer x par $x^{p^{-n}}$, on peut s'arranger pour que $v_{\mathbf{E}}(x)\geqslant-\delta$.

Lemme 2.33. — *Soit $\beta\in\widetilde{\mathbf{E}}_K^{++}$. Si $[L:K]<+\infty$, si n est un entier $\geqslant 2$, et si $\tau\to U_\tau$ est un 1-cocycle continu de H_L dans $1+\beta^nM_d(\widetilde{\mathbf{E}}^+)$, alors il existe $M\in 1+\beta^{n-1}M_d(\widetilde{\mathbf{E}}^+)$ tel que le cocycle $M^{-1}U_\tau\tau(M)$ soit à valeurs dans $1+\beta^{n+1}\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$.*

Démonstration. — Soit M une extension finie de L telle que U_τ appartienne à $1+\beta^{n+2}\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$, pour tout $\tau\in \mathrm{H}_M$, et soit α un élément de $\widetilde{\mathbf{E}}_M$ vérifiant $\mathrm{T}_{M/L}(\alpha)=1$ et $v_{\mathbf{E}}(\alpha)\geqslant -v_{\mathbf{E}}(\beta)$. Si T est un système de représentants de $\mathrm{H}_M/\mathrm{H}_L$, posons

$$M_T=\sum_{\tau\in T}\tau(\alpha)U_\tau.$$

Les hypothèses mises sur α entraînent que M_T est élément de $1+\beta^{n-1}\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$. D'autre part, si T' est un autre système de représentants de $\mathrm{H}_M/\mathrm{H}_L$, la relation de cocycle et le choix de M font que $M_T-M_{T'}\in\beta^{n+1}\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$. Finalement la relation de cocycle permet d'obtenir la relation $M_T^{-1}U_\tau\tau(M_T)=1+M_T^{-1}(M_{\tau T}-M_T)$ qui permet de montrer que M_T répond à la question (quel que soit le choix de T).

Corollaire 2.34. — *Soit $\beta\in\widetilde{\mathbf{E}}_K^{++}$. Si $[L:K]<+\infty$, si n est un entier $\geqslant 2$, et si $\tau\to U_\tau$ est un 1-cocycle continu de H_L dans $1+\beta^2M_d(\widetilde{\mathbf{E}}^+)$, alors il existe $M\in 1+\beta\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$ tel que l'on ait $M^{-1}U_\tau\tau(M)=1$ quel que soit $\tau\in\mathrm{H}_L$.*

Démonstration. — Une récurrence utilisant le lemme précédent permet de construire une suite de matrices $(M_m)_{m\geqslant 1}$ telle que $M_m\in 1+\beta^m\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$ et que le cocycle $\tau\to(\prod_{i=1}^m M_i)^{-1}U_\tau\tau(\prod_{i=1}^m M_i)$ soit à valeurs dans $1+\beta^{m+2}\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$. Le produit infini $\prod_{i=1}^{+\infty}M_i$ converge alors vers une matrice M qui répond à la question.

Proposition 2.35. — (i) $H^1(\mathrm{H}_K,\mathrm{GL}_d(\widetilde{\mathbf{E}}))=\{1\}$.
(ii) $H^1(\mathrm{H}_K,\widetilde{\mathbf{E}})=0$.
(iii) $H^1(\mathrm{H}_K,\widetilde{\mathbf{E}}^{++})=0$.
(iv) $H^1(\mathrm{H}_K,1+\mathrm{M}_d(\widetilde{\mathbf{E}}^{++}))=\{1\}$.

Démonstration. — Considérons un 1-cocycle continu $\tau\to U_\tau$ de H_K à valeurs dans $\mathrm{GL}_d(\widetilde{\mathbf{E}})$. La continuité de U_τ implique l'existence d'une extension finie L de K_∞ telle que U_τ soit à valeurs dans $1+\beta^2M_d(\widetilde{\mathbf{E}}^+)$ si $\tau\in\mathrm{G}_L$. Le corollaire précédent nous donne l'existence de $M\in 1+\beta\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$ tel que l'on ait $M^{-1}U_\tau\tau(M)=1$ quel que soit $\tau\in\mathrm{G}_L$. Le cocycle $\tau\to M^{-1}U_\tau\tau(M)=1$ peut donc être vu comme un cocycle sur $\mathrm{H}_K/\mathrm{G}_L$ à valeurs dans $\mathrm{GL}_d(\widetilde{\mathbf{E}}_L)$ et est donc trivial d'après le théorème de Hilbert 90 puisque l'extension $\widetilde{\mathbf{E}}_L/\widetilde{\mathbf{E}}_K$ est séparable. Ceci démontre le (i).

Soient $\tau\to c_\tau$ un cocycle continu de H_K dans $\widetilde{\mathbf{E}}$, et $\alpha,\beta\in\mathbf{E}_K^{++}$ tels que αc_τ soit à valeurs dans $\beta^2\widetilde{\mathbf{E}}^+$. Si $\tau\in\mathrm{H}_K$, soit $U_\tau=\left(\begin{smallmatrix}1&\alpha c_\tau\\0&1\end{smallmatrix}\right)\in 1+\beta^2\mathrm{M}_2(\widetilde{\mathbf{E}}^+)$. La relation de cocycle satisfaite par c_τ se traduit par le fait que $\tau\to U_\tau$ est un cocycle. D'après le corollaire 2.34, il existe donc une matrice $\left(\begin{smallmatrix}a&c\\b&d\end{smallmatrix}\right)\in 1+\beta\mathrm{M}_2(\widetilde{\mathbf{E}}^+)$ telle que l'on ait $U_\tau\tau(M)=M$ quel que soit $\tau\in\mathrm{H}_K$. Cette dernière identité se traduit par le fait que d est un élément de $\widetilde{\mathbf{E}}_K^+$ (inversible car congru à 1 modulo β) et par la relation $\alpha c_\tau=(1-\tau)\cdot(d^{-1}c)$ qui permet de conclure au fait que αc_τ est trivial et de démontrer le (ii).

Pour démontrer le (iii) [resp. le (iv)], il suffit de remarquer que la compacité de H_K implique que si $\tau\to c_\tau$ est un cocycle continu à valeurs dans $\widetilde{\mathbf{E}}^{++}$ [resp. $1+\mathrm{M}_d(\widetilde{\mathbf{E}}^{++})$], alors la condition (C3) implique qu'il existe $\beta\in\widetilde{\mathbf{E}}_K^{++}$ tel que c_τ soit à valeurs dans $\beta^2\widetilde{\mathbf{E}}^+$ [resp. $1+\beta^2\mathrm{M}_d(\widetilde{\mathbf{E}}^+)$] ; on conclut alors comme pour le (ii) [resp. en utilisant le corollaire 2.34].

Lemme 2.36. — *Si V est une $\mathbf{F}_p$-représentation de $\mathrm{H}_{\mathbf{Q}_p}$ de dimension d, alors*
(i) $\widetilde{\mathbf{E}}\otimes V\cong\widetilde{\mathbf{E}}^d$ *en tant que* $\mathrm{H}_{\mathbf{Q}_p}$*-module.*

(ii) *Le sous-*$\widetilde{\mathbf{E}}^+$*-module de* $\widetilde{\mathbf{E}}\otimes V$ *engendré par* $(\widetilde{\mathbf{E}}^{++}\otimes V)^{\mathrm{H}_{\mathbf{Q}_p}}$ *est égal à* $\widetilde{\mathbf{E}}^{++}\otimes V$.

(iii) $H^1(\mathrm{H}_{\mathbf{Q}_p},\widetilde{\mathbf{E}}^{++}\otimes V)=0$.

Démonstration. — Le (i) suit de la trivialité de $H^1(\mathrm{H}_K,\mathrm{GL}_d(\widetilde{\mathbf{E}}))$. On en déduit l'existence d'une base $f_1,\dots,f_d$ de $\widetilde{\mathbf{E}}\otimes V$ fixe par $\mathrm{H}_{\mathbf{Q}_p}$ et, quitte à multiplier les f_i par une puissance de $\overline{\pi}$, on peut supposer que cette base est constituée d'éléments de $\widetilde{\mathbf{E}}^{++}\otimes V$. Soient $e_1,\dots,e_d$ une base de V sur $\mathbf{F}_p$ et M la matrice de $f_1,\dots,f_d$ dans la base $e_1,\dots,e_d$. Si $n\in\mathbf{N}$, $\varphi^{-n}(f_i)$ est aussi un élément de $\widetilde{\mathbf{E}}^{++}\otimes V$ fixe par $\mathrm{H}_{\mathbf{Q}_p}$ et la matrice de $\varphi^{-n}(f_1),\dots,\varphi^{-n}(f_d)$ dans la base $e_1,\dots,e_d$ est $\varphi^{-n}(M)$ et vérifie $\lim_{n\to+\infty}v_{\mathbf{E}}(\det\varphi^{-n}(M))=0$, ce qui permet de montrer que tout élément de $\widetilde{\mathbf{E}}^{++}\otimes V$ est dans le $\widetilde{\mathbf{E}}^{+}$-module engendré par $\varphi^{-n}(f_1),\dots,\varphi^{-n}(f_d)$ si n est assez grand ; d'où le (ii).

Passons au (iii). Comme $\mathrm{H}_{\mathbf{Q}_p}$ est compact, il existe $\eta>0$ tel que si $\tau\to c_\tau$ est un 1-cocycle continu à valeurs dans $\widetilde{\mathbf{E}}^{++}\otimes V$, alors les coordonnées de c_τ dans la base $e_1,\dots,e_d$ ont une image par $v_{\mathbf{E}}$ supérieure ou égale à η quel que soit $\tau\in\mathrm{H}_{\mathbf{Q}_p}$. On en déduit l'existence de $n\in\mathbf{N}$ tel que les coordonnées de c_τ dans la base $\varphi^{-n}(f_1),\dots,\varphi^{-n}(f_d)$ appartiennent à $\widetilde{\mathbf{E}}^{++}$ quel que soit $\tau\in\mathrm{H}_{\mathbf{Q}_p}$ et comme $\varphi^{-n}(f_1),\dots,\varphi^{-n}(f_d)$ sont stables par $\mathrm{H}_{\mathbf{Q}_p}$, on peut utiliser le (iii) de la proposition 2.35 pour conclure.

Proposition 2.37. — (i) *Si* $0\to V_1\to V\to V_3\to 0$ *est une suite exacte de* $\mathscr{O}_L$*-représentations de* $\mathrm{G}_{\mathbf{Q}_p}$*, alors la suite* $0\to\widetilde{\mathbf{D}}^{++}(V_1)\to\widetilde{\mathbf{D}}^{++}(V)\to\widetilde{\mathbf{D}}^{++}(V_2)\to 0$ *est exacte.*

(ii) *Si* V *est un objet de* $\mathrm{Rep}_{\mathrm{tors}}\mathrm{G}_{\mathbf{Q}_p}$ (*resp.* $\mathrm{Rep}_{\mathscr{O}_L}\mathrm{G}_{\mathbf{Q}_p}$), *alors* $H^1(\mathrm{H}_K,\widetilde{\mathbf{A}}^{++}\otimes V)=0$ *et le sous* $\mathbf{A}^+$*-module de* $\widetilde{\mathbf{A}}^{++}\otimes V$ *engendré par* $\widetilde{\mathbf{D}}^+(V)$ *est égal à* (*resp. est dense dans*) $\widetilde{\mathbf{A}}^{++}\otimes V$.

Démonstration. — Le (ii) se déduit, par dévissage, du lemme 2.36, dans le cas de torsion. Le cas non torsion s'en déduit par limite projective. L'exactitude du foncteur $\widetilde{\mathbf{D}}^{++}$ se déduit alors de la suite exacte de cohomologie obtenue à partir de la suite exacte $0\to\widetilde{\mathbf{A}}^{++}\otimes_{\mathbf{Z}_p}V_1\to\widetilde{\mathbf{A}}^{++}\otimes_{\mathbf{Z}_p}V\to\widetilde{\mathbf{A}}^{++}\otimes_{\mathbf{Z}_p}V_2\to 0$.

PIERRE COLMEZ