NOTES DU COURS 2009

par

Pierre Colmez

Table des matières

I. Espaces fonctionnels p-adiques

I.1. Espaces de Banach p-adiques. — Ce § ne contient que des généralités (sans démonstrations) sur les espaces de Banach p-adiques.

1. L-banach. — On normalise la valuation p-adique v_p sur $\mathbf{C}_p$ par $v_p(p) = 1$. Si L est un sous-corps fermé de $\mathbf{C}_p$, on note $\mathscr{O}_L$ l'anneau de ses entiers, $\mathfrak{m}_L = \{x \in L, v_p(x) > 0\}$ l'idéal maximal de $\mathscr{O}_L$, et $k_L = \mathscr{O}_L/\mathfrak{m}_L$ le corps résiduel de L.

Si B est un L-espace vectoriel, une *valuation* sur B est une fonction $v_B : B \to \mathbf{R} \cup \{+\infty\}$ vérifiant les propriétés suivantes :

(i) $v_B(x) = +\infty$ si et seulement si $x = 0$;

(ii) $v_B(x + y) \geqslant \inf(v_B(x), v_B(y))$ quels que soient $x, y \in B$;

(iii) $v_B(\lambda x) = v_p(\lambda) + v_B(x)$ quels que soient $\lambda \in L$ et $x \in B$.

Un *L-banach* B est un L-espace vectoriel topologique, la topologie étant définie par une valuation v_B pour laquelle il est complet.

Exemple I.1.1. — (i) Si I est un ensemble, soit $\ell_\infty(I, L)$ l'ensemble des familles bornées $(a_i)_{i\in I}$ d'éléments de L. On munit $\ell_\infty(I, L)$ de la valuation v_{ℓ_∞} définie par $v_{\ell_\infty}((a_i)_{i\in I}) = \inf_{i\in I} v_p(a_i)$, ce qui en fait un L-banach.

(ii) Soit $\ell^0_\infty(I, L)$ le sous-espace de $\ell_\infty(I, L)$ des suites $(a_i)_{i\in I}$ d'éléments de L tendant vers 0 suivant le filtre des complémentaires des parties finies. C'est un L-banach comme sous-L-espace vactoriel fermé d'un L-banach. C'est aussi l'adhérence dans $\ell_\infty(I, L)$ de l'espace des suites n'ayant qu'un nombre fini de termes non nuls.

(iii) Plus généralement, si I est un ensemble, et si B est un L-banach, l'espace $\ell_\infty(I, B)$ (resp. $\ell^0_\infty(I, B)$) des suites $(a_i)_{i\in I}$ d'éléments de B, qui sont bornées (resp. qui tendent vers 0 suivant le filtre des complémentaires des parties finies), muni de la valuation v_{ℓ_∞} définie par $v_{\ell_\infty}((a_i)_{i\in I}) = \inf_{i\in I} v_B(a_i)$, est un L-banach.

La plupart des résultats classiques de la théorie des espaces de Banach réels restent valables pour les L-banach (le théorème de Hahn-Banach demande un peu de précaution). En particulier, on a les résultats suivants.

Proposition I.1.2. — (i) *Si $f : B_1 \to B_2$ est une application linéaire continue bijective entre deux espaces de Banach p-adiques, alors f^{-1} est continue (théorème de l'image ouverte).*

(ii) *Une limite simple d'applications linéaires continues sur un espace de Banach est continue (Théorème de Banach-Steinaus).*

Démonstration. — Voir n'importe quel livre traitant des espaces de Banach.

2. Bases de Banach. — La théorie des espaces de Banach p-adiques est très loin d'être aussi riche que son homologue archimédienne ; elle se rapproche plutôt de celle des espaces de Hilbert réels. En particulier, la notion suivante remplace celle de base hilbertienne dans un espace de Hilbert.

Définition I.1.3. — *Soit B un L-banach. Une famille $(e_i)_{i\in I}$ d'éléments de B est une base orthonormale de B de B si l'application $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i e_i$, de $\ell^0_\infty(I, L)$ dans B, est une isométrie. On dit que c'est une base de Banach si cette application est seulement un isomorphisme de L-banach. Autrement dit, une famille $(e_i)_{i\in I}$ est une base de Banach de B si et seulement si*

(i) *tout élément x de B peut s'écrire de manière unique sous la forme d'une série convergente $x = \sum_{i\in I} a_i e_i$, où les a_i sont des éléments de L tendant vers 0 suivant le filtre des complémentaires des parties finies,*

(ii) $v_B(x) = \inf_{i\in I} v_p(a_i)$.

C'est une base de Banach si elle est bornée et vérifie la condition (i), ce qui implique, d'après le théorème de l'image ouverte, la propriété suivante.

(ii') *il existe une constante $C \geqslant 0$ telle que l'on ait $-C + \inf_{i\in I} v_p(a_i) \leqslant v_B(x) \leqslant C + \inf_{i\in I} v_p(a_i)$.*

Une famille $(e_i)_{i\in I}$ d'éléments de B est orthogonale s'il existe une famille $(\lambda_i)_{i\in I}$ d'éléments de L telle que, quelle que soit la famille $(x_i)_{i\in I}$ d'éléments de L, on ait $v_B(\sum_{i\in I} x_i\lambda_i e_i) = \inf_{i\in I} v_p(x_i)$. En particulier une base orthonormale est orthogonale.

Exemple I.1.4. — Si I est un ensemble, et si $i \in I$, on note δ_i la suite dont tous les termes sont nuls sauf celui d'indice i qui est égal à 1. Par définition, ou presque, les δ_i, pour $i \in I$, forment une base orthonormale de $\ell^0_\infty(I, \mathbf{Q}_p)$.

Proposition I.1.5. — *Si L est de valuation discrète, et π_L est une uniformisante de L, alors :*

(i) *Tout L-banach possède des bases de Banach.*

(ii) *Un L-banach possède des bases orthonormales si et seulement si $v_B(B) = v_p(L)$. De plus, sous cette hypothèse, si on note $B^0 = \{x \in B \mid v_B(x) \geqslant 0\}$, alors $(e_i)_{i\in I}$ est une base orthonormale de B si et seulement si $(\overline{e}_i)_{i\in I}$ est une base algébrique du k_L-espace vectoriel $\overline{B} = B^0/\pi_L B^0$.*

Démonstration. — Si B est un L-banach muni de la valuation v_B, alors $v'_B : B \to v_p(L)$, définie par $v'_B(x) = v_p(\pi_L) \cdot \left[\frac{v_B(x)}{v_p(\pi_L)}\right]$, est une valuation sur B, équivalente à v_B, ce qui permet de déduire le (i) du (ii). Supposons donc que $v_B(B) = v_p(L)$, et montrons que $(e_i)_{i\in I}$ est une base orthonormale de B si et seulement si $(\overline{e}_i)_{i\in I}$ est une base algébrique du k_L-espace vectoriel $\overline{B}$.

Soit $(e_i)_{i\in I}$ une famille d'éléments de B^0 telle que la famille $(\overline{e}_i)_{i\in I}$ soit une base du k_L-espace vectoriel $\overline{B}$. Soient S un système de représentants de k_L dans $\mathscr{O}_L$ contenant 0 et $s : k_L \to S$ l'inverse de la réduction modulo π_L. Si $x \in B^0$, on peut écrire $\overline{x}$ comme une somme finie $\sum_{i\in I} a_i\overline{e}_i$, où les a_i sont des éléments de k_L presque tous nuls. Soit $s(x) = \sum_{i\in I} s(a_i)e_i$. Par construction, on a $x - s(x) \in \pi_L B^0$.

Si $x \in B^0$, définissons par récurrence une suite x_n d'éléments de B_0 par $x_0 = x$ et $x_{n+1} = \frac{1}{\pi_L}(x_n - s(x_n))$. On a alors $x = \sum_{n=0}^{k} \pi_L^n s(x_n) + \pi_L^{k+1}x_{k+1}$ quel que soit $k \in \mathbf{N}$. On peut écrire $s(x_n) = \sum_{i\in I} s_{n,i}e_i$, où les $s_{n,i}$ sont des éléments de S presque tous nuls, ce qui montre que si on pose $a_i = \sum_{n=0}^{+\infty} \pi_L^n s_{n,i}$, alors la suite des a_i tend vers 0 suivant le filtre des complémentaires des parties finies. Ceci montre que l'application de $\ell_\infty^0(I,L)$ dans B qui à $(a_i)_{i\in I}$ associe $\sum_{i\in I} a_ie_i$ est surjective. Si $(a_i)_{i\in I}$ est un élément non nul de $\ell_\infty^0(I,L)$, alors quitte à multiplier a par une puissance de π_L, on peut supposer $v_{\ell_\infty}(a) = 0$, et le fait que les $(\overline{e}_i)_{i\in I}$ forment une base de $\overline{B}$ implique que $\sum_{i\in I} a_ie_i \neq 0$ modulo π_L et donc que $0 \leqslant v_{\ell_\infty}\big(\sum_{i\in I} a_ie_i\big) < v_p(\pi_L)$. Comme on a supposé $v_B(B) = v_p(L)$, ceci implique $v_{\ell_\infty}\big(\sum_{i\in I} a_ie_i\big) = 0$, et on en tire le fait que l'application $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_ie_i$ est une isométrie de $\ell_\infty^0(I,L)$ sur B.

La réciproque est immédiate.

Proposition I.1.6. — *Si L est de valuation discrète, si B est un L-banach, et si F est un sous-L-espace vectoriel fermé de B, alors F admet un supplémentaire fermé.*

Démonstration. — On peut supposer que B vérifie $v_B(B) = v_p(L)$, ce qui implique $v_B(F) = v_p(L)$. Soient $F^0 = F \cap B^0$ et $\overline{F} = F^0/pF^0 \subset \overline{B}$. Soient $(f_j)_{j\in J}$ une base orthonormale de F et $(g_i)_{i\in I}$ une famille d'éléments de B telle que la famille des $(\overline{f}_j)_{j\in J}$ et des $(\overline{g}_i)_{i\in I}$ forme une base de $\overline{B}$. On peut alors prendre pour G l'adherence dans B de l'espace vectoriel engendré par les $(g_j)_{j\in J}$.

Corollaire I.1.7. — *Si L est de valuation discrète, si $f : B_1 \to B_2$ est une application linéaire continue surjective entre deux L-banach p-adiques, alors f admet un scindage continu, c'est-à-dire qu'il existe $s : B_2 \to B_1$ linéaire continue telle que l'on ait $f\circ s = \mathrm{id}_{B_2}$.*

Démonstration. — Il suffit de prendre un supplémentaire fermé de $\ker f$ dans B_1 et d'utiliser le théorème de l'image ouverte.

3. Le dual d'un L-banach. — Si B est un L-banach, on note B^* le L-espace vectoriel des formes L-linéaires continues $f : B \to L$. Muni de la *topologie forte* définie par la valuation v_{B^*} donnée par la formule

$$v_{B^*}(f) = \inf_{x\in B-\{0\}} v_p(f(x)) - v_B(x),$$

cet espace est un L-banach. On peut aussi munir B^* de la *topologie faible* de la convergence simple (topologie la plus faible telle qu'une suite f_n, $n \in \mathbf{N}$, ait pour limite f, si et seulement si, quel que soit $x \in B$, $f_n(x)$ tend vers $f(x)$ quand n tend vers $+\infty$). D'après le théorème de Banach-Steinaus, B^* est aussi complet pour la topologie faible, mais l'espace ainsi obtenu n'est un L-banach que si B est de dimension finie.

Proposition I.1.8. — *Soit I un ensemble.*

(i) *Si $b = (b_i)_{i\in I} \in \ell_\infty(I, L)$, et si $a = (a_i)_{i\in I} \in \ell^0_\infty(I, L)$, la série $\sum_{i\in I} b_i a_i$ converge dans L.*

(ii) *Si $f_b(a)$ désigne la somme de la série $\sum_{i\in I} b_i a_i$, l'application $b \mapsto f_b$ est une isométrie de $\ell_\infty(I, L)$ sur le dual de $\ell^0_\infty(I, L)$.*

Démonstration. — La seule chose non totalement évidente est la surjectivité de $b \mapsto f_b$. Soit donc $f \in \ell^0_\infty(I, L)^*$. Comme f est continue, si on pose $b_i = f(\delta_i)$, on a $v_p(b_i) \geqslant v_{\ell^0_\infty(I,L)^*}(f)$, ce qui prouve que $b = (b_i)_{i\in I} \in \ell_\infty(I, L)$. Mais alors $f - f_b$ est nul sur le sous-espace de $\ell^0_\infty(I, L)^*$ engendré par les δ_i ; comme celui-ci est dense et $f - f_b$ continue, cela implique $f = f_b$. Ceci permet de conclure.

Remarque I.1.9. — Soit δ_i^* l'élément de $\ell^0_\infty(I, L)^*$ défini par $\delta_i^*(\delta_j) = 1$, si $j = i$, et $\delta_i^*(\delta_j) = 0$, si $j \neq i$. Il résulte de la démonstration ci-dessus que, si $f \in \ell^0_\infty(I, L)^*$, alors $f = \sum_{i\in I} f(\delta_i)\delta_i^*$ dans $\ell^0_\infty(I, L)^*$, muni de la topologie faible (la série ne converge pas pour la topologie forte, sauf si I est un ensemble fini).

4. Produit tensoriel de L-banach. — Soient B_1 et B_2 deux L-banach. Si $z \in B_1 \otimes_L B_2$, on définit $v_{B_1\otimes B_2}$ comme le maximum des $\inf_{j\in J}(v_{B_1}(x_j) + v_{B_2}(y_j))$ pour toutes les écritures possibles de z sous la forme $\sum_{j\in J} x_j \otimes y_j$. Ceci munit $B_1 \otimes_L B_2$ d'une semi-valuation, et on note $B_1 \widehat{\otimes}_L B_2$ le séparé complété de $B_1 \otimes_L B_2$ pour cette semi-valuation. C'est le *produit tensoriel complété* de B_1 et B_2.

Proposition I.1.10. — *Si I est un ensemble et B est un L-banach, alors $\ell^0_\infty(I, L)\widehat{\otimes}_L B$ est isométrique à $\ell^0_\infty(I, B)$.*

Démonstration. — L'espace $\ell^0_\infty(I, L) \otimes_L B$ est le sous-espace de $\ell^0_\infty(I, B)$ des suites $(a_i)_{i\in I}$ telles que le sous-L-espace vectoriel de B engendré par les a_i, $i \in I$, soit de dimension finie. Il contient en particulier l'espace des suites $(a_i)_{i\in I}$ d'éléments de B, avec $a_i = 0$ en dehors d'un sous-ensemble fini de I. Comme cet dernier espace est dense dans $\ell^0_\infty(I, B)$, il suffit de vérifier que la valuation v définie ci-dessus sur $\ell^0_\infty(I, L) \otimes_L B$ est celle induite par l'inclusion de $\ell^0_\infty(I, L) \otimes_L B$ dans $\ell^0_\infty(I, B)$.

Soit donc $z = \sum_{j\in J} x_j \otimes y_j \in \ell^0_\infty(I, L) \otimes_L B$. On peut écrire x_j, de manière unique, sous la forme $x_j = \sum_{i\in I} a_{i,j}\delta_i$, avec $a_{i,j} \in L$, tendant vers 0 quand i tend vers l'infini. On a alors

$$\inf_{j\in J}(v_{\ell_\infty}(x_j) + v_B(y_j)) = \inf_{j\in J,\, i\in I}(v_p(a_{i,j}) + v_B(y_j)) \leqslant \inf_{i\in I} v_B\big(\sum_{j\in J} a_{i,j}y_j\big) = v_{\ell_\infty(I,B)}(z).$$

Ceci étant vrai pour toute écriture de z sous la forme $z = \sum_{j\in J} x_j \otimes y_j$, on en déduit l'inégalité $v(z) \leqslant v_{\ell_\infty(I,B)}(z)$.

Pour montrer l'inégalité inverse, partons d'une écriture de z sous la forme $z = \sum_{j\in J} x_j \otimes y_j$, et choisissons une base e_r, $r \in R$, du sous-L-espace vectoriel (de dimension finie) de B engendré par les y_j, $j \in J$. Écrivons aussi, comme ci-dessus, x_j sous la forme $x_j = \sum_{i\in I} a_{i,j}\delta_i$, avec $a_{i,j} \in L$, tendant vers 0 quand i tend vers l'infini. Soient $b_{i,r}$, $r \in R$, les coordonnées de $z_i = \sum_{j\in J} a_{i,j}y_j$

dans la base des e_r, $r \in R$. Il existe $I_0 \subset I$ fini, tel que $v_B(b_{i,r}e_r) > v(z)$ si $i \notin I_0$. Soit alors $a_r = \sum_{i \in I - I_0} b_{i,r} e_r \in \ell^0_\infty(I, L)$. On peut écrire z sous la forme

$$z = \sum_{r \in R} a_r \otimes e_r + \sum_{i \in I_0} \delta_i \otimes z_i.$$

On a donc

$$v(z) \geqslant \min\big(\inf_{r\in R} v_{\ell_\infty}(a_r) + v_B(e_r), \inf_{i \in I_0} v_B(z_i)\big) \geqslant \min\big(\inf_{r\in R} v_{\ell_\infty}(a_r) + v_B(e_r), v_{\ell_\infty(I,B)}(z)\big),$$

et comme $v_{\ell_\infty}(a_r) + v_B(e_r) > v(z)$ par construction, on en déduit l'inégalité $v(z) \geqslant v_{\ell_\infty(I,B)}(z)$ que l'on cherchait à établir. Ceci permet de conclure.

Corollaire I.1.11. — *Si B est un L-banach, si $(e_i)_{i\in I}$ est une base orthonormale de B, et si K est un sous-corps complet de $\mathbf{C}_p$ contenant L, alors $(e_i)_{i \in I}$ est une base orthonormale du K-banach $K\widehat{\otimes}_L B$.*

I.2. Fonctions continues sur $\mathbf{Z}_p$

1. Exemples, fonctions localement constantes. — Soit $\mathscr{C}^0(\mathbf{Z}_p, L)$ l'ensemble des fonctions continues de $\mathbf{Z}_p$ dans L. Comme $\mathbf{Z}_p$ est compact, une fonction continue sur $\mathbf{Z}_p$ est bornée. Ceci permet de munir $\mathscr{C}^0(\mathbf{Z}_p, L)$ de la valuation $v_{\mathscr{C}^0}$ définie par $v_{\mathscr{C}^0}(\phi) = \inf_{x \in \mathbf{Z}_p} v_p(\phi(x))$, ce qui en fait un L-banach.

• *Polynômes binomiaux.*— Si $n \in \mathbf{N}$, soit $\binom{x}{n}$ le polynôme défini par

$$\binom{x}{n} = \begin{cases} 1 & \text{si } n = 0 \\ \frac{x(x-1)\dots(x-n+1)}{n!} & \text{si } n \geqslant 1. \end{cases}$$

Proposition I.2.1. — *Si $n \in \mathbf{N}$, alors $v_{\mathscr{C}^0}\big(\binom{x}{n}\big) = 0$.*

Démonstration. — On a $\binom{n}{n} = 1$ et donc $v_{\mathscr{C}^0}\big(\binom{x}{n}\big) \leqslant 0$. D'autre part, si $k \in \mathbf{N}$, $\binom{n+k}{n}$ est le nombre de manière de choisir n objets parmi $n+k$ et est donc entier. On en déduit le fait que $v_p\big(\binom{n+k}{n}\big) \geqslant 0$ quel que soit $k \in \mathbf{N}$, et comme $n + \mathbf{N}$ est dense dans $\mathbf{Z}_p$, cela implique que $v_p\big(\binom{x}{n}\big) \geqslant 0$ quel que soit $x \in \mathbf{Z}_p$, ce qui permet de conclure.

• *Fonctions puissances.*— Si $z \in L$ vérifie $v_p(z-1) > 0$, la série $\phi_z(x) = \sum_{n=0}^{+\infty} \binom{x}{n}(z-1)^n$ converge normalement d'après la proposition I.2.1 et définit donc une fonction continue $\phi_z(x)$ de $x \in \mathbf{Z}_p$. D'autre part, si $k \in \mathbf{N}$, on a $\phi_z(k) = z^k$, ce qui nous permet de noter de manière plus parlante $x \mapsto z^x$ la fonction $x \mapsto \phi_z(x)$. On a $z^{x+y} = z^x z^y$ quels que soient $x, y \in \mathbf{Z}_p$ car cette formule est vraie si $x, y \in \mathbf{N}$, et $\mathbf{N}^2$ est dense dans $\mathbf{Z}_p^2$.

• *Racines de l'unité.*— Un cas particulièrement utile est celui où z est une racine de l'unité d'ordre une puissance p. Si $z^{p^n} = 1$, on a $z^{x+p^n k} = z^x$ quel que soit $k \in \mathbf{N}$ et donc $z^x = z^y$ si $y \in x + p^n\mathbf{Z}_p$, ce qui fait que la fonction z^x est localement constante.

• *Fonctions localement constantes.*— Si $h \in \mathbf{N}$, on note $\mathrm{LC}_h(\mathbf{Z}_p, L)$ l'ensemble des fonctions de $\mathbf{Z}_p$ dans L dont la restriction à $a + p^h\mathbf{Z}_p$ est constante, quel que soit $a \in \mathbf{Z}_p$. On note $\mathrm{LC}(\mathbf{Z}_p, L)$

l'espace des fonctions localement constantes sur $\mathbf{Z}_p$, à valeurs dans L. Comme $\mathbf{Z}_p$ est compact, c'est la limite inductive (i.e. la réunion croissante) des $\mathrm{LC}_h(\mathbf{Z}_p, L)$, pour $h \in \mathbf{N}$.

Lemme I.2.2. — *$\mathrm{LC}(\mathbf{Z}_p, L)$ est dense dans $\mathscr{C}^0(\mathbf{Z}_p, L)$.*

Démonstration. — $\mathbf{Z}_p$ étant compact, une fonction continue sur $\mathbf{Z}_p$ est uniformément continue. Autrement dit, si $\phi \in \mathscr{C}^0(\mathbf{Z}_p, L)$ et $C \geqslant 0$, il existe $m \in \mathbf{N}$ tel que, si $v_p(x-y) \geqslant m$, alors $v_p(\phi(x) - \phi(y)) \geqslant C$. Soit ϕ_m la fonction localement constante définie par $\phi_m(x) = \sum_{i=0}^{p^m-1} \phi(i)\mathbf{1}_{i+p^m\mathbf{Z}_p}$. Si $x \in \mathbf{Z}_p$, il existe $i \in \{0, \ldots, p^m-1\}$ tel que $x \in i+p^m\mathbf{Z}_p$ et $v_p(\phi(x)-\phi_m(x)) = v_p(\phi(x)-\phi(i)) \geqslant C$ par construction de m ; on a donc $v_{\mathscr{C}^0}(\phi - \phi_m) \geqslant C$, ce qui permet de conclure.

Proposition I.2.3. — (i) *Si L contient $\boldsymbol{\mu}_{p^h}$, les ζ^x, pour $\zeta \in \boldsymbol{\mu}_{p^h}$, forment une base de* $\mathrm{LC}_h(\mathbf{Z}_p, L)$.

(ii) *Si L contient $\boldsymbol{\mu}_{p^\infty}$, les ζ^x, pour $\zeta \in \boldsymbol{\mu}_{p^\infty}$, forment une base de* $\mathrm{LC}(\mathbf{Z}_p, L)$.

Démonstration. — On a

$$\sum_{\zeta^{p^h}=1} \zeta^x = \begin{cases} p^h & \text{si } x \in p^h\mathbf{Z}_p, \\ 0 & \text{sinon,} \end{cases}$$

et la fonction caractéristique de $a + p^h\mathbf{Z}_p$ est donc $\frac{1}{p^h}\sum_{\zeta^{p^h}=1} \zeta^{x-a}$. Ceci montre que les ζ^x, pour $\zeta \in \boldsymbol{\mu}_{p^h}$, engendrent $\mathrm{LC}_h(\mathbf{Z}_p, L)$, et comme il y en a le bon nombre, cela permet de conclure.

2. Coefficients de Mahler des fonctions continues. — On définit *la k-ième dérivée discrète* $\phi^{[k]}$ d'une fonction ϕ par récurrence à partir des formules

$$\phi^{[0]} = \phi \quad \text{et} \quad \phi^{[k+1]}(x) = \phi^{[k]}(x+1) - \phi^{[k]}(x),$$

et, si $n \in \mathbf{N}$, on définit le n-ième *coefficient de Mahler* $a_n(\phi)$ de ϕ, par la formule $a_n(\phi) = \phi^{[n]}(0)$. On a aussi

$$\phi^{[k]}(x) = \sum_{i=0}^{k}(-1)^i\binom{k}{i}\phi(x+k-i) \quad \text{et} \quad a_n(\phi) = \sum_{i=0}^{n}(-1)^i\binom{n}{i}\phi(n-i).$$

Lemme I.2.4. — *Si P_n désigne le polynôme binomial $\binom{x}{n}$, alors*

(i) *$P_n^{[k]} = P_{n-k}$ si $k \leqslant n$, et $P_n^{[k]} = 0$ si $k > n$;*

(ii) *$a_k(P_n) = 0$ si $k \neq n$, et $a_k(P_n) = 1$ si $k = n$.*

Démonstration. — C'est une récurrence immédiate à partir de la formule $\binom{x+1}{n+1} - \binom{x}{n+1} = \binom{x}{n}$.

***Théorème I.2.5* (Mahler).** — (i) *Si $\phi \in \mathscr{C}^0(\mathbf{Z}_p, L)$, alors*

a) $\lim_{n\to+\infty} a_n(\phi) = 0$,

b) $\sum_{n=0}^{+\infty} a_n(\phi)\binom{x}{n} = \phi(x)$ *quel que soit $x \in \mathbf{Z}_p$.*

(ii) *L'application $\phi \mapsto a(\phi) = (a_n(\phi))_{n\in\mathbf{N}}$ est une isométrie de $\mathscr{C}^0(\mathbf{Z}_p, L)$ sur $\ell_\infty^0(\mathbf{N}, L)$.*

Corollaire I.2.6. — *Les $\binom{x}{n}$, pour $n \in \mathbf{N}$, forment une base orthonormale de $\mathscr{C}^0(\mathbf{Z}_p, L)$.*

Démonstration. — Le corollaire est immédiat. Passons à la démonstration du théorème.

• La formule définissant $a_n(\phi)$ montre que $v_p(a_n(\phi)) \geqslant v_{\mathscr{C}^0}(\phi)$ quel que soit $n \in \mathbf{N}$. L'application $\phi \mapsto a(\phi)$ est donc une application continue de $\mathscr{C}^0(\mathbf{Z}_p, L)$ dans $\ell_\infty(\mathbf{N}, L)$, et on a $v_{\ell_\infty}(a(\phi)) \geqslant v_{\mathscr{C}^0}(\phi)$.

• Le sous-espace B de $\mathscr{C}^0(\mathbf{Z}_p, L)$ des ϕ tels que $a(\phi) \in \ell^0_\infty(\mathbf{N}, L)$ est fermé dans $\mathscr{C}^0(\mathbf{Z}_p, L)$ puisque $\ell^0_\infty(\mathbf{N}, L)$ est fermé dans $\ell_\infty(\mathbf{N}, L)$.

• Si $a = (a_n)_{n\in\mathbf{N}} \in \ell^0_\infty(\mathbf{N}, L)$, la série $\sum_{n=0}^{+\infty} a_n\binom{x}{n}$ converge normalement dans $\mathscr{C}^0(\mathbf{Z}_p, L)$ en vertu de la proposition I.2.1, et la somme ϕ_a de cette série vérifie $v_{\mathscr{C}^0}(\phi_a) \geqslant v_{\ell_\infty}(a)$. D'autre part, le lemme I.2.4 nous fournit la formule $\phi_a^{[k]}(x) = \sum_{n=0}^{+\infty} a_{n+k}\binom{x}{n}$ et donc $a(\phi_a) = a$.

• L'application $\phi \mapsto a(\phi)$ est injective car « $a(\phi) = 0$ » implique « $\phi(k) = 0$ quel que soit $k \in \mathbf{N}$ », et $\mathbf{N}$ est dense dans $\mathbf{Z}_p$.

Maintenant, si $\phi \in B$, on a $\phi - \phi_{a(\phi)} = 0$ puisque $a(\phi - \phi_{a(\phi)}) = 0$ et a est injective. Donc $\phi \in B$ implique que ϕ satisfait le b) de la propriété (i) du théorème. De plus, on a

$$v_{\ell_\infty}(a(\phi)) \geqslant v_{\mathscr{C}^0}(\phi) = v_{\mathscr{C}^0}(\phi_{a(\phi)}) \geqslant v_{\ell_\infty}(a(\phi)),$$

ce qui montre que ϕ satisfait aussi la propriété (ii) du théorème. Pour démontrer le théorème, il suffit donc de prouver le a) du (i) ou, autrement dit, $B = \mathscr{C}^0(\mathbf{Z}_p, L)$. Or $a_n(\zeta^x) = (\zeta - 1)^n$, si $\zeta \in \boldsymbol{\mu}_{p^\infty}$, et comme $v_p(\zeta - 1) > 0$, il s'ensuit que B contient les ζ^x, pour $\zeta \in \boldsymbol{\mu}_{p^\infty}$, et donc aussi $\mathrm{LC}(\mathbf{Z}_p, L)$. Comme B est fermé et $\mathrm{LC}(\mathbf{Z}_p, L)$ est dense dans $\mathscr{C}^0(\mathbf{Z}_p, L)$, cela permet de conclure.

I.3. Mesures sur $\mathbf{Z}_p$

1. Le dual de $\mathscr{C}^0(\mathbf{Z}_p, L)$. — Si A est un $\mathscr{O}_L$-module complet, on note $\mathscr{D}_0(\mathbf{Z}_p, A)$ l'espace des mesures sur $\mathbf{Z}_p$, à valeurs dans A, c'est-à-dire l'espace des applications $\mathscr{O}_L$-linéaires continues de $\mathscr{C}^0(\mathbf{Z}_p, \mathscr{O}_L)$ dans A. Si A est un L-espace vectoriel, alors tout élément de $\mathscr{D}_0(\mathbf{Z}_p, A)$ s'étend, par linéarité en une application L-linéaire continues de $\mathscr{C}^0(\mathbf{Z}_p, L)$ dans A ; l'espace $\mathscr{D}_0(\mathbf{Z}_p, L)$ sera souvent noté simplement $\mathscr{D}_0(\mathbf{Z}_p)$. Si $\phi \in \mathscr{C}^0(\mathbf{Z}_p, \mathscr{O}_L)$ et $\mu \in \mathscr{D}_0(\mathbf{Z}_p, A)$, on écrira $\mu(\phi)$ sous la forme plus parlante $\int_{\mathbf{Z}_p} \phi(x)\mu(x)$ ou simplement sous la forme $\int_{\mathbf{Z}_p} \phi, \mu$.

On munit l'espace $\mathscr{D}_0(\mathbf{Z}_p)$ des mesures sur $\mathbf{Z}_p$ de la valuation $v_{\mathscr{D}_0}$ du dual définie par

$$v_{\mathscr{D}_0}(\mu) = \inf_{\phi\in\mathscr{C}^0(\mathbf{Z}_p)-\{0\}} v_p\Big(\int_{\mathbf{Z}_p} \phi\,\mu\Big) - v_{\mathscr{C}^0}(\phi),$$

et donc $v_p\big(\int_{\mathbf{Z}_p} \phi\,\mu\big) \geqslant v_{\mathscr{D}_0}(\mu) + v_{\mathscr{C}^0}(\phi)$, pour tout $\phi \in \mathscr{C}^0(\mathbf{Z}_p)$.

A une mesure, on associe la série formelle

$$\mathscr{A}_\mu(T) = \sum_{n=0}^{+\infty} T^n \int_{\mathbf{Z}_p} \binom{x}{n}\mu(x)$$

appelée *transformée d'Amice* de μ. On a formellement

$$\mathscr{A}_\mu(T) = \int_{\mathbf{Z}_p} (1+T)^x\mu(x).$$

Lemme I.3.1. — *Si $|z| < 1$, alors $\int_{\mathbf{Z}_p}(1+z)^x\mu(x) = \mathscr{A}_\mu(z)$*

Démonstration. — La suite de fonctions $\sum_{n=0}^{N}\binom{x}{n}z^n$ converge uniformément sur $\mathbf{Z}_p$ vers $(1+z)^x$ (la valuation $v_{\mathscr{C}^0}$ du reste est $\geqslant (n+1)v_p(z)$) ; on peut donc échanger intégration et somme, d'où le résultat.

Théorème I.3.2. — *L'application qui à une mesure μ associe sa transformée d'Amice est une isométrie de l'espace des mesures muni de la norme ci-dessus sur l'espace des séries formelles à coefficients bornés muni de la norme du sup. des normes des coefficients.*

Démonstration. — C'est une conséquence immédiate du théorème de Malher et du fait que le dual de $l_\infty^0(\mathbf{N})$ est $l_\infty(\mathbf{N})$ (proposition I.1.8).

Remarque I.3.3. — Le th. I.3.2 permet de construire une mesure à partir d'une série entière dont les coefficients sont bornés. On peut aussi utiliser le fait que les fonctions localement constantes sont denses dans les fonctions continues, ce qui permet de définir une mesure, comme expliqué ci-dessous, en ne connaissant que les intégrales $\int_{\mathbf{Z}_p}\mathbf{1}_{a+p^n\mathbf{Z}_p}\mu(x)$ pour $a\in\mathbf{Z}_p$ et $n\in\mathbf{N}$.

Soit μ une mesure sur $\mathbf{Z}_p$. Si $a\in\mathbf{Z}_p$ et $n\in\mathbf{N}$, soit $\mu(a+p^n\mathbf{Z}_p)=\int_{\mathbf{Z}_p}\mathbf{1}_{a+p^n\mathbf{Z}_p}\mu(x)$ *la mesure de* $a+p^n\mathbf{Z}_p$. Comme $a+p^n\mathbf{Z}_p$ est la réunion disjointe des $a+jp^n+p^{n+1}\mathbf{Z}_p$ pour $0\leqslant j\leqslant p-1$, on a $\mu(a+p^n\mathbf{Z}_p)=\sum_{j=0}^{p-1}\mu(a+jp^n+p^{n+1}\mathbf{Z}_p)$. De plus, comme $v_{\mathscr{C}^0}(\mathbf{1}_{a+p^n\mathbf{Z}_p})=0$, les $\mu(a+p^n\mathbf{Z}_p)$ sont bornés. Si ϕ est une fonction continue sur $\mathbf{Z}_p$, alors $\sum_{a=0}^{p^n-1}\phi(a)\mathbf{1}_{a+p^n\mathbf{Z}_p}$ tend vers ϕ dans $\mathscr{C}^0(\mathbf{Z}_p,L)$ et donc

$$\int_{\mathbf{Z}_p}\phi(x)\mu(x)=\lim_{n\to+\infty}\sum_{a=0}^{p^n-1}\phi(a)\mu(a+p^n\mathbf{Z}_p),$$

formule qui ressemble beaucoup à une somme de Riemann.

Réciproquement, si on se donne une famille $\mu(a+p^n\mathbf{Z}_p)$, $a\in\mathbf{Z}_p$, $n\in\mathbf{N}$, d'éléments de L vérifiant les conditions

(i) $\mu(a+p^n\mathbf{Z}_p)=\mu(b+p^n\mathbf{Z}_p)$ si $v_p(a-b)\geqslant n$,

(ii) $\mu(a+p^n\mathbf{Z}_p)=\sum_{j=0}^{p-1}\mu(a+jp^n+p^{n+1}\mathbf{Z}_p)$,

(iii) il existe $C\in\mathbf{R}$ tel que $v_p(\mu(a+p^n\mathbf{Z}_p))\geqslant C$ quels que soient $a\in\mathbf{Z}_p$ et $n\in\mathbf{N}$,

alors les propriétés (i) et (ii) permettent d'étendre μ en une forme linéaire sur $\mathrm{LC}(\mathbf{Z}_p,L)$, et la propriété (iii) permet de montrer que $v_p(\mu(\phi))\geqslant v_{\mathscr{C}^0}(\phi)+C$, ce qui permet d'étendre μ, par continuité, à $\mathscr{C}^0(\mathbf{Z}_p,L)$.

Remarque I.3.4. — Il y a 2 topologies naturelles que l'on peut mettre sur $\mathbf{Z}_p[[T]]$.

-La topologie donnée par le sup. des normes des coefficients

-la topologie de la limite projective $\mathbf{Z}_p[[T]]=\varprojlim\mathbf{Z}_p[T]/T^n$ qui en fait un anneau compact

Proposition I.3.5. — *La première correspond à la topologie de la convergence forte sur les mesures et la seconde à la topologie de la convergence faible. (i.e. un suite $(\mu_n)_{n\in\mathbf{N}}$ de mesures converge si pour toute fonction continue ϕ, la suite $\int_{\mathbf{Z}_p}\phi\,\mu_n$ converge).*

Démonstration. — Exercice.

2. Exemples de mesures et opérations sur les mesures

• *La mesure de Haar.*— On cherche une mesure invariante par translation sur $\mathbf{Z}_p$, ce qui implique $\mu(a+p^n\mathbf{Z}_p)=\frac{1}{p^n}\mu(\mathbf{Z}_p)$ quels que soient $a\in\mathbf{Z}_p$ et $n\in\mathbf{N}$. Ceci n'est possible que si $\mu(\mathbf{Z}_p)=0$ (et donc si $\mu=0$) car on doit avoir $v_p(\mu(a+p^n\mathbf{Z}_p))\geqslant v_{\mathscr{D}_0}(\mu)$, pour tous $a\in\mathbf{Z}_p$ et $n\in\mathbf{N}$. Il n'y a donc pas de mesure de Haar en p-adique et donc aucun moyen canonique d'associer une mesure à une fonction.

• *Masses de Dirac.*— si $a\in\mathbf{Z}_p$, soit Dir_a la masse de Dirac en a, c'est-à-dire la mesure qui à f associe $f(a)$. Sa transformée d'Amice est $(1+T)^a$.

Comme les polynômes sont denses dans $\mathscr{E}^+$, l'espace vectoriel engendré par les masses de Dirac (et même celui engendré par les masses de Dirac aux entiers $\geqslant 0$) est dense dans $\mathscr{D}_0(\mathbf{Z}_p,L)$.

• *Multiplication par une fonction.*— Si μ est une mesure sur $\mathbf{Z}_p$ et f est une fonction continue sur $\mathbf{Z}_p$, on définit la mesure $f\mu$ par la formule $\int_{\mathbf{Z}_p}\phi\,(g\mu)=\int_{\mathbf{Z}_p}f\phi\,\mu$.

—*Multiplication par x.* On a $x\cdot\binom{x}{n}=((x-n)+n)\binom{x}{n}=(n+1)\binom{x}{n+1}+n\binom{x}{n}$. On en déduit la formule

$$\mathscr{A}_{x\mu}=\partial\mathscr{A}_\mu,\quad \text{avec } \partial=(1+T)\frac{d}{dT}.$$

—*Multiplication par z^x si* $v_p(z-1)>0$. D'après le lemme I.3.1, si $v_p(y-1)>0$, et si λ est une mesure sur $\mathbf{Z}_p$, alors $\int_{\mathbf{Z}_p}y^x\lambda(x)=\mathscr{A}_\lambda(y-1)$. Appliquant ceci à $\lambda=z^x\mu$, on obtient $\mathscr{A}_\lambda(y-1)=\mathscr{A}_\mu(yz-1)$ quel que soit $y\in B(0,0^+)$. On en déduit la formule

$$\mathscr{A}_{z^x\mu}(T)=\mathscr{A}_\mu((1+T)z-1).$$

• *Restriction à un ouvert compact.*— C'est la multiplication par la fonction caractéristique de l'ouvert compact. Si $n\in\mathbf{N}$ et $b\in\mathbf{Z}_p$, la fonction caractéristique de $b+p^n\mathbf{Z}_p$ est $x\mapsto p^{-n}\sum_{\eta^{p^n}=1}\eta^{-b}\eta^x$. Cela se traduit, au niveau des transformées d'Amice, par la formule

$$\mathscr{A}_{\mathrm{Res}_{b+p^n\mathbf{Z}_p}(\mu)}(T)=p^{-n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{-b}\mathscr{A}_\mu((1+T)\eta-1).$$

• *Convolution des mesures.*

Lemme I.3.6. — *Si f est une fonction continue sur $\mathbf{Z}_p$ et μ est une mesure sur $\mathbf{Z}_p$, la fonction $\mu*f$ définie par $\int_{\mathbf{Z}_p}f(x+y)\mu(x)$ est une fonction continue de $y\in\mathbf{Z}_p$ et l'appliction $f\to\mu*f$ est une application linéaire continue de $\mathscr{C}^0(\mathbf{Z}_p,\mathbf{Q}_p)$ dans lui-même.*

Démonstration. — La continuité de $\mu*f$ est une conséquence de l'uniforme continuité de f et d'autre part, $\|\mu*f\|_\infty\leqslant\|\mu\|\|f\|_\infty$ d'où la continuité de $f\to\mu*f$.

Ceci nous permet, si λ et μ sont deux mesures sur $\mathbf{Z}_p$ de définir leur convolée $\lambda*\mu$ par la formule $\lambda*\mu(f)=\lambda(\mu*f)$ ou encore

$$\int_{\mathbf{Z}_p}f(x)\lambda*\mu(x)=\int_{\mathbf{Z}_p}\Big(\int_{\mathbf{Z}_p}f(x+y)\mu(x)\Big)\lambda(y).$$

Un calcul immédiat nous donne $\delta_a*\delta_b=\delta_{a+b}$.

D'autre part, si $|z| < 1$, alors

$$\int_{\mathbf{Z}_p}\Big(\int_{\mathbf{Z}_p}(1+z)^{x+y}\mu(x)\Big)\lambda(y) = \mathscr{A}_\mu(z)\int_{\mathbf{Z}_p}(1+z)^y\lambda(y) = \mathscr{A}_\mu(z)\mathscr{A}_\lambda(z);$$

On en déduit la formule

$$\mathscr{A}_{\lambda*\mu}(T) = \mathscr{A}_\lambda(T)\mathscr{A}_\mu(T)$$

ce qui prouve que les mesures munies de la convolution forment une algèbre commutative et associative et que $\mu \to \mathscr{A}_\mu$ est un isomorphisme d'algèbres de l'espace des mesures sur celui des séries entières bornées.

Remarque I.3.7. — La formule $\mathscr{A}_{\lambda*\mu} = \mathscr{A}_\lambda\mathscr{A}_\mu$ montre que si $\delta_a * \mu = \mu$ quel que soit $a \in \mathbf{Z}_p$, alors $\mu = 0$. On retrouve la non existence de mesures de Haar p-adiques.

• *Actions de P^+ et ψ.*— Ces actions permettent de faire le lien entre la théorie des (φ,Γ)-modules et celles des mesures. On note P^+ le semi-groupe $\left(\begin{smallmatrix}\mathbf{Z}_p-\{0\} & \mathbf{Z}_p\\ 0 & 1\end{smallmatrix}\right)$.

— On fait agir $\left(\begin{smallmatrix}p^ka & b\\ 0 & 1\end{smallmatrix}\right) \in P^+$, avec $k \in \mathbf{N}$, $a \in \mathbf{Z}_p^*$ et $b \in \mathbf{Z}_p$, sur une mesure μ, par :

$$\int_{\mathbf{Z}_p}\phi(x)\left(\begin{smallmatrix}p^ka & b\\ 0 & 1\end{smallmatrix}\right)\cdot\mu = \int_{\mathbf{Z}_p}\phi(p^kax+b)\,\mu \quad \text{et on a} \quad \mathscr{A}_{\left(\begin{smallmatrix}p^ka & b\\ 0 & 1\end{smallmatrix}\right)\cdot\mu}(T) = (1+T)^b\varphi^k(\sigma_a(\mathscr{A}_\mu)),$$

où l'on a posé

$$\varphi(f(T)) = f((1+T)^p-1) \quad \text{et} \quad \sigma_a(f(T)) = f((1+T)^a-1), \text{ si } a \in \mathbf{Z}_p^*.$$

— Si μ est une mesure sur $\mathbf{Z}_p$, on note $\psi(\mu)$ la mesure sur $\mathbf{Z}_p$ définie par

$$\int_{\mathbf{Z}_p}\phi(x)\,\psi(\mu) = \int_{p\mathbf{Z}_p}\phi(p^{-1}x)\,\mu \quad \text{et on a} \quad \mathscr{A}_{\psi(\mu)}((1+T)^p-1) = \frac{1}{p}\sum_{\zeta^p=1}\mathscr{A}_\mu((1+T)\zeta-1),$$

et donc $\mathscr{A}_{\psi(\mu)} = \psi(\mathscr{A}_\mu)$.

On définit une action de φ sur une mesure comme étant celle de $\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)$; on a donc $\mathscr{A}_{\varphi(\mu)} = \varphi(\mathscr{A}_\mu)$. Alors φ et ψ commutent à l'action de $\left(\begin{smallmatrix}\mathbf{Z}_p^* & 0\\ 0 & 1\end{smallmatrix}\right)$; on a $\psi\circ\varphi = \mathrm{id}$ et $\varphi\circ\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & pb\\ 0 & 1\end{smallmatrix}\right)\circ\varphi$ et $\psi\circ\left(\begin{smallmatrix}1 & pb\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)\circ\psi$, si $b \in \mathbf{Z}_p$.

Par ailleurs, « $\psi(\mu) = 0$ » si et seulement si « μ est à support dans $\mathbf{Z}_p^*$ », et

$$\mathrm{Res}_{\mathbf{Z}_p^*}(\mu) = (1-\varphi\circ\psi)\mu.$$

I.4. Dictionnaire d'analyse fonctionnelle p-adique

1. Le corps $\mathscr{E}$. — Soit $\mathscr{E}$ l'ensemble des séries de Laurent $\sum_{k\in\mathbf{Z}} a_kT^k$, avec $a_k \in L$, telles que la suite $(v_p(a_k))_{k\in\mathbf{Z}}$ soit minorée et vérifie $\lim_{k\to-\infty} v_p(a_k) = +\infty$. Muni de la valuation $v^{\{0\}}$ définie par $v^{\{0\}}(\sum_{k\in\mathbf{Z}} a_kT^k) = \inf_{k\in\mathbf{Z}} v_p(a_k)$, le corps $\mathscr{E}$ est un corps complet pour une valuation discrète. L'anneau $\mathscr{O}_\mathscr{E}$ des entiers de $\mathscr{E}$ est l'anneau des séries de Laurent $\sum_{k\in\mathbf{Z}} a_kT^k$, avec $a_k \in \mathscr{O}_L$, telles que la suite $v_p(a_k)$ vérifie $\lim_{k\to-\infty} v_p(a_k) = +\infty$. Le corps résiduel $k_\mathscr{E}$ de $\mathscr{E}$ est $k_L((T))$.

On note $\mathscr{O}_{\mathscr{E}}^+$ le sous-anneau $\mathscr{O}_L[[T]]$ de $\mathscr{O}_{\mathscr{E}}$, $\mathscr{E}^+$ le sous-anneau $\mathscr{O}_{\mathscr{E}}^+[\frac{1}{p}]$ de $\mathscr{E}$ et $k_{\mathscr{E}}^+ = k_L[[T]]$ l'anneau des entiers de $k_{\mathscr{E}}$. Les anneaux $\mathscr{O}_{\mathscr{E}}^+$, $\mathscr{E}^+$ et $k_{\mathscr{E}}^+$ sont aussi parfois notés $\mathscr{O}_{\mathscr{E}}^\natural$, $\mathscr{E}^\natural$ et $k_{\mathscr{E}}^\natural$ suivant le contexte.

La topologie naturelle sur $\mathscr{O}_{\mathscr{E}}$ n'est pas celle définie par la valuation $v^{\{0\}}$ (*topologie forte*) : c'est la *topologie faible* qui est la topologie d'anneau la plus faible rendant continue la réduction $\mathscr{O}_{\mathscr{E}} \to k_{\mathscr{E}}$ modulo $\mathfrak{m}_L$, si $k_{\mathscr{E}}$ est muni de la topologie induite par la valuation v_T ; cette topologie est obtenue en munissant $\mathscr{O}_{\mathscr{E}}$ de la base de voisinages de 0 donnée par les $p^k\mathscr{O}_{\mathscr{E}} + T^n\mathscr{O}_{\mathscr{E}}^+$, pour $k, n \in \mathbf{N}$. On munit alors $\mathscr{E} = \cup_{m\in\mathbf{N}} p^{-m}\mathscr{O}_{\mathscr{E}}$ de la topologie de la limite inductive.

2. Résidus. — Soit $\Gamma = \mathrm{Gal}(\mathbf{Q}_p(\boldsymbol{\mu}_{p^\infty})/\mathbf{Q}_p)$. Le caractère cyclotomique χ induit un isomorphisme de Γ sur $\mathbf{Z}_p^*$; si $a \in \mathbf{Z}_p^*$, on note $\sigma_a \in \Gamma$ l'image inverse de a par χ. Les actions de φ et Γ définies ci-dessus sur $\mathscr{O}_{\mathscr{E}}^+$ (i.e. $\varphi(T) = (1+T)^p - 1$ et $\sigma_a(T) = (1+T)^a - 1$) s'étendent à $\mathscr{O}_{\mathscr{E}}$ et $\mathscr{E}$; celle de ψ demande à être réinterprétée. Le corps $\mathscr{E}$ est une extension de degré p de $\varphi(\mathscr{E})$, ce qui permet de définir un inverse à gauche ψ de φ par la formule $\psi(f) = p^{-1}\varphi^{-1}(\mathrm{Tr}_{\mathscr{E}/\varphi(\mathscr{E})} f)$. Alors ψ laisse stable $\mathscr{O}_{\mathscr{E}}$.

- ψ commute à Γ,
- $\psi(f\varphi(g)) = g\psi(f)$, pour tous f, g,
- $\psi\big(\sum_{i=0}^{p-1}(1+T)^i\varphi(f_i)\big) = f_0$,
- $\psi(f)\big((1+T)^p - 1\big) = \frac{1}{p}\sum_{\zeta^p=1} f\big((1+T)\zeta - 1\big)$, si $f \in \mathscr{O}_{\mathscr{E}}^+$. (En effet, les $f\big((1+T)\zeta - 1\big)$ sont les conjugués de f sous l'action de $\mathrm{Gal}(\mathscr{E}/\varphi(\mathscr{E}))$.)
- $\psi(\frac{1}{T}) = \frac{1}{T}$. (En effet, $\frac{1}{T} = \sum_{i=0}^{p-1}(1+T)^i\varphi(\frac{1}{T})$.)

Si $f = \sum_{k\in\mathbf{Z}} a_kT^k$ est un élément de $\mathscr{E}$, on définit le résidu de la forme différentielle $\omega = f\,dT$ par la formule $\mathrm{rés}_0(\omega) = a_{-1}$. On a $\mathrm{rés}_0(df) = 0$, si $f \in \mathscr{E}$.

Comme $\mathrm{rés}_0$ envoie $\mathscr{O}_{\mathscr{E}}\,\frac{dT}{1+T}$ dans $\mathscr{O}_L$, elle induit une application $\mathrm{rés}_0 : \mathscr{E}/\mathscr{O}_{\mathscr{E}}\,\frac{dT}{1+T} \to L/\mathscr{O}_L$.

On note ∂ l'opérateur différentiel $(1+T)\frac{d}{dT}$ de telle sorte que $df = \partial f\,\frac{dT}{1+T}$.

Lemme I.4.1. — *On a*

$$\partial\circ\varphi = p\,\varphi\circ\partial, \quad p\,\partial\circ\psi = \psi\circ\partial \quad \text{et} \quad \partial\circ\sigma_a = a\,\sigma_a\circ\partial, \ \textit{si } a \in \mathbf{Z}_p^*.$$

Démonstration. — Dans le cas de φ et σ_a, cela résulte de ce que, si $b \in \mathbf{Z}_p$,

$$\begin{aligned}\partial\big(f((1+T)^b - 1)\big) &= \partial((1+T)^b - 1)f'((1+T)^b - 1)\\ &= b\,(1+T)^b f'((1+T)^b - 1) = (\partial f)((1+T)^b - 1).\end{aligned}$$

Maintenant, si $f = \sum_{i=0}^{p=1}(1+T)^i\varphi(f_i)$, on a

$$\partial f = \sum_{i=0}^{p-1}\big(i(1+T)^i\varphi(f_i) + p(1+T)^i\varphi(\partial f_i)\big) = \sum_{i=0}^{p-1}(1+T)^i\varphi(if_i + p\partial f_i),$$

et donc $\psi(\partial f) = p\partial f_0 = p\partial(\psi(f))$. Ceci permet de conclure.

Proposition I.4.2. — *Si $f \in \mathscr{E}$, alors :*

(i) $\mathrm{rés}_0(\sigma_a(f)\,\frac{dT}{1+T}) = a^{-1}\mathrm{rés}_0(f\,\frac{dT}{1+T})$, *pour tout $a \in \mathbf{Z}_p^*$,*

(ii) $\mathrm{rés}_0(\varphi(f)\,\frac{dT}{1+T}) = \mathrm{rés}_0(\psi(f)\,\frac{dT}{1+T}) = \mathrm{rés}_0(f\,\frac{dT}{1+T})$.

Démonstration. — Soit $f \in \mathscr{E}$. S'il existe $g \in \mathscr{E}$ tel que $f = \partial g$, alors $f\frac{dT}{1+T} = dg$ et, d'après le lemme I.4.1, on a $\psi(f)\frac{dT}{1+T} = pd(\psi(g))$ et $\sigma_a(f)\frac{dT}{1+T} = a^{-1}d(\sigma_a(g))$. On a donc, dans ce cas $\mathrm{rés}_0(f\,\frac{dT}{1+T}) = \mathrm{rés}_0(\psi(f)\,\frac{dT}{1+T}) = \mathrm{rés}_0(\sigma_a(f)\,\frac{dT}{1+T}) = 0$. Ceci s'applique en particulier à $f = T^{k-1}(1+T)$, si $k \in \mathbf{Z} - \{0\}$. Comme l'adhérence dans $\mathscr{O}_{\mathscr{E}}$ du $\mathscr{O}_L$-module engendré par les $T^{k-1}(1+T)$, pour $k \in \mathbf{Z} - \{0\}$, admet $\mathscr{O}_L \cdot \frac{1}{T}$ comme supplémentaire, on déduit les formules de la proposition pour ψ et σ_a de ce que

$$\psi(\frac{1}{T}) = \frac{1}{T} \quad \text{et} \quad \sigma_a(\frac{1}{T}) = \frac{1}{aT + \binom{a}{2}T^2 + \cdots} = \frac{1}{aT} + \frac{a-1}{2} + \cdots .$$

Enfin, la formule pour φ se déduit de celle pour ψ appliquée à $\varphi(f)$. Ceci permet de conclure.

Si $f \in \mathscr{R}$ ou si $f \in \mathscr{E}$, on définit $\phi_f : \mathbf{Z}_p \to L$ par la formule

$$\phi_f(x) = \mathrm{rés}_0\big((1+T)^x f(T)\,\frac{dT}{1+T}\big).$$

Théorème I.4.3. — (i) *L'application $\mu \mapsto A_\mu(T)$ induit des isomorphismes de $\mathscr{D}_0(\mathbf{Z}_p, \mathscr{O}_L)$ sur $\mathscr{O}_{\mathscr{E}}^\natural$ et de $\mathscr{D}_0(\mathbf{Z}_p)$ sur $\mathscr{E}^\natural$.*

(ii) *L'application $f \mapsto \phi_f$ induit des isomorphismes de $\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}^\natural$ sur $\mathscr{C}^0(\mathbf{Z}_p, \mathscr{O}_L)$ et de $\mathscr{E}/\mathscr{E}^\natural$ sur $\mathscr{C}^0(\mathbf{Z}_p)$.*

(iii) *Si $\mu \in \mathscr{D}_0(\mathbf{Z}_p)$ et $f \in \mathscr{E}$, alors $\int_{\mathbf{Z}_p} \phi_f\,\mu = \mathrm{rés}_0\big(A_\mu f\,\frac{dT}{1+T}\big)$.*

Démonstration. — Le (i) a déjà été démontré (th. I.3.2). Pour démontrer le (ii), considérons $\psi_f(x) = \mathrm{rés}_0\big((1+T)^x f(T) dT\big)$, si $f = \sum_{k\in\mathbf{Z}} a_k T^k$ appartient à $\mathscr{O}_{\mathscr{E}}$, $\mathscr{E}$ ou $\mathscr{R}$. Comme $(1+T)^x = \sum_{k\in\mathbf{N}} \binom{x}{k} T^k$, on a $\psi_f(x) = \sum_{k\in\mathbf{N}} a_{-1-k}\binom{x}{k}$. On en déduit, en utilisant la définition de $\mathscr{O}_{\mathscr{E}}$ ou $\mathscr{E}$, et le th. de Mahler, que $f \mapsto \psi_f$ induit des isomorphismes de $\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}^\natural$ sur $\mathscr{C}^0(\mathbf{Z}_p, \mathscr{O}_L)$, et de $\mathscr{E}/\mathscr{E}^\natural$ sur $\mathscr{C}^0(\mathbf{Z}_p)$. Comme $\phi_f(x) = \psi_f(x-1)$, cela démontre le (ii). Le (iii) peut se réécrire sous la forme

$$\mathrm{rés}_0\Big(\big(f(T)\int_{\mathbf{Z}_p}(1+T)^x\,\mu\big)\,\frac{dT}{1+T}\Big) = \int_{\mathbf{Z}_p} \mathrm{rés}_0\Big(f(T)(1+T)^x\,\frac{dT}{1+T}\Big)\,\mu,$$

ce qui suit formellement de la linéarité de $\int_{\mathbf{Z}_p}$ et de $\mathrm{rés}_0$.

I.5. Mesures sur $\mathbf{Q}_p$

1. Mesures sur $\mathbf{Q}_p$ et familles de mesures sur $\mathbf{Z}_p$. — Une mesure μ sur $\mathbf{Q}_p$ est un élément du dual de l'espace $\mathscr{C}_c^0(\mathbf{Q}_p)$ des fonctions continues à support compact dans $\mathbf{Q}_p$. Si μ est une telle mesure, et si $n \in \mathbf{N}$, on note $\mu^{(n)}$ l'élément de $\mathscr{D}_0(\mathbf{Z}_p)$ défini par

$$\int_{\mathbf{Z}_p} \phi\,\mu^{(n)} = \int_{p^{-n}\mathbf{Z}_p} \phi(p^n x)\mu,$$

si $\phi \in \mathscr{C}^0(\mathbf{Z}_p)$. Il n'est pas difficile de vérifier que l'on a $\psi(\mu^{(n+1)}) = \mu^{(n)}$ si $n \in \mathbf{N}$. Réciproquement, si $(\mu_n)_{n\in\mathbf{N}}$ est une famille de mesures sur $\mathbf{Z}_p$ vérifiant $\psi(\mu_{n+1}) = \mu_n$ si $n \in \mathbf{N}$, alors il existe une unique mesure μ sur $\mathbf{Q}_p$ telle que l'on ait $\mu^{(n)} = \mu_n$ quel que soit $n \in \mathbf{N}$: si $\phi \in \mathscr{C}_c^0(\mathbf{Q}_p)$ est à support dans $p^{-n}\mathbf{Z}_p$, alors $\int_{\mathbf{Q}_p} \phi(x)\,\mu = \int_{\mathbf{Z}_p} \phi(p^{-n}x)\mu_n$, la relation $\psi(\mu_{n+1}) = \mu_n$ permettant de montrer que $\int_{\mathbf{Z}_p} \phi(p^{-n}x)\mu_n$ ne dépend pas du choix de n tel que ϕ soit à support dans $p^{-n}\mathbf{Z}_p$.

Une mesure μ sur $\mathbf{Q}_p$ est dite bornée, s'il existe $C \in \mathbf{R}$ tel que $v_p(\int_{\mathbf{Q}_p} \phi\, \mu) \geqslant v_{\mathscr{C}^0}(\phi) + C$, pour tout $\phi \in \mathscr{C}_c^0(\mathbf{Q}_p)$. On note $\mathscr{D}_0(\mathbf{Q}_p)$ l'espace des mesures bornées sur $\mathbf{Q}_p$; c'est le dual de l'espace des fonctions continues sur $\mathbf{Q}_p$ tendant vers 0 à l'infini, et on a $\mathscr{D}_0(\mathbf{Q}_p) = L \otimes_{\mathscr{O}_L} \mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$.

On note $\mathscr{A}_\mu^{(n)}$ la transformée d'Amice de $\mu^{(n)}$, et on définit la transformée d'Amice $\mathscr{A}_\mu$ de μ par la formule $\mathscr{A}_\mu = (\mathscr{A}_\mu^{(n)})_{n\in\mathbf{N}}$.

Proposition I.5.1. — *L'application $\mu \mapsto \mathscr{A}_\mu$ induit une bijection de l'espace des mesures sur $\mathbf{Q}_p$ (resp. de $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$) sur l'ensemble des suites $F = (F^{(n)})_{n\in\mathbf{N}}$ d'éléments de $\mathscr{E}^+$ (resp. de $\mathscr{O}_{\mathscr{E}}^+$) vérifiant $\psi(F^{(n+1)}) = F^{(n)}$ quel que soit $n \in \mathbf{N}$.*

Démonstration. — C'est une simple traduction du résultat correspondant sur $\mathbf{Z}_p$.

2. Action du sous-groupe mirabolique de $\mathbf{GL}_2(\mathbf{Q}_p)$. — On munit $\mathscr{D}(\mathbf{Q}_p)$ d'une action de $P(\mathbf{Q}_p) = \{\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right),\ a \in \mathbf{Q}_p^*, b \in \mathbf{Q}_p\}$ en posant

$$\int_{\mathbf{Q}_p} \phi(x)\ \left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right) \star \mu = \int_{\mathbf{Q}_p} \phi(ax+b)\, \mu.$$

Si $n \in \mathbf{N}$ est tel que $p^n a \in \mathbf{Z}_p$ et $p^n b \in \mathbf{Z}_p$, et si ϕ est une fonction à support dans $\mathbf{Z}_p$, on a

$$\int_{p^{-n}\mathbf{Z}_p} \phi(p^n x) \left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right) \star \mu = \int_{p^{-n-v_p(a)}\mathbf{Z}_p} \phi(p^n ax + p^n b)\mu,$$

ce qui, appliqué à $\phi(x) = (1+T)^x$, nous donne

$$\mathscr{A}^{(n)}_{\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right)\star\mu}(T) = (1+T)^{p^n b} \mathscr{A}_\mu^{(n+v_p(a))}((1+T)^{p^{-v_p(a)}a} - 1),\ \text{si } n \geqslant \sup(-v_p(a), -v_p(b)).$$

On remarquera que, si $\mu \in \mathscr{D}(\mathbf{Q}_p)$, et si $n \in \mathbf{Z}$, alors $\mu^{(n)}$ est aussi donné par la formule

$$\mu^{(n)} = \left(\begin{smallmatrix} p^n & 0 \\ 0 & 1\end{smallmatrix}\right) \star (\mathrm{Res}_{p^{-n}\mathbf{Z}_p}\mu) = \mathrm{Res}_{\mathbf{Z}_p}(\left(\begin{smallmatrix} p^n & 0 \\ 0 & 1\end{smallmatrix}\right) \star \mu).$$

3. Les anneaux $\widetilde{\mathscr{O}}_{\mathscr{E}}$ et $\widetilde{\mathscr{O}}_{\mathscr{E}}^+$. — Soit $\mathbf{A}_{\mathbf{Q}_p}$ l'ensemble des $f \in \mathscr{O}_{\mathscr{E}}$ à coefficients dans $\mathbf{Z}_p$. Le corps résiduel $\mathbf{E}_{\mathbf{Q}_p}$ de $\mathbf{A}_{\mathbf{Q}_p}$ n'est autre que $\mathbf{F}_p((T))$, et on note $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ le complété de sa clôture radicielle (pour la valuation v_T) ; celui-ci est naturellement muni d'actions continues de Γ et φ, commutant entre elles et coïncidant avec celles précédemment définies sur $\mathbf{E}_{\mathbf{Q}_p} \subset k_{\mathscr{E}}$.

On note $\widetilde{\mathbf{A}}_{\mathbf{Q}_p} = W(\widetilde{\mathbf{E}}_{\mathbf{Q}_p})$ l'anneau des vecteurs de Witt à coefficients dans $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$; comme $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ est parfait, tout élément de $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}$ s'écrit de manière unique sous la forme $\sum_{k=0}^{+\infty} p^k[x_k]$, où les x_k sont des éléments de $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ et $[x]$ désigne le représentant de Teichmüller de x dans $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}$, si $x \in \widetilde{\mathbf{E}}_{\mathbf{Q}_p}$. Les actions de Γ et φ sur $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ s'étendent de manière unique à $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}$, l'action de φ devenant bijective, et $\mathbf{A}_{\mathbf{Q}_p}$ (muni des actions de φ et Γ) s'identifie naturellement au sous-anneau de $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}$ engendré topologiquement par $[1+T]-1$ (que l'on identifie à $T \in \mathbf{A}_{\mathbf{Q}_p}$) et son inverse.

On dispose d'un[(1)] analogue p-adique $x \mapsto [(1+T)^x]$ de $x \mapsto e^{2i\pi x}$: si $p^n x \in \mathbf{Z}_p$, alors

$$[(1+T)^x] = \varphi^{-n}((1+T)^{p^n x}) = \varphi^{-n}\Big(\sum_{k=0}^{+\infty} \binom{p^n x}{k} T^k\Big).$$

Comme on a identifié $[1+T]-1$ à T, on a $[(1+T)^x] = (1+T)^x$, si $x \in \mathbf{Z}_p$. On fera attention au fait que ce n'est pas le cas si $x \notin \mathbf{Z}_p$: la série définissant $(1+T)^x$ ne converge pas dans $\widetilde{\mathbf{A}}^+_{\mathbf{Q}_p}$, et si on complète $\widetilde{\mathbf{A}}^+_{\mathbf{Q}_p}[\frac{1}{p}]$ pour obtenir un anneau dans lequel cette série converge, on tombe sur la fonction $x \mapsto e^{tx}$ de la note de bas de page.

On note $\widetilde{\mathscr{O}}_{\mathscr{E}}$ l'anneau $\mathscr{O}_L \otimes_{\mathbf{Z}_p} \widetilde{\mathbf{A}}_{\mathbf{Q}_p}$ auquel on étend par $\mathscr{O}_L$-linéarité les actions de φ et Γ. On a alors $\widetilde{\mathscr{O}}_{\mathscr{E}} = (\mathscr{O}_L \otimes_{\mathbf{Z}_p} \widetilde{\mathbf{A}})^{\mathscr{H}}$, l'action résiduelle de Γ étant celle définie ci-dessus. De plus, $(\mathscr{O}_L \otimes_{\mathbf{Z}_p} \widetilde{\mathbf{A}})^{\varphi=1} = \mathscr{O}_L$.

4. Traces de Tate normalisées. — Soit $I = p^{-\infty}\mathbf{Z} \cap [0,1[$; c'est un système de représentants de $\mathbf{Q}_p/\mathbf{Z}_p$. Si $m \in \mathbf{N}$, soit $I_m = \{i \in I \mid v_p(i) \geqslant -m\}$, ce qui fait que I est la réunion croissante pour $m \in \mathbf{N}$ des I_m. Soit aussi $\mathbf{E}_{\mathbf{Q}_p,m} = \varphi^{-m}(\mathbf{E}_{\mathbf{Q}_p})$; alors $\mathbf{E}_{\mathbf{Q}_p,\infty} = \cup_{m\in\mathbf{N}} \mathbf{E}_{\mathbf{Q}_p,m}$ est la clôture radicielle de $\mathbf{E}_{\mathbf{Q}_p}$.

Lemme I.5.2. — *Si $m \in \mathbf{N}$, les $(1+T)^i$, pour $i \in I_m$, forment une base de $\mathbf{E}^+_{\mathbf{Q}_p,m}$ sur $\mathbf{E}^+_{\mathbf{Q}_p}$.*

Démonstration. — T étant une uniformisante de $\mathbf{E}_{\mathbf{Q}_p}$, tout élément de $\mathbf{E}^+_{\mathbf{Q}_p}$ peut s'écrire de manière unique sous la forme

$$\sum_{n=0}^{+\infty} a_n T^n = \sum_{r=0}^{p^m-1} T^r \varphi^m(b_r),$$

où les a_n sont des éléments de k_F et $b_r = \sum_{k=0}^{+\infty} a_{r+kp^m} T^k$. On en déduit le fait que les T^r pour $0 \leqslant r \leqslant p^m-1$ forment une base de $\mathbf{E}^+_{\mathbf{Q}_p}$ sur $\varphi^m(\mathbf{E}^+_{\mathbf{Q}_p})$ et la matrice faisant passer de T^r aux $(1+T)^r$ étant triangulaire avec des 1 sur la diagonale, il en est de même des $(1+T)^r$ pour $0 \leqslant r \leqslant p^m-1$. Il n'y a plus qu'à appliquer φ^{-m} pour en déduire le lemme.

Proposition I.5.3. — (i) *tout élément x de $\mathbf{E}_{\mathbf{Q}_p,m}$ s'écrit de manière unique sous la forme $x = \sum_{i\in I_m} (1+T)^i a_i(x)$, où $a_i(x) \in \mathbf{E}_{\mathbf{Q}_p}$ si $i \in I$, et on a l'encadrement*

$$v_T(x) - 1 < \inf_{i\in I_m} v_T(a_i(x)) \leqslant v_T(x);$$

(ii) *tout élément x de $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ s'écrit de manière unique sous la forme $x = \sum_{i\in I} (1+T)^i a_i(x)$, où $(a_i(x))_{i\in I}$ est une suite d'éléments de $\mathbf{E}_K$ tendant vers 0 suivant le filtre des complémentaires des parties finies, et on a l'encadrement*

$$v_T(x) - 1 < \inf_{i\in I} v_T(a_i(x)) \leqslant v_T(x).$$

[(1)] On a en fait trois tels analogues : en sus de $x \mapsto [(1+T)^x]$, on peut considérer $x \mapsto e^{tx}$, où $t = \log(1+T)$ est le $2i\pi$ p-adique de Fontaine, ainsi que $x \mapsto \varepsilon(x) = e^{-tx}[(1+T)^x]$ qui est à valeurs dans $\boldsymbol{\mu}_{p^\infty}$.

Démonstration. — Une base de $\mathbf{E}^+_{\mathbf{Q}_p,m}$ sur $\mathbf{E}^+_{\mathbf{Q}_p}$ est aussi une base de $\mathbf{E}_{\mathbf{Q}_p,m}$ sur $\mathbf{E}_{\mathbf{Q}_p}$; on en déduit l'existence et l'unicité de l'écriture.

D'autre part, l'inégalité $\inf_{i\in I_m} v_T(a_i(x)) \leqslant v_T(x)$ est une évidence ; l'autre inégalité est une conséquence des deux remarques suivantes :

(a) $\inf_{i\in I_m} v_T(a_i(x)) \geqslant 0$ si $v_T(x) \geqslant 0$ (les $(1+T)^i$ forment une base de $\mathbf{E}^+_{\mathbf{Q}_p,m}$ sur $\mathbf{E}^+_{\mathbf{Q}_p}$).

(b) $a_i(T^k x) = T^k a_i(x)$ si $k \in \mathbf{Z}$ (par unicité de l'écriture).

Maintenant, $\cup_{m\in\mathbf{N}}\mathbf{E}_{\mathbf{Q}_p,m}$ est dense dans $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ et l'inégalité $v_T(a_i(x)) > v_T(x) - 1$ montre que a_i s'étend par continuité en une application $\mathbf{F}_p$-linéaire continue de $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$ dans $\mathbf{E}_{\mathbf{Q}_p}$, ce qui permet de déduire le (ii) du (i) par passage à la limite.

Remarque I.5.4. — Le lemme I.5.2 montre que l'on $a_i(x) \in \mathbf{E}^+_{\mathbf{Q}_p}$ si $x \in \mathbf{E}^+_{\mathbf{Q}_p,m}$; un passage à la limite montre que ceci reste vrai si $x \in \widetilde{\mathbf{E}}^+_{\mathbf{Q}_p}$.

Si $m \in \mathbf{N}$, on note $\mathbf{A}_{\mathbf{Q}_p,m}$ le sous-anneau $\varphi^{-m}(\mathbf{A}_{\mathbf{Q}_p})$ de $\widetilde{\mathbf{A}}$. On a donc $\mathbf{A}_{\mathbf{Q}_p,m}/p\mathbf{A}_{\mathbf{Q}_p,m} = \mathbf{E}_{\mathbf{Q}_p,m}$. On note $\mathscr{O}_{\mathscr{E},m}$ le sous-anneau $\mathscr{O}_L \cdot \mathbf{A}_{\mathbf{Q}_p,m}$ de $\widetilde{\mathscr{O}}_{\mathscr{E}}$.

Proposition I.5.5. — (i)

(a) *tout élément x de $\mathscr{O}_{\mathscr{E},m}$ s'écrit de manière unique sous la forme $x = \sum_{i\in I_m}[(1+T)^i]a_i(x)$, où $a_i(x) \in \mathscr{O}_{\mathscr{E}}$, si $i \in I_m$;*

(b) *tout élément x de $\widetilde{\mathscr{O}}_{\mathscr{E}}$ s'écrit de manière unique sous la forme $x = \sum_{i\in I}[(1+T)^i]a_i(x)$, où $(a_i(x))_{i\in I}$ est une famille d'éléments de $\mathscr{O}_{\mathscr{E}}$ tendant vers* 0 (pour la topologie faible) *quand i tend vers l'infini.*

(ii) *Si $x \in \widetilde{\mathscr{O}}^+_{\mathscr{E}}$, alors $a_i(x) \in \mathscr{O}^+_{\mathscr{E}}$ quel que soit $i \in I$.*

Démonstration. — Les trois énoncés se démontrent de la même manière et il suffit de les démontrer pour $L = \mathbf{Q}_p$ et de tensoriser par $\mathscr{O}_L$ ensuite ; commençons par le (i) (b). Soit M le $\mathbf{A}_{\mathbf{Q}_p}$-module des familles $(a_i(x))_{i\in I}$ d'éléments de $\mathbf{A}_{\mathbf{Q}_p}$ tendant vers 0 quand i tend vers l'infini. Pour démontrer le (i), il s'agit de prouver que l'application $(a_i)_{i\in I} \mapsto \sum_{i\in I}[(1+T)^i]a_i$ est un isomorphisme de M sur $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}$, ce qu'il suffit de vérifier modulo p puisque les modules considérés sont sans p-torsion et complets pour la topologie p-adique. Le (i) de la proposition I.5.3 permet donc de conclure.

Le (i) (a) se démontre en remplaçant I par I_m dans la démonstration ci-dessus et en utilisant le (i) de la proposition I.5.3. Le (ii) se démontre en remplaçant $\mathbf{A}_{\mathbf{Q}_p}$ par $\mathbf{A}^+_{\mathbf{Q}_p}$ et en utilisant la remarque I.5.4.

• *Traces de Tate normalisées.*— Si $n \in \mathbf{N}$, et si x appartient à un des anneaux $\widetilde{\mathbf{E}}_{\mathbf{Q}_p}$, $\widetilde{\mathbf{E}}^+_{\mathbf{Q}_p}$, $\widetilde{\mathscr{O}}^+_{\mathscr{E}}$ ou $\widetilde{\mathscr{O}}_{\mathscr{E}}$, on pose[(2)] :

$$\mathrm{Res}_{p^{-n}\mathbf{Z}_p} x = \sum_{i\in I_n}[(1+T)^i]a_i(x).$$

Proposition I.5.6. — (i) $\mathrm{Res}_{p^{-n}\mathbf{Z}_p}$ *commute à l'action de* Γ.

(ii) $\varphi \circ \mathrm{Res}_{p^{-n}\mathbf{Z}_p} = \mathrm{Res}_{p^{1-n}\mathbf{Z}_p} \circ \varphi$.

(iii) $\mathrm{Res}_{p^{-n}\mathbf{Z}_p}([(1+T)^b]x) = [(1+T)^b]\mathrm{Res}_{p^{-n}\mathbf{Z}_p} x$, *si $x \in p^{-n}\mathbf{Z}_p$.*

---

(2) Si on est en caractéristique p, alors $[(1+T)^i] = (1+T)^i$, par définition du représentant de Teichmüller.

(iv) $\mathrm{Res}_{\mathbf{Z}_p} \circ \varphi^{-1} = \psi \circ \mathrm{Res}_{\mathbf{Z}_p}$.

(v) $x = \lim_{n\to+\infty} \mathrm{Res}_{p^{-n}\mathbf{Z}_p} x$.

Démonstration. — C'est une conséquence facile des prop. I.5.3 et I.5.5.

5. Mesures nulles à l'infini. — L'ensemble $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$ des mesures sur $\mathbf{Q}_p$ à valeurs dans $\mathscr{O}_L$ n'est pas un anneau car on ne peut pas faire la convolution de deux mesures sans prendre de précautions concernant leurs supports. Ceci nous amène à définir le sous-ensemble $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)_{\mathrm{pc}}$ des *mesures nulles à l'infini*, c'est-à-dire les mesures μ telles que $\mathrm{Dir}_b * \mu \to 0$ (pour la topologie faible sur $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$) quand $b \to \infty$, où Dir_b désigne la *masse de Dirac* en b. Il est facile de vérifier que $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)_{\mathrm{pc}}$ est un anneau pour la convolution, et que $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)_{\mathrm{pc}}$ est dense dans $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$.

Proposition I.5.7. — *La transformée de Fourier $\mu \mapsto \int_{\mathbf{Q}_p}[(1+T)^x]\mu$ induit un isomorphisme d'anneaux de $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)_{\mathrm{pc}}$ sur $\widetilde{\mathscr{O}}_{\mathscr{E}}^+$.*

Démonstration. — Soit $I = \mathbf{Z}[\frac{1}{p}] \cap [0,1[$ le système standard de représentants de $\mathbf{Q}_p/\mathbf{Z}_p$. Alors $\mu = \sum_{i\in I} \mathrm{Dir}_i * \mathrm{Res}_{\mathbf{Z}_p}(\mathrm{Dir}_{-i} * \mu)$, ce qui nous donne

$$\int_{\mathbf{Q}_p}[(1+T)^x]\mu = \sum_{i\in I}\int_{\mathbf{Z}_p}[(1+T)^{x+i}]\,\mathrm{Res}_{\mathbf{Z}_p}(\mathrm{Dir}_{-i}*\mu) = \sum_{i\in I}\Big(\int_{\mathbf{Z}_p}(1+T)^x\,\mathrm{Res}_{\mathbf{Z}_p}(\mathrm{Dir}_{-i}*\mu)\Big)\,[(1+T)^i].$$

Modulo le fait que la transformée d'Amice $\lambda \mapsto \int_{\mathbf{Z}_p}(1+T)^x\,\lambda$ induit un isomorphisme d'anneaux de $\mathscr{D}_0(\mathbf{Z}_p, \mathscr{O}_L)$ sur $\mathscr{O}_{\mathscr{E}}^+$, le résultat suit donc de la prop. I.5.5.

6. Fonctions continues nulles à l'infini. — On étend $\mathrm{rés}_0$ à $\widetilde{\mathscr{O}}_{\mathscr{E}}\,\frac{dT}{1+T}$ en posant $\mathrm{rés}_0(z\,\frac{dT}{1+T}) = \mathrm{rés}_0\big((\mathrm{Res}_{\mathbf{Z}_p} z)\,\frac{dT}{1+T}\big)$.

Proposition I.5.8. — *L'application* $\mathrm{rés}_0 : \widetilde{\mathscr{O}}_{\mathscr{E}}\,\frac{dT}{1+T} \to \mathscr{O}_L$ *vérifie les propriétés suivantes :*

(i) $\mathrm{rés}_0(\varphi(z)\frac{dT}{1+T}) = \mathrm{rés}_0(z\,\frac{dT}{1+T})$ *et* $\mathrm{rés}_0(\sigma_a(z)\,\frac{dT}{1+T})) = a^{-1}\mathrm{rés}_0(z\,\frac{dT}{1+T})$, *si* $a \in \mathbf{Z}_p^*$

(ii) $\mathrm{rés}_0$ *est identiquement nul sur* $\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T} \boxtimes U$, *si* $U \subset \mathbf{Q}_p^*$.

Démonstration. — La formule pour l'action de Γ suit, via la prop. I.4.2, de ce que $\mathrm{Res}_{\mathbf{Z}_p}$ commute à l'action de Γ. Celle pour φ vient de ce que $\mathrm{Res}_{\mathbf{Z}_p}(\varphi^{-1}(z)) = \psi(\mathrm{Res}_{\mathbf{Z}_p}(z))$, ce qui permet d'utiliser la prop. I.4.2 pour montrer que $\mathrm{rés}_0(\varphi^{-1}(z)\frac{dT}{1+T}) = \mathrm{rés}_0(z\,\frac{dT}{1+T})$.

Maintenant, si $z \in \mathscr{O}_{\mathscr{E}}\,\frac{dT}{1+T} \boxtimes U$, et si $n \in \mathbf{N}$, alors $\varphi^{-n}(z) \in \mathscr{O}_{\mathscr{E}}\,\frac{dT}{1+T} \boxtimes p^{-n}U$. Or l'hypothèse $U \subset \mathbf{Q}_p^*$ implique que $\mathbf{Z}_p \cap p^{-n}U = \emptyset$, si n est assez grand. On a donc $\mathrm{Res}_{\mathbf{Z}_p}(\varphi^{-n}(z)) = 0$, si n est assez grand, et donc $\mathrm{rés}_0(z) = \mathrm{rés}_0(\varphi^{-n}(z)) = \mathrm{rés}_0(\mathrm{Res}_{\mathbf{Z}_p}(\varphi^{-n}(z))) = 0$. Ceci permet de conclure.

Proposition I.5.9. — *L'application $z \mapsto \phi_z$ définie par $\phi_z(x) = \mathrm{rés}_0([(1+T)^x]z\,\frac{dT}{1+T})$ induit un isomorphisme de $\widetilde{\mathscr{O}}_{\mathscr{E}}/\widetilde{\mathscr{O}}_{\mathscr{E}}^+$ sur l'espace $\mathscr{C}^0(\mathbf{Q}_p, \mathscr{O}_L)_0$ des fonctions continues sur $\mathbf{Q}_p$ tendant vers 0 à l'infini.*

Démonstration. — Fixons un système I de représentants de $\mathbf{Q}_p/\mathbf{Z}_p$ dans $\mathbf{Q}_p$. Cela permet, d'après la prop. I.5.5, d'écrire tout élément z de $\widetilde{\mathscr{O}}_{\mathscr{E}}$ sous la forme $z = \sum_{i\in I}[(1+T)^i]\,z_i$, où

$(z_i)_{i\in I}$ est une suite d'éléments de $\mathscr{O}_{\mathscr{E}}$ tendant vers 0 à l'infini pour la topologie faible. On a alors $\phi_z(x) = \phi_{z_i}(x+i)$, si $x+i \in \mathbf{Z}_p$. Comme z_i tend vers 0, il existe, pour tout $k \in \mathbf{N}$, un entier $n(k) \in \mathbf{N}$ tel que $z_i \in \widetilde{\mathscr{O}}_{\mathscr{E}}^{+} + p^k\widetilde{\mathscr{O}}_{\mathscr{E}}$, si $v_p(i) \leqslant -n(k)$, ce qui se traduit par le fait que $\phi_z(x) \in p^k\mathscr{O}_L$, si $v_p(i) \leqslant -n(k)$ et si $x+i \in \mathbf{Z}_p$. On en déduit l'appartenance de ϕ_z à $\mathscr{C}^0(\mathbf{Q}_p, \mathscr{O}_L)_0$.

Réciproquement, soit $\phi \in \mathscr{C}^0(\mathbf{Q}_p, \mathscr{O}_L)_0$. Si ϕ_i est la restriction de $x \mapsto \phi(x+i)$ à $\mathbf{Z}_p$, soit $k(i)$ le plus grand entier k tel que ϕ_i soit à valeurs dans $p^k\mathscr{O}_L$, et soit $z_i \in \mathscr{O}_{\mathscr{E}}$ tel que $\phi_{z_i} = p^{-k(i)}\phi_i$. L'appartenance de ϕ à $\mathscr{C}^0(\mathbf{Q}_p, \mathscr{O}_L)_0$ se traduit par le fait que $k(i)$ tend vers $+\infty$ à l'infini. La série $\sum_{i\in I} p^{k(i)}[(1+T)^i]z_i$ converge donc dans $\widetilde{\mathscr{O}}_{\mathscr{E}}$ et la somme z de cette série vérifie $\phi_z = \phi$ par construction. Ceci permet de conclure.

I.6. Construction de représentations du mirabolique

Ce qui suit est issu de la description (prop. I.5.1) de $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$ à partir de $\mathscr{D}_0(\mathbf{Z}_p, \mathscr{O}_L)$ et de l'action du mirabolique qui en résulte (alinéa 2 du n° I.5) ; dans le cas $M = \mathscr{D}_0(\mathbf{Z}_p, \mathscr{O}_L)$, on retombe sur les objets précédents.

1. $(P(\mathbf{Z}_p), \psi)$-modules et représentations de $P(\mathbf{Q}_p)$. — On note $P = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ le sous-groupe mirabolique de $\mathbf{GL}_2$. Si A est un anneau, on note $P(A) \subset \mathbf{GL}_2(A)$ le groupe des éléments de P à coefficients dans A. On a donc, en particulier, $P(\mathbf{Q}_p) = \left(\begin{smallmatrix} \mathbf{Q}_p^* & \mathbf{Q}_p \\ 0 & 1 \end{smallmatrix}\right)$ et $P(\mathbf{Z}_p) = \left(\begin{smallmatrix} \mathbf{Z}_p^* & \mathbf{Z}_p \\ 0 & 1 \end{smallmatrix}\right)$.

Un $(P(\mathbf{Z}_p), \psi)$-*module* M est un $\mathscr{O}_L$-module topologique muni d'une action continue de $P(\mathbf{Z}_p)$ et d'un opérateur $\mathscr{O}_L$-linéaire continu ψ, surjectif, commutant à l'action de $\left(\begin{smallmatrix} \mathbf{Z}_p^* & 0 \\ 0 & 1 \end{smallmatrix}\right)$, et tel que $\psi(\left(\begin{smallmatrix} 1 & pb \\ 0 & 1 \end{smallmatrix}\right)z) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\psi(z)$, si $b \in \mathbf{Z}_p$ et $z \in M$.

Les exemples auxquels nous aurons affaire sont les suivants.

• L'espace $\mathscr{D}_0(\mathbf{Z}_p, A)$ des mesures sur $\mathbf{Z}_p$ à valeurs dans A, où $A = k_L, \mathscr{O}_L, L, \dots$, est naturellement un $(P(\mathbf{Z}_p), \psi)$-module, l'action de $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in P(\mathbf{Z}_p)$ sur $\mu \in \mathscr{D}_0(\mathbf{Z}_p, A)$ étant donnée par $\int_{\mathbf{Z}_p} \phi \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot \mu = \int_{\mathbf{Z}_p} \phi(ax+b)\,\mu$, et $\psi = \left(\begin{smallmatrix} p^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ \mathrm{Res}_{p\mathbf{Z}_p}$ étant défini par $\int_{\mathbf{Z}_p} \phi\,\psi(\mu) = \int_{p\mathbf{Z}_p} \phi(p^{-1}x)\,\mu$.

• Un (φ, Γ)-module D est aussi naturellement un $(P(\mathbf{Z}_p), \psi)$-module, l'action de ψ étant l'action précédemment définie, et celle de $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in P(\mathbf{Z}_p)$ étant donnée par $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z = (1+T)^b\sigma_a(z)$. Les sous-modules $D^\sharp$ et $D^\natural$, étant stables par ψ et $P(\mathbf{Z}_p)$, sont aussi des exemples de $(P(\mathbf{Z}_p), \psi)$-modules.

Si M est un $(P(\mathbf{Z}_p), \psi)$-module, on définit $M \boxtimes \mathbf{Q}_p$ comme l'ensemble des suites[(3)] $(x^{(n)})_{n\in\mathbf{N}}$ d'éléments de M, telles que $\psi(x^{(n+1)}) = x^{(n)}$, pour tout $n \in \mathbf{N}$.

Proposition I.6.1. — *Sur $M \boxtimes \mathbf{Q}_p$, il existe une unique action de $P(\mathbf{Q}_p)$ telle que :*

(a) *si $a \in \mathbf{Z}_p^*$, alors $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot (x^{(n)})_{n\in\mathbf{Z}} = (\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n)})_{n\in\mathbf{Z}}$;*

(b) *si $k \in \mathbf{Z}$, alors $\left(\begin{smallmatrix} p^k & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot (x^{(n)})_{n\in\mathbf{Z}} = (x^{(n+k)})_{n\in\mathbf{Z}}$;*

---

(3) Notons que, si on pose $w^{(n)} = \psi^{-n}(w^{(0)})$, si $n \leqslant -1$, on obtient une bijection de $M \boxtimes \mathbf{Q}_p$ sur l'ensemble des suites sur $\mathbf{Z}$ vérifiant les propriétés ci-dessus. Nous utiliserons donc indifféremment la notation $(w^{(n)})_{n\in\mathbf{N}}$ ou $(w^{(n)})_{n\in\mathbf{Z}}$ pour désigner un élément de $M \boxtimes \mathbf{Q}_p$.

(c) *si* $b \in \mathbf{Q}_p$, *alors* $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot (x^{(n)})_{n\in\mathbf{Z}} = (y^{(n)})_{n\in\mathbf{Z}}$, *avec* $y^{(n)} = \left(\begin{smallmatrix} 1 & p^n b \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n)}$ *si* $p^n b \in \mathbf{Z}_p$, *et* $y^{(n)} = \psi^{-v_p(b)-n}\big(y^{(-v_p(b))}\big)$, *si* $n \leqslant -v_p(b)$.

Démonstration. — Remarquons qu'un élément $x = (x^{(n)})_{n\in\mathbf{Z}}$ de $M \boxtimes \mathbf{Q}_p$ est uniquement déterminé, si on connaît $x^{(n)}$ pour tout n assez grand, puisqu'il suffit d'itérer ψ pour récupérer les $x^{(n)}$ manquants. Soit $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in P(\mathbf{Q}_p)$, et soit $r = v_p(a)$. Comme $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} p^{-r}a & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} p^r & 0 \\ 0 & 1 \end{smallmatrix}\right)$, et comme $p^{-r}a \in \mathbf{Z}_p^*$, une action de groupe de $P(\mathbf{Q}_p)$ sur $M \boxtimes \mathbf{Q}_p$ vérifiant les propriétés (a), (b) et (c) de la proposition doit être donnée par la formule

$$\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot (x^{(n)})_{n\gg 0} = \Big(\left(\begin{smallmatrix} 1 & p^n b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} p^{-r}a & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n+r)}\Big)_{n\gg 0} = \Big(\left(\begin{smallmatrix} p^{-r}a & p^n b \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n+r)}\Big)_{n\gg 0}.$$

En particulier, une telle action, si elle existe, est unique. Soient alors $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} a' & b' \\ 0 & 1 \end{smallmatrix}\right)$ deux éléments de $P(\mathbf{Q}_p)$, et soient $r = v_p(a)$ et $r' = v_p(a')$. Soit aussi $y^{(n)} = \left(\begin{smallmatrix} p^{-r}a & p^n b \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n+r)}$, si $n \gg 0$. On a

$$\begin{aligned}\left(\begin{smallmatrix} a' & b' \\ 0 & 1 \end{smallmatrix}\right) \cdot \Big(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot (x^{(n)})_{n\gg 0}\Big) &= \Big(\left(\begin{smallmatrix} p^{-r'}a' & p^n b' \\ 0 & 1 \end{smallmatrix}\right) \cdot y^{(n+r')}\Big)_{n\gg 0} \\ &= \Big(\left(\begin{smallmatrix} p^{-r'}a' & p^n b' \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} p^{-r}a & p^{n+r'} b \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n+r'+r)}\Big)_{n\gg 0} \\ &= \Big(\left(\begin{smallmatrix} p^{-(r+r')}aa' & p^n(b'+a'b) \\ 0 & 1 \end{smallmatrix}\right) \cdot x^{(n+r'+r)}\Big)_{n\gg 0} = \left(\begin{smallmatrix} aa' & b'+a'b \\ 0 & 1 \end{smallmatrix}\right) \cdot (x^{(n)})_{n\gg 0}\end{aligned}$$

et comme $\left(\begin{smallmatrix} a' & b' \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa' & b'+a'b \\ 0 & 1 \end{smallmatrix}\right)$, cela montre que l'on a bien défini une action de groupe.

2. $(P(\mathbf{Z}_p), \varphi, \psi)$*-modules et restriction à un ouvert compact.* — Un $(P(\mathbf{Z}_p), \varphi, \psi)$-module est un $(P(\mathbf{Z}_p), \psi)$-module muni en plus d'un opérateur injectif φ vérifiant les conditions suivantes :

- $\varphi \circ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & pb \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi$, si $b \in \mathbf{Z}_p$, et $\varphi \circ \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi$, si $a \in \mathbf{Z}_p^*$;
- $\psi \circ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi = 0$, si $b \in \mathbf{Z}_p^*$ et $\psi \circ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi = \left(\begin{smallmatrix} 1 & p^{-1}b \\ 0 & 1 \end{smallmatrix}\right)$, si $b \in p\mathbf{Z}_p$;
- $\sum_{i=0}^{p-1} \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi \circ \psi \circ \left(\begin{smallmatrix} 1 & -i \\ 0 & 1 \end{smallmatrix}\right) = \mathrm{id}$.

Notons que les conditions $\varphi \circ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & pb \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi$ et $\varphi \circ \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi$ sont équivalentes à ce que l'action de $P(\mathbf{Z}_p)$ se prolonge en une action du semi-groupe $P^+ = \left(\begin{smallmatrix} \mathbf{Z}_p - \{0\} & \mathbf{Z}_p \\ 0 & 1 \end{smallmatrix}\right)$, l'action de $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ étant définie par $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot z = \varphi(z)$.

La condition $\psi \circ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi = \left(\begin{smallmatrix} 1 & p^{-1}b \\ 0 & 1 \end{smallmatrix}\right)$, si $b \in p\mathbf{Z}_p$, implique en particulier que ψ est un inverse à gauche de φ ; on en déduit que $\left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi \circ \psi \circ \left(\begin{smallmatrix} 1 & -i \\ 0 & 1 \end{smallmatrix}\right)$ est un projecteur, si $i \in \{0, \dots, p-1\}$. La condition $\psi \circ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi = 0$, si $b \in \mathbf{Z}_p^*$, assure quant à elle que ces projecteurs sont orthogonaux deux à deux (la composée de deux d'entre eux est nulle si $i \neq j$).

Si M est un $(P(\mathbf{Z}_p), \varphi, \psi)$-module, si $a \in \mathbf{Z}_p$ et $k \in \mathbf{N}$, soit

$$\beta_{k,a} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right).$$

Alors $\beta_{k,a} : M \to M$ est $\mathscr{O}_L$-linéaire, et on a le résultat suivant.

Lemme I.6.2. — (i) $\beta_{k,a} \circ \beta_{k,b} = 0$, *si* $a - b \notin p^k\mathbf{Z}_p$, *et* $\beta_{k,a} \circ \beta_{k,b} = \beta_{k,a} = \beta_{k,b}$, *si* $a - b \in p^k\mathbf{Z}_p$.

(ii) $\sum_{i=0}^{p-1} \beta_{k+1,a+ip^k} = \beta_{k,a}$.

Démonstration. — Par définition, on a

$$\beta_{k,a} \circ \beta_{k,b} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right).$$

Or la seconde des propriétés de φ permet de montrer, par une récurrence immédiate sur k, que $\psi^k \circ \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k = 0$, si $b-a \notin p^k\mathbf{Z}_p$, et $\psi^k \circ \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k = \left(\begin{smallmatrix} 1 & p^{-k}(b-a) \\ 0 & 1 \end{smallmatrix}\right)$, si $b-a \in p^k\mathbf{Z}_p$. On en déduit que $\beta_{k,a} \circ \beta_{k,b} = 0$, si $a-b \notin p^k\mathbf{Z}_p$, et que dans le cas où $a-b \in p^k\mathbf{Z}_p$, alors

$$\beta_{k,a} \circ \beta_{k,b} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \left(\begin{smallmatrix} 1 & p^{-k}(b-a) \\ 0 & 1 \end{smallmatrix}\right) \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right).$$

Or on a $\varphi^k \circ \left(\begin{smallmatrix} 1 & p^{-k}(b-a) \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k$ et $\left(\begin{smallmatrix} 1 & p^{-k}(b-a) \\ 0 & 1 \end{smallmatrix}\right) \circ \psi^k = \psi^k \circ \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right)$. En utilisant la première de ces formules, on obtient

$$\beta_{k,a} \circ \beta_{k,b} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) = \beta_{k,b},$$

et en utilisant la seconde, on obtient

$$\beta_{k,a} \circ \beta_{k,b} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & b-a \\ 0 & 1 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right) = \beta_{k,a}.$$

On en déduit le (i).

Passons au (ii). On a

$$\begin{aligned}\sum_{i=0}^{p-1} \beta_{k+1,a+ip^k} &= \sum_{i=0}^{p-1} \left(\begin{smallmatrix} 1 & a+ip^k \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^{k+1} \circ \psi^{k+1} \circ \left(\begin{smallmatrix} 1 & -a-ip^k \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \Big(\sum_{i=0}^{p-1} \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi \circ \psi \circ \left(\begin{smallmatrix} 1 & -i \\ 0 & 1 \end{smallmatrix}\right)\Big) \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right) = \beta_{k,a}.\end{aligned}$$

Ceci permet de conclure.

Le lemme précédent montre, en particulier, que $\beta_{k,a}$ ne dépend que de la classe de a modulo p^k, ce qui permet de noter cette application sous la forme $\mathrm{Res}_{a+p^k\mathbf{Z}_p}$. Le reste du lemme peut alors se reformuler de manière plus parlante :

Corollaire I.6.3. — (i) *Si $a, b \in \mathbf{Z}_p$, alors*

$$\mathrm{Res}_{a+p^k\mathbf{Z}_p} \circ \mathrm{Res}_{b+p^k\mathbf{Z}_p} = \begin{cases} \mathrm{Res}_{a+p^k\mathbf{Z}_p} = \mathrm{Res}_{b+p^k\mathbf{Z}_p} & \text{si } a+p^k\mathbf{Z}_p = b+p^k\mathbf{Z}_p, \\ 0 & \text{si } (a+p^k\mathbf{Z}_p) \cap (b+p^k\mathbf{Z}_p) = \emptyset. \end{cases}$$

(ii) *Si $a \in \mathbf{Z}_p$, alors* $\sum_{i=0}^{p-1} \mathrm{Res}_{a+ip^k+p^{k+1}\mathbf{Z}_p} = \mathrm{Res}_{a+p^k\mathbf{Z}_p}$.

Remarque I.6.4. — (i) On a $\psi = \varphi^{-1} \circ \mathrm{Res}_{p\mathbf{Z}_p} = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \circ \mathrm{Res}_{p\mathbf{Z}_p}$.

(ii) Si $M = \mathscr{D}_0(\mathbf{Z}_p)$, alors $\mathrm{Res}_{a+p^k\mathbf{Z}_p}$ est l'application de restriction à $a+p^k\mathbf{Z}_p$ (i.e. la multiplication par $\mathbf{1}_{a+p^k\mathbf{Z}_p}$) ; c'est ce qui justifie le nom que nous lui avons donné.

La propriété (ii) du corollaire montre que, si U est un ouvert compact de $\mathbf{Z}_p$, et si $k \in \mathbf{N}$ est assez grand pour que U soit une réunion de translatés de $p^k\mathbf{Z}_p$, alors l'application $\mathscr{O}_L$-linéaire $\sum_{a \in U \bmod p^k} \mathrm{Res}_{a+p^k\mathbf{Z}_p}$ ne dépend pas du choix de k (ni de celui du système de représentants de U modulo $p^k\mathbf{Z}_p$ par existence de $\mathrm{Res}_{a+p^k\mathbf{Z}_p}$). On note $\mathrm{Res}_U : M \to M$ cette application. On a en particulier $\mathrm{Res}_{\mathbf{Z}_p} = \mathrm{id}$. On pose $\mathrm{Res}_\emptyset = 0$.

Lemme I.6.5. — *Soient U et V des ouverts compacts de $\mathbf{Z}_p$.*

(i) $\mathrm{Res}_U + \mathrm{Res}_V = \mathrm{Res}_{U\cap V} + \mathrm{Res}_{U\cup V}$.

(ii) $\mathrm{Res}_U \circ \mathrm{Res}_V = \mathrm{Res}_V \circ \mathrm{Res}_U = \mathrm{Res}_{U\cap V}$.

Démonstration. — On choisit $k \in \mathbf{N}$ assez grand pour que U et V soient des réunions de translatés de $p^k\mathbf{Z}_p$. Le (i) est alors immédiat sur la définition, et le (ii) suit du (i) du cor. I.6.3.

Si U est un ouvert compact de $\mathbf{Z}_p$, on définit le sous-$\mathscr{O}_L$-module $M \boxtimes U$ de M comme l'image de Res_U. On a donc en particulier $M \boxtimes \mathbf{Z}_p = M$, $M \boxtimes \emptyset = 0$ et $M \boxtimes \mathbf{Z}_p^* = M^{\psi=0}$.

Lemme I.6.6. — (i) Res_U *est un projecteur de M sur $M \boxtimes U$.*

(ii) *Si les U_j, pour $j \in J$ forment une partition* (automatiquement finie) *de U par des ouverts compacts, et si $x \in M \boxtimes U$, alors $\sum_{j\in J} \mathrm{Res}_{U_j}(x) = x$, et donc $M \boxtimes U = \oplus_{j\in J} M \boxtimes U_j$.*

Démonstration. — C'est une conséquence immédiate du lemme I.6.5.

On dispose d'une action naturelle de $P(\mathbf{Q}_p)$ sur $\mathbf{Q}_p$ (définie par $\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right) \cdot x = ax + b$). Le semi-groupe P^+ laisse stable $\mathbf{Z}_p$, et l'image de $i + p^k\mathbf{Z}_p$ par $\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right)$ est $ai + b + p^{k+r}\mathbf{Z}_p$, si $r = v_p(a)$.

Lemme I.6.7. — *Si U est un ouvert compact de $\mathbf{Z}_p$, et si $g \in P^+$, alors $g \circ \mathrm{Res}_U = \mathrm{Res}_{gU} \circ g$.*

Démonstration. — Par linéarité, il suffit de le vérifier pour U de la forme $i + p^k\mathbf{Z}_p$. Si $g = \left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right)$, et $r = v_p(a)$, on a

$$g \circ \mathrm{Res}_{i+p^k\mathbf{Z}_p} = \left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & i \\ 0 & 1\end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -i \\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & ai+b \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right) \circ \varphi^k \circ \psi^k \circ \left(\begin{smallmatrix} 1 & -i \\ 0 & 1\end{smallmatrix}\right).$$

Or $\left(\begin{smallmatrix} p^r & 0 \\ 0 & 1\end{smallmatrix}\right) = \varphi^r$, et $p^{-r}a \in \mathbf{Z}_p^*$, ce qui fait que $\left(\begin{smallmatrix} p^{-r}a & 0 \\ 0 & 1\end{smallmatrix}\right)$ commute à φ et ψ, et donc

$$\left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right) \circ \varphi^k \circ \psi^k = \left(\begin{smallmatrix} p^{-r}a & 0 \\ 0 & 1\end{smallmatrix}\right) \circ \varphi^{k+r} \circ \psi^k = \varphi^{k+r} \circ \psi^k \circ \left(\begin{smallmatrix} p^{-r}a & 0 \\ 0 & 1\end{smallmatrix}\right) = \varphi^{k+r} \circ \psi^{k+r} \circ \left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right).$$

Comme $\left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -i \\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -(ai+b) \\ 0 & 1\end{smallmatrix}\right) g$, on obtient finalement

$$g \circ \mathrm{Res}_{i+p^k\mathbf{Z}_p} = \left(\begin{smallmatrix} 1 & ai+b \\ 0 & 1\end{smallmatrix}\right) \circ \varphi^{k+r} \circ \psi^{k+r} \circ \left(\begin{smallmatrix} 1 & -(ai+b) \\ 0 & 1\end{smallmatrix}\right) \circ g = \mathrm{Res}_{ai+b+p^{k+r}\mathbf{Z}_p} \circ g = \mathrm{Res}_{g(i+p^k\mathbf{Z}_p)} \circ g.$$

Ceci permet de conclure.

3. Les applications Res_U *sur* $M \boxtimes \mathbf{Q}_p$ *et les modules* $(M \boxtimes \mathbf{Q}_p)_c$ *et* $(M \boxtimes \mathbf{Q}_p)_{\mathrm{pc}}$. — Remarquons que l'on dispose d'une identification naturelle de M à un sous-module de $M \boxtimes \mathbf{Q}_p$ en envoyant $x \in M$ sur $\iota(x) = (\varphi^n(x))_{n\in\mathbf{N}} \in M \boxtimes \mathbf{Q}_p$; on note $M \boxtimes \mathbf{Z}_p$ l'image de M par ι de telle sorte que ι soit un isomorphisme de M sur $M \boxtimes \mathbf{Z}_p$. Alors ι commute à l'action de P^+ comme le montre un calcul immédiat et on dispose d'un projecteur $\mathrm{Res}_{\mathbf{Z}_p} : M \boxtimes \mathbf{Q}_p \to M \boxtimes \mathbf{Z}_p$ envoyant $(x^{(n)})_{n\in\mathbf{N}}$ sur $\iota(x^{(0)})$.

Plus généralement, si U est un ouvert compact de $\mathbf{Z}_p$, on note $M \boxtimes U$ le sous-espace de $M \boxtimes \mathbf{Q}_p$ image de $M \boxtimes U \subset U$ par ι, et $\mathrm{Res}_{\mathbf{Z}_p} : M \boxtimes \mathbf{Q}_p \to M \boxtimes U$ le projecteur $\iota \circ \mathrm{Res}_U \circ \mathrm{Res}_{\mathbf{Z}_p}$, où $\mathrm{Res}_U : M \to M \boxtimes U$ est le projecteur défini plus haut.

Si U est un ouvert compact de $\mathbf{Q}_p$, on choisit $k \in \mathbf{N}$ tel que $p^kU \subset \mathbf{Z}_p$, et on définit $M \boxtimes U \subset M \boxtimes \mathbf{Q}_p$ et $\mathrm{Res}_U : M \boxtimes \mathbf{Q}_p \to M \boxtimes U$, en posant

$$M \boxtimes U = \left(\begin{smallmatrix} p^{-k} & 0 \\ 0 & 1\end{smallmatrix}\right)(M \boxtimes p^kU) \quad \text{et} \quad \mathrm{Res}_U = \left(\begin{smallmatrix} p^{-k} & 0 \\ 0 & 1\end{smallmatrix}\right) \circ \mathrm{Res}_{p^kU} \circ \left(\begin{smallmatrix} p^{k} & 0 \\ 0 & 1\end{smallmatrix}\right).$$

Que ceci ne dépende pas du choix de k est une conséquence du lemme I.6.7.

Proposition I.6.8. — (i) *Si U et V sont des ouverts compacts de $\mathbf{Q}_p$, alors*

$$\mathrm{Res}_U + \mathrm{Res}_V = \mathrm{Res}_{U\cup V} + \mathrm{Res}_{U\cap V} \quad \text{et} \quad \mathrm{Res}_U \circ \mathrm{Res}_V = \mathrm{Res}_V \circ \mathrm{Res}_U = \mathrm{Res}_{U\cap V}.$$

(ii) *Si U est un ouvert compact de $\mathbf{Q}_p$, alors Res_U est un projecteur de $M \boxtimes \mathbf{Q}_p$ sur $M \boxtimes U$, et si les U_j, pour $j \in J$ forment une partition de U par des ouverts compacts, alors $M \boxtimes U = \oplus_{j\in J} M \boxtimes U_j$.*

(iii) *Si U est un ouvert compact de $\mathbf{Q}_p$, et si $g \in P(\mathbf{Q}_p)$, alors $g \circ \mathrm{Res}_U = \mathrm{Res}_{gU} \circ g$.*

Démonstration. — Pour démontrer le (i), on choisit k assez grand pour que p^kU et p^kV soient inclus dans $\mathbf{Z}_p$, et on utilise le lemme I.6.5. Pour démontrer le (ii), on choisit k assez grand pour que $p^kU \subset \mathbf{Z}_p$, et on utilise le lemme I.6.6. Pour démontrer le (iii), on choisit k assez grand pour que $p^kU \subset \mathbf{Z}_p$, et r assez grand pour que $h = \left(\begin{smallmatrix} p^r a & p^{r+k}b \\ 0 & 1 \end{smallmatrix}\right) \in P^+$, si $g = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$. Alors

$$g \circ \mathrm{Res}_U = g \circ \left(\begin{smallmatrix} p^{-k} & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ \mathrm{Res}_{p^kU} \circ \left(\begin{smallmatrix} p^k & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} p^{-k-r} & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ h \circ \mathrm{Res}_{p^kU} \circ \left(\begin{smallmatrix} p^k & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

On peut alors utiliser le lemme I.6.7 pour écrire $h \circ \mathrm{Res}_{p^kU}$ sous la forme $\mathrm{Res}_{h(p^kU)} \circ h$, et comme $h\left(\begin{smallmatrix} p^k & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} p^{k+r} & 0 \\ 0 & 1 \end{smallmatrix}\right) g$ et $h(p^kU) = p^r a(p^kU) + p^{r+k}b = p^{r+k}(gU)$, on obtient

$$g \circ \mathrm{Res}_U = \left(\begin{smallmatrix} p^{-k-r} & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ \mathrm{Res}_{p^{r+k}(gU)} \circ \left(\begin{smallmatrix} p^{k+r} & 0 \\ 0 & 1 \end{smallmatrix}\right) \circ g = \mathrm{Res}_{gU} \circ g.$$

Ceci permet de conclure.

Remarque I.6.9. — L'opérateur $\psi : M \to M$ est relié à l'action de $\left(\begin{smallmatrix} p^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$: on a

$$\psi \circ \mathrm{Res}_{\mathbf{Z}_p} = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \circ \mathrm{Res}_{p\mathbf{Z}_p} = \mathrm{Res}_{\mathbf{Z}_p} \circ \left(\begin{smallmatrix} p^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right),$$

comme le montrent le (i) de la rem. I.6.4 et le (iii) de la prop. I.6.8.

On dit que $x \in M \boxtimes \mathbf{Q}_p$ est *à support dans U*, si $x \in M \boxtimes U$. On note

$$(M \boxtimes \mathbf{Q}_p)_c = \cup_{k\in\mathbf{N}} (M \boxtimes p^{-k}\mathbf{Z}_p)$$

l'ensemble des éléments de $M \boxtimes \mathbf{Q}_p$ *à support compact* dans $\mathbf{Q}_p$. Comme $M \boxtimes (p^{-k}\mathbf{Z}_p)$ est l'ensemble des $(x^{(n)})_{n\in\mathbf{Z}} \in M \boxtimes \mathbf{Q}_p$ vérifiant $x^{(n)} = \varphi^{n-k}(x^{(k)})$ si $n \geqslant k$, on voit que $(M \boxtimes \mathbf{Q}_p)_c$ est aussi l'ensemble des $(x^{(n)})_{n\in\mathbf{Z}} \in M \boxtimes \mathbf{Q}_p$ vérifiant $x^{(n+1)} = \varphi(x^{(n)})$ pour tout $n \in \mathbf{N}$ assez grand.

Remarque I.6.10. — (i) Si $M = \mathscr{D}_0(\mathbf{Z}_p, A)$, et si U est un ouvert compact de $\mathbf{Q}_p$, alors $M \boxtimes U$ est le module $\mathscr{D}_0(U, A)$ des mesures à support dans U, et l'application $\mathrm{Res}_U : M \boxtimes \mathbf{Q}_p \to M \boxtimes U$ n'est autre que l'application de restriction à U (i.e. la multiplication par la fonction caractéristique de U) de $\mathscr{D}_0(\mathbf{Q}_p, A)$ dans $\mathscr{D}_0(U, A)$. On en déduit que $(M \boxtimes \mathbf{Q}_p)_c$ est l'ensemble des mesures à support compact dans $\mathbf{Q}_p$.

(ii) Comme $g \in P(\mathbf{Q}_p)$ envoie $M \boxtimes U$ dans $M \boxtimes gU$, d'après le (iii) de la prop. I.6.8, le sous-module $(M \boxtimes \mathbf{Q}_p)_c$ de $M \boxtimes \mathbf{Q}_p$ est stable par $P(\mathbf{Q}_p)$.

Si M est un $(P(\mathbf{Z}_p),\psi)$-module, on munit $M\boxtimes\mathbf{Q}_p$ de la topologie induite par la topologie produit sur $M^{\mathbf{N}}$. On note $(M\boxtimes\mathbf{Q}_p)_{\rm pc}$ l'ensemble des éléments z de $M\boxtimes\mathbf{Q}_p$ *nuls à l'infini*, c'est-à-dire tels que $\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\cdot z\to 0$ dans $M\boxtimes\mathbf{Q}_p$ quand $b\to\infty$ dans $\mathbf{Q}_p$; c'est un sous-$P(\mathbf{Q}_p)$-module de $M\boxtimes\mathbf{Q}_p$.

Remarque I.6.11. — (i) Si M est un $(P(\mathbf{Z}_p),\varphi,\psi)$-module, on a $(M\boxtimes\mathbf{Q}_p)_c\subset(M\boxtimes\mathbf{Q}_p)_{\rm pc}$. En effet, si $-b+p^{-n}\mathbf{Z}_p$ n'intersecte pas le support de z, on a ${\rm Res}_{p^{-n}\mathbf{Z}_p}(\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\cdot z)=0$, ce qui se traduit, en notant $y_b=(y_b^{(n)})_{n\in\mathbf{N}}$ l'élément $\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\cdot z$ de $M\boxtimes\mathbf{Q}_p$, par la nullité de $y_b^{(n)}$, pour tout $n<k$, si $v_p(b)\leqslant -k$, et si z est à support dans $p^{-k}\mathbf{Z}_p$. En revenant à la définition de la topologie produit, cela se traduit par l'existence, pour tout voisinage V de 0 dans $M\boxtimes\mathbf{Q}_p$, de $k\in\mathbf{N}$ tel que $\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\cdot z\in V$, si $v_p(b)\leqslant -k$; autrement dit, $\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\cdot z\to 0$ quand $b\to\infty$.

(ii) Si M est un $(P(\mathbf{Z}_p),\varphi,\psi)$-module, $(M\boxtimes\mathbf{Q}_p)_c$ et donc, a fortiori, $(M\boxtimes\mathbf{Q}_p)_{\rm pc}$ est dense dans $M\boxtimes\mathbf{Q}_p$. En effet, z est la limite, dans $M\boxtimes\mathbf{Q}_p$, des ${\rm Res}_{p^{-n}\mathbf{Z}_p}z$, par définition ou presque de la topologie produit.

II. (φ,Γ)-modules

II.1. $\mathscr{O}_{\mathscr{E}}$-modules de type fini

Ce § regroupe des définitions et des résultats purement techniques qui seront utilisés dans le reste de l'article.

1. Réseaux et treillis. — Si A est un anneau local complet pour une valuation discrète, d'idéal maximal $\mathfrak{m}$, et si D est un A-module de type fini, on définit la *dimension* $\dim_A D$ de D sur A par la formule
$$\dim_A D=\dim_{A/\mathfrak{m}} D/\mathfrak{m}D.$$
Si D est libre de rang d sur A, alors $\dim_A D=d$, et dans le cas général, le théorème de structure des modules sur les anneaux principaux montre que, si $\dim_A D=d$, alors il existe $k_1,\dots,k_d\in\mathbf{N}\cup\{+\infty\}$ non nuls, et $e_1,\dots,e_d\in D$, tels que $(x_1,\dots,x_d)\mapsto x_1e_1+\cdots+x_de_d$ induise un isomorphisme de $\prod_{i=1}^d(A/\mathfrak{m}^{k_i})$ sur D. Si A est muni d'une topologie (d'anneau) plus faible que celle induite par la valuation discrète, cela permet de munir D d'une topologie faisant de l'isomorphisme précédent un homéomorphisme, $\prod_{i=1}^d(A/\mathfrak{m}^{k_i})$ étant muni de la topologie produit. La topologie ainsi obtenue sur D ne dépend pas du choix de $e_1,\dots,e_d$. En effet, un autre choix se traduit par une bijection A-linéaire de $\prod_{i=1}^d(A/\mathfrak{m}^{k_i})$ dans lui-même, et une telle bijection est continue car A-linéaire, et donc est un homéomorphisme puisque son inverse est aussi continu pour la même raison.

Ce qui précède s'applique en particulier aux $\mathscr{O}_{\mathscr{E}}$-modules de type fini. On munit $\mathscr{O}_{\mathscr{E}}$ de la *topologie faible* pour laquelle les $T^n\mathscr{O}_{\mathscr{E}}^+ +p^k\mathscr{O}_{\mathscr{E}}$, pour $k,n\in\mathbf{N}$, forment une base de voisinages de 0 et pour laquelle $\mathscr{O}_{\mathscr{E}}$ est complet, ce qui munit tout $\mathscr{O}_{\mathscr{E}}$-module de type fini de la topologie faible (la topologie forte étant juste la topologie p-adique). On note $\mathscr{E}=\mathscr{O}_{\mathscr{E}}[\frac{1}{p}]$ le corps des fractions de $\mathscr{O}_{\mathscr{E}}$, et on munit $\mathscr{E}=\cup_{n\in\mathbf{N}}p^{-n}\mathscr{O}_{\mathscr{E}}$ de la topologie de la limite inductive, chacun des $\mathscr{O}_{\mathscr{E}}$-module $p^{-n}\mathscr{O}_{\mathscr{E}}$ étant muni de la topologie faible.

Définition II.1.1. — (i) *Si D est un $k_{\mathscr{E}}$-(resp. un $\mathscr{E}$)-espace vectoriel de dimension finie d, un réseau de D est un sous-$k_{\mathscr{E}}^+$-(resp. $\mathscr{O}_{\mathscr{E}}$)-module de type fini de D contenant une base de D ; comme $k_{\mathscr{E}}^+$ (resp. $\mathscr{O}_{\mathscr{E}}$) est un anneau de valuation discrète (et donc principal), un réseau de D est libre de rang d sur $k_{\mathscr{E}}^+$ (resp. sur $\mathscr{O}_{\mathscr{E}}$).*

(ii) *Si D est un $\mathscr{O}_{\mathscr{E}}$-module de type fini, un treillis M de D est un sous-$\mathscr{O}_{\mathscr{E}}^+$-module compact de D dont l'image dans $D/\mathfrak{m}_L D$ est un réseau.*

Proposition II.1.2. — *Soit D un $\mathscr{O}_{\mathscr{E}}$-module de type fini et de torsion.*

(i) *Un sous-$\mathscr{O}_{\mathscr{E}}^+$-module compact de D est un treillis si et seulement si il est ouvert.*

(ii) *Si M est un treillis de D, alors $D = \cup_{k\in\mathbf{Z}} T^{-k}M$ et les T^kM, pour $k \in \mathbf{N}$, forment une base de voisinages de 0 dans D.*

(iii) *Si M et N sont deux treillis, alors il existe $a \geqslant b \in \mathbf{Z}$ tels que $T^aM \subset N \subset T^bM$.*

(iv) *Si $M \subset N$ sont des treillis de D, alors N/M est un $\mathscr{O}_L$-module de longueur finie.*

Démonstration. — Soit $d = \dim_{\mathscr{O}_{\mathscr{E}}} D$. Comme D est supposé de torsion, il existe $e_1, \dots, e_d \in D$ et $k_1, \dots, k_d \in \mathbf{N}$ tels que $D = (\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^{k_1})e_1 \oplus \cdots \oplus (\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^{k_d})e_d$. On note M_0 le sous-$\mathscr{O}_{\mathscr{E}}^+$-module de D engendré par $e_1, \dots, e_d$; c'est un treillis. Par définition de la topologie de D, les T^nM_0, pour $n \in \mathbf{N}$, forment une base de voisinages de 0 dans D, et D est la réunion croissante des ouverts $T^{-m}M_0$, pour $m \in \mathbf{N}$. En particulier, si M est un sous-$\mathscr{O}_{\mathscr{E}}^+$-module ouvert de D, alors il existe $b \in \mathbf{N}$ tel que M contiennent T^bM_0. Ceci implique que l'image de M modulo $\mathfrak{m}_L$ contient le réseau engendré par $T^b\overline{e}_1, \dots, T^b\overline{e}_d$, et donc que M est un treillis s'il est compact.

Réciproquement, si M est un treillis, il existe c tel que l'image de M modulo $\mathfrak{m}_L$ contienne $T^c\overline{e}_1, \dots, T^c\overline{e}_d$. Il existe donc $f_1, \dots, f_d \in D$ tels que f_i ait pour image $T^c\overline{e}_i$ modulo $\mathfrak{m}_L$, si $1 \leqslant i \leqslant d$. Les f_i, pour $1 \leqslant i \leqslant d$, forment alors une famille génératrice de D sur $\mathscr{O}_{\mathscr{E}}$, et on peut donc écrire e_j, pour $1 \leqslant j \leqslant d$, sous la forme $\sum_{i=1}^d a_{i,j}f_i$, avec $a_{i,j} \in \mathscr{O}_{\mathscr{E}}$, pour $1 \leqslant i,j \leqslant d$. Soit $k \in \mathbf{N}$ tel que $\mathfrak{m}_L^kD = 0$. Il existe alors $b \in \mathbf{N}$ tel que $T^ba_{i,j} \in \mathscr{O}_{\mathscr{E}}^+ + \mathfrak{m}_L^k\mathscr{O}_{\mathscr{E}}$, quels que soient $1 \leqslant i,j \leqslant d$. Ceci implique que M contient $b \in \mathbf{N}$ tel que $T^ba_{i,j} \in \mathscr{O}_{\mathscr{E}}^+ + \mathfrak{m}_L^k\mathscr{O}_{\mathscr{E}}$, quels que soient $1 \leqslant i,j \leqslant d$. Ceci implique que M contient $T^be_1, \dots, T^be_d$ et donc aussi T^bM_0. On en déduit le (i).

Par ailleurs, si M est un treillis, on peut extraire du recouvrement de M par les $T^{-m}M_0$ un sous-recouvrement fini, ce qui montre qu'il existe $a \in \mathbf{Z}$ tel que $M \subset T^aM_0$. Les points (ii)-(iii) se déduisent alors sans difficulté de l'existence de $a, b \in \mathbf{Z}$ tels que $T^aM_0 \supset M \supset T^bM_0$, et le (iv) se déduit du (iii) et de ce que $\mathscr{O}_{\mathscr{E}}^+/(p^k, T^n)$ est de longueur finie sur $\mathscr{O}_L$, quels que soient $k, n \in \mathbf{N}$.

II.2. (φ, Γ)-modules étales

1. Catégories de (φ, Γ)-modules. — Si A est un anneau topologique muni d'actions continues de φ et Γ commutant entre elles, un (φ, Γ)-*module* D sur A est un A-module de type fini muni d'actions semi-linéaires continues de φ et Γ commutant entre elles.

Ce qui précède s'applique en particulier à $\mathscr{O}_{\mathscr{E}}$ et $\mathscr{E}$.

• Un (φ, Γ)-*module* D sur $\mathscr{O}_{\mathscr{E}}$ est *étale* si $\varphi(D)$ engendre D comme $\mathscr{O}_{\mathscr{E}}$-module ; l'action de φ est alors injective.

• Un (φ, Γ)-*module* sur $\mathscr{E}$ est *étale* s'il possède un $\mathscr{O}_{\mathscr{E}}$-réseau stable par φ et Γ qui est étale.

Nous aurons besoin des catégories suivantes :

• $\Phi\Gamma^{\rm et}_{\rm tors}$, catégorie des (φ, Γ)-modules étales, de torsion sur $\mathscr{O}_{\mathscr{E}}$,
• $\Phi\Gamma^{\rm et}(k_{\mathscr{E}})$, catégorie des objets de $\Phi\Gamma^{\rm et}_{\rm tors}$ tués par $\mathfrak{m}_L$ (i.e. des (φ, Γ)-*modules étales sur* $k_{\mathscr{E}}$),
• $\Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$, catégorie des (φ, Γ)-modules étales, libres sur $\mathscr{O}_{\mathscr{E}}$,
• $\Phi\Gamma^{\rm et}(\mathscr{E})$, catégorie des (φ, Γ)-modules étales sur $\mathscr{E}$.

Si $D \in \Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$, alors $D/p^kD \in \Phi\Gamma^{\rm et}_{\rm tors}$ pour tout $k \in \mathbf{N}$, et D est la limite projective des D/p^kD. Par ailleurs, si $D \in \Phi\Gamma^{\rm et}(\mathscr{E})$, alors D possède un sous-$\mathscr{O}_{\mathscr{E}}$-réseau qui est un objet de $\Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$. Dans la suite du texte,

• *un* (φ, Γ)-*module étale sur* $\mathscr{O}_{\mathscr{E}}$ désigne un objet de $\Phi\Gamma^{\rm et}_{\rm tors}$ ou de $\Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$,
• *un* (φ, Γ)-*module étale* désigne un objet de $\Phi\Gamma^{\rm et}_{\rm tors}$, de $\Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$ ou de $\Phi\Gamma^{\rm et}(\mathscr{E})$.

Un objet de $\Phi\Gamma^{\rm et}(\mathscr{E})$ est *irréductible* s'il ne possède pas de sous-$\mathscr{E}$-espace vectoriel strict, stable par φ et Γ. Un objet D de $\Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$ est *irréductible* si $L \otimes_{\mathscr{O}_L} D$ est irréductible comme objet de $\Phi\Gamma^{\rm et}(\mathscr{E})$.

2. Le dual de Tate d'un (φ, Γ)-*module.* — Le module $\Omega^1_{\mathscr{O}_{\mathscr{E}}}$ des $\mathscr{O}_L$-différentielles continues de $\mathscr{O}_{\mathscr{E}}$ est libre de rang 1 engendré, au choix, par dT ou par $\frac{dT}{1+T}$. On le munit d'une structure de (φ, Γ)-module étale en faisant agir Γ et φ sur $\frac{dT}{1+T}$ par[(4)]

$$\sigma_a\Big(\frac{dT}{1+T}\Big) = a\frac{dT}{1+T}, \quad \text{si } a \in \mathbf{Z}_p^*, \quad \text{et} \quad \varphi\Big(\frac{dT}{1+T}\Big) = \frac{dT}{1+T}.$$

A partir de maintenant, on note :

• $\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T}$ le (φ, Γ)-module étale $\Omega^1_{\mathscr{O}_{\mathscr{E}}}$,
• $\mathscr{E}\frac{dT}{1+T}$ l'objet $L \otimes_{\mathscr{O}_L} \Omega^1_{\mathscr{E}}$ de $\Phi\Gamma^{\rm et}(\mathscr{E})$
• $\mathscr{E}/\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T}$ le quotient de $\mathscr{E}\frac{dT}{1+T}$ par $\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T}$; c'est la réunion croissante des $p^{-k}\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T}$ qui sont des objets de $\Phi\Gamma^{\rm et}_{\rm tors}$.

On définit le *dual de Tate* $\check{D}$ d'un (φ, Γ)-module étale D par :

• $\check{D} = {\rm Hom}_{\mathscr{O}_{\mathscr{E}}}(D, \mathscr{E}/\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T})$, si $D \in \Phi\Gamma^{\rm et}_{\rm tors}$,
• $\check{D} = {\rm Hom}_{\mathscr{O}_{\mathscr{E}}}(D, \mathscr{O}_{\mathscr{E}}\frac{dT}{1+T})$, si $D \in \Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$,
• $\check{D} = {\rm Hom}_{\mathscr{E}}(D, \mathscr{E}\frac{dT}{1+T})$, si $D \in \Phi\Gamma^{\rm et}(\mathscr{E})$.

Si $D \in \Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$, et si $D_k = D/p^kD$, alors ${\rm Hom}_{\mathscr{O}_{\mathscr{E}}}(D, \mathscr{E}/\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T})$ est la limite inductive des $\check{D}_k$, et $\check{D}$ est le module de Tate de ${\rm Hom}_{\mathscr{O}_{\mathscr{E}}}(D, \mathscr{E}/\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T})$ (l'isomorphisme implicite dans cet énoncé est celui qui envoie $\mu \in \check{D}$ sur $(\mu_k)_{k\in\mathbf{N}}$, où $\mu_k(x)$ est l'image de $p^{-k}\mu(x)$ modulo $\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T}$).

L'accouplement naturel sur $\check{D} \times D$ est noté $\langle\ ,\ \rangle$. On munit $\check{D}$ d'actions de Γ et φ en imposant que

$$\langle\gamma(x), \gamma(y)\rangle = \gamma(\langle x, y\rangle), \quad \text{si } \gamma \in \Gamma, \quad \text{et} \quad \langle\varphi(x), \varphi(y)\rangle = \varphi(\langle x, y\rangle).$$

(4) La formule $\varphi(\frac{dT}{1+T}) = p\frac{dT}{1+T}$, qui semblerait naturelle, ne fournit pas un (φ, Γ)-module étale.

(La condition « D étale » est précisément ce qu'il faut pour garantir l'existence et l'unicité d'un tel φ sur $\check{D}$, si D est un (φ, Γ)-module sur $\mathscr{O}_{\mathscr{E}}$.) Alors $\check{D}$ est un objet de $\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}$ (resp. $\Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})$, resp. $\Phi\Gamma^{\mathrm{et}}(\mathscr{E})$), si D est un objet de $\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}$ (resp. $\Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})$, resp. $\Phi\Gamma^{\mathrm{et}}(\mathscr{E})$).

Dans tous les cas, le dual de Tate de $\check{D}$ est naturellement isomorphe, en tant que (φ, Γ)-module, à D.

3. Dual de Tate et dual topologique. — La formule

$$\{x, y\} = \mathrm{rés}_0\big(\langle \sigma_{-1} \cdot x, y\rangle\big)$$

définit un accouplement $\mathscr{O}_L$-bilinéaire sur $\check{D} \times D$ à valeurs dans :
- $L/\mathscr{O}_L$ si $D \in \Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}$,
- $\mathscr{O}_L$ si $D \in \Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})$,
- L si $D \in \Phi\Gamma^{\mathrm{et}}(\mathscr{E})$.

Proposition II.2.1. — *Si $x \in \check{D}$ et $y \in D$, alors*

$$\begin{aligned}
&\{\varphi(x), \varphi(y)\} = \{x, y\},\\
&\{(1+T)^b x, (1+T)^b y\} = \{x, y\}, \ \textit{si } b \in \mathbf{Z}_p,\\
&\{\gamma(x), \gamma(y)\} = \{x, y\}, \ \textit{si } \gamma \in \Gamma.
\end{aligned}$$

Démonstration. — On a $\langle \sigma_{-1}(\varphi(x)), \varphi(y)\rangle = \langle \varphi(\sigma_{-1}(x)), \varphi(y)\rangle = \varphi(\langle \sigma_{-1}(x), y\rangle)$. On déduit donc la formule pour φ du (ii) de la prop. I.4.2 et de ce que $\varphi(\frac{dT}{1+T}) = \frac{dT}{1+T}$.

On a $\langle \sigma_{-1}((1+T)^b x), (1+T)^b y\rangle = \langle (1+T)^{-b}\sigma_{-1}(x), (1+T)^b y\rangle = \langle \sigma_{-1}\cdot x, y\rangle$, par $\mathscr{O}_{\mathscr{E}}$-bilinéarité de $\langle\ ,\ \rangle$. On en déduit la seconde formule.

Si $a \in \mathbf{Z}_p^*$, on a $\langle \sigma_{-1}(\sigma_a(x)), \sigma_a(y)\rangle = \langle \sigma_a(\sigma_{-1}(x)), \sigma_a(y)\rangle = \sigma_a(\langle \sigma_{-1}(x), y\rangle)$. On déduit donc la formule pour σ_a du (i) de la prop. I.4.2 et de ce que $\sigma_a(\frac{dT}{1+T}) = a\frac{dT}{1+T}$.

Si M est un $\mathscr{O}_L$-module topologique, on note $M^\vee$ le dual de Pontryagin de M, ensemble des applications $\mathscr{O}_L$-linéaires continues de M dans $L/\mathscr{O}_L$. Si M est de longueur finie sur $\mathscr{O}_L$, il en est de même de $M^\vee$, et on a $\mathrm{lg}_{\mathscr{O}_L} M^\vee = \mathrm{lg}_{\mathscr{O}_L} M$.

Si M est un $\mathscr{O}_L$-module topologique, sans élément p-divisible, on note M^* le $\mathscr{O}_L$-dual de M, ensemble des applications $\mathscr{O}_L$-linéaires continues de M dans $\mathscr{O}_L$. Alors M^* est le module de Tate de $M^\vee$.

Si M est un L-espace vectoriel topologique, on note M^* son dual topologique, ensemble des applications L-linéaires continues de M dans L. Si M_0 est un $\mathscr{O}_L$-réseau de M, on a $M^* = L \otimes_{\mathscr{O}_L} M_0^*$.

On munit ces duaux de la topologie faible ($\mu_n \to \mu$ si et seulement si $\mu_n(v) \to \mu(v)$ pour tout $v \in M$).

Lemme II.2.2. — *Si $k \in \mathbf{N}$, l'application qui à $y \in \mathfrak{m}_L^{-k}\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}$ associe la forme linéaire $x \mapsto [y, x] = \mathrm{rés}_0(xy\,\frac{dT}{1+T})$ est un isomorphisme de $\mathfrak{m}_L^{-k}\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}$ sur $(\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^k)^\vee$.*

Démonstration. — Soit $D = \mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^k$. Si $f : D \to L/\mathscr{O}_L$ est $\mathscr{O}_L$-linéaire continue, alors $f(D) \subset \mathfrak{m}_L^{-k}\mathscr{O}_L/\mathscr{O}_L$ et il existe $m_0 \in \mathbf{N}$ tel que l'on ait $f(T^m) = 0$ si $m \geqslant m_0$. Ceci implique que la série

$(1+T)\big(\sum_{m\in\mathbf{Z}} T^{-m-1}f(T^m)\big)$ converge dans $\mathfrak{m}_L^{-k}\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}} = D^\vee$. La somme y de cette série est l'unique élément de $\mathfrak{m}_L^{-k}\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}$ vérifiant $[y, T^m] = f(T^m)$ quel que soit $m \in \mathbf{Z}$, et par continuité et linéarité, c'est aussi l'unique élément de $\mathfrak{m}_L^{-k}\mathscr{O}_{\mathscr{E}}/\mathscr{O}_{\mathscr{E}}$ vérifiant $[y,x] = f(x)$ quel que soit $x \in D$. Ceci permet de conclure.

Si D est un (φ,Γ)-module, et si $x \in \check{D}$, on note $\iota(x)$ la forme linéaire $y \mapsto \{x,y\}$ sur D.

Proposition II.2.3. — *Si $D \in \Phi\Gamma^{\rm et}_{\rm tors}$ (resp. $D \in \Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$, resp. $D \in \Phi\Gamma^{\rm et}(\mathscr{E})$), alors ι induit un isomorphisme de $\check{D}$ sur $D^\vee$ (resp. sur D^*, resp. sur D^*).*

Démonstration. — Si D est de torsion, on déduit du lemme II.2.2 et du théorème de structure des modules sur les anneaux principaux, que $x \mapsto \iota'(x) = \iota(\sigma_{-1}(x))$ est un isomorphisme de $\check{D}$ sur $D^\vee$. Il en est donc de même de ι. Le cas $D \in \Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$ s'en déduit en utilisant le fait que $\check{D}$ et D^* sont respectivement les modules de Tate des limites inductive des $\check{D}_k$ et $D_k^\vee$, où $D_k = D/p^kD$. Enfin, le cas $D \in \Phi\Gamma^{\rm et}(\mathscr{E})$ s'en déduit en tensorisant par L, cela permet de conclure.

Remarque II.2.4. — En utilisant le fait que le dual de Tate de $\check{D}$ est D, cela permet d'échanger les rôles de D et $\check{D}$ dans la prop. II.2.3, et donc d'obtenir des isomorphismes naturels $\iota : D \cong \check{D}^\vee$, si $D \in \Phi\Gamma^{\rm et}_{\rm tors}$, et $\iota : D \cong \check{D}^*$, si $D \in \Phi\Gamma^{\rm et}(\mathscr{O}_{\mathscr{E}})$ ou si $D \in \Phi\Gamma^{\rm et}(\mathscr{E})$.

4. Orthogonalité et treillis

Dans ce n°, D est un objet de $\Phi\Gamma^{\rm et}_{\rm tors}$.

Définition II.2.5. — *Si M est un treillis de D, on note $M^\perp$ le sous-$\mathscr{O}_L$-module de $\check{D}$ constitué des $x \in \check{D}$ tels que $\{x,y\} = 0$ quel que soit $y \in M$.*

Lemme II.2.6. — *Si M est un treillis de D, alors $M^\perp$ est un treillis de $\check{D}$. De plus, $(M^\perp)^\perp = M$.*

Démonstration. — Écrivons D sous la forme $D = \oplus_{i=1}^d (\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^{k_i})f_i$. Comme M est un treillis de D, il existe $a \geqslant b \in \mathbf{Z}$ tels que

$$\oplus_{i=1}^d T^a\mathscr{O}_{\mathscr{E}}^+ \cdot f_i \subset M \subset \oplus_{i=1}^d T^b\mathscr{O}_{\mathscr{E}}^+ \cdot f_i.$$

Soit π_L une uniformisante de L, et soit $f_i^\vee \in \check{D}$ l'homomorphisme envoyant f_i sur $\pi_L^{-k_i}\frac{dT}{1+T}$ et f_j sur 0 si $j \neq i$. On a alors $\check{D} = \oplus_{i=1}^d(\mathscr{O}_{\mathscr{E}}/\pi_L^{k_i}\mathscr{O}_{\mathscr{E}})f_i^\vee$. Maintenant, $\mathrm{rés}_0(xy\frac{dT}{1+T}) = 0$ quel que soit $y \in \mathscr{O}_{\mathscr{E}}^+/\pi_L^k$ si et seulement si $x \in \mathscr{O}_{\mathscr{E}}^+/\pi_L^k$; on en déduit les inclusions

$$\oplus_{i=1}^d T^{-b}\mathscr{O}_{\mathscr{E}}^+ \cdot f_i^\vee \subset M^\perp \subset \oplus_{i=1}^d T^{-a}\mathscr{O}_{\mathscr{E}}^+ \cdot f_i^\vee.$$

Finalement, comme $\{x, ay\} = \{\sigma_{-1}(a)x, y\}$, si $a \in \mathscr{O}_{\mathscr{E}}^+$, cela implique que $M^\perp$ est un $\mathscr{O}_{\mathscr{E}}^+$-module, et donc un treillis de D au vu des inclusions ci-dessus.

Enfin, l'égalité $(M^\perp)^\perp = M$ suit de ce que M est fermé dans D et $\{\ ,\ \}$ est une dualité parfaite d'après la prop. II.2.3. Ceci permet de conclure.

Lemme II.2.7. — *Si M est un treillis de D, alors $\iota : \check{D} \to D^\vee$ induit un isomorphisme de $M^\perp$ sur* $\mathrm{Hom}(D/M, L/\mathscr{O}_L)$.

Démonstration. — Par définition de $M^\perp$, la restriction de ι à $M^\perp$ se factorise en une application injective $\iota_M : M^\perp \to \mathrm{Hom}(D/M, L/\mathscr{O}_L)$. Maintenant, M étant un treillis de D, et D étant de torsion, M est ouvert dans D et D/M est un $\mathscr{O}_L$-module discret. Donc $\mathrm{Hom}(D/M, L/\mathscr{O}_L)$ s'identifie naturellement au sous-ensemble des $x \in D^\vee$ tels que $\{x, y\} = 0$ quel que soit $y \in M$. La surjectivité de ι permet de conclure à celle de ι_M

Lemme II.2.8. — *Si I est un ensemble fini, et si M_i, $i \in I$ sont des treillis de D, alors il existe un treillis M' de D, contenant les M_i, $i \in I$, tel que $D/M_i = D/M' \oplus M'/M_i$ quel que soit $i \in I$.*

Démonstration. — Écrivons D sous la forme $D = \oplus_{j=1}^d (\mathscr{O}_\mathscr{E}/\mathfrak{m}_L^{k_j}) f_j$. Il existe alors $b_i \in \mathbf{Z}$ tel que $M_i \subset \oplus_{j=1}^d T^{b_i} \mathscr{O}_\mathscr{E}^+ \cdot f_j$, et on peut prendre $M' = \oplus_{j=1}^d T^b \mathscr{O}_\mathscr{E}^+ \cdot f_j$, où $b = \sup_{i \in I} b_i$.

Proposition II.2.9. — *Si $M_1 \subset M_2$ sont des treillis de D, alors*

$$\lg_{\mathscr{O}_L}(M_1^\perp / M_2^\perp) = \lg_{\mathscr{O}_L}(M_2/M_1).$$

Démonstration. — Choisissons un treillis M' de D contenant M_1 et M_2, tel que $D/M_1 = D/M' \oplus M'/M_1$ et $D/M_2 = D/M' \oplus M'/M_2$. En utilisant le lemme II.2.7, on voit que l'on est ramené à prouver que

$$\lg_{\mathscr{O}_L}\big(\mathrm{Hom}(M'/M_1, L/\mathscr{O}_L)/\mathrm{Hom}(M'/M_2, L/\mathscr{O}_L)\big) = \lg_{\mathscr{O}_L}(M_2/M_1),$$

ce qui suit de ce que tous les modules en présence sont de longueur finie sur $\mathscr{O}_L$, et donc

$$\begin{aligned}\lg_{\mathscr{O}_L}\big((M'/M_1)^\vee/(M'/M_2)^\vee\big) &= \lg_{\mathscr{O}_L}(M'/M_1) - \lg_{\mathscr{O}_L}(M'/M_2) \\ &= \lg_{\mathscr{O}_L}((M'/M_1)/(M'/M_2)) = \lg_{\mathscr{O}_L}(M_2/M_1).\end{aligned}$$

II.3. Les foncteurs $D \mapsto D^\sharp$ et $D \mapsto D^\natural$

Ce chapitre est consacré à la définition et l'étude des sous-modules D^+, D^{++}, D^{nr}, $D^\natural$ et $D^\sharp$ d'un (φ, Γ)-module étale D. Sauf mention explicite du contraire, les (φ, Γ)-modules considérés sont étales sur $\mathscr{O}_\mathscr{E}$, et les résultats valables pour $D \in \Phi\Gamma^{\mathrm{et}}(\mathscr{O}_\mathscr{E})$ s'étendent à $\Phi\Gamma^{\mathrm{et}}(\mathscr{E})$ en tensorisant par L.

1. Les modules D^+ et D^{++}. — Dans tout ce §, on fixe un (φ, Γ)-module D étale sur $\mathscr{O}_\mathscr{E}$. On note :

- D^+ l'ensemble des $x \in D$ tels que la suite $(\varphi^n(x))_{n \in \mathbf{N}}$ soit bornée dans D,
- D^{++} l'ensemble des $x \in D$ tels que $\varphi^n(x) \to 0$,

Proposition II.3.1. — *Si D est de torsion, alors D^+ et D^{++} sont des treillis de D.*

Démonstration. — Il est immédiat que D^+ et D^{++} sont des sous-$\mathscr{O}_\mathscr{E}^+$-modules de D. Le fait que ce soient des treillis est une conséquence du (ii) du lemme II.3.2 ci-dessous.

Lemme II.3.2. — *Soient $e_1, \dots, e_d \in D$ tels que $D = (\mathscr{O}_\mathscr{E}/\mathfrak{m}_L^{k_1})e_1 \oplus \cdots \oplus (\mathscr{O}_\mathscr{E}/\mathfrak{m}_L^{k_d})e_d$, et soit k le maximum des k_i, pour $1 \leqslant i \leqslant d$.*

(i) *Il existe des entiers relatifs $n_0 \geqslant n_1$, et des matrices $A = (a_{i,j})_{1\leqslant i,j\leqslant d}$ et $B = (b_{i,j})_{1\leqslant i,j\leqslant d}$, à coefficients dans $T\mathscr{O}_{\mathscr{E}}^{+}/\mathfrak{m}_L^k$, éléments de $\mathbf{GL}_d(\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^k)$, telles que l'on ait*

$$\varphi(T^{n_0}e_i) = \sum_{j=1}^{d} a_{i,j}T^{n_0}e_j \quad \text{et} \quad T^{n_1}e_i = \sum_{j=1}^{d} b_{i,j}\varphi(T^{n_1}e_j), \quad \text{si } 1 \leqslant i \leqslant d.$$

(ii) *Si N_0 (resp. N_1) est le $\mathscr{O}_{\mathscr{E}}^{+}$-module de D engendré par les $T^{n_0}e_i$ (resp. les $T^{n_1}e_i$), pour $1 \leqslant i \leqslant d$, alors*

$$\varphi(N_0) \subset TN_0 \subset D^{++} \subset D^{+} \subset N_1 \subset \mathscr{O}_{\mathscr{E}}^{+} \cdot \varphi(N_1).$$

Démonstration. — $e_1, \dots, e_d$ et $\varphi(e_1), \dots, \varphi(e_d)$ sont des familles génératrices de D sur $\mathscr{O}_{\mathscr{E}}$. Comme D est tué par $\mathfrak{m}_L^k$, il existe des matrices $A' = (a'_{i,j})_{1\leqslant i,j\leqslant d}$ et $B' = (b'_{i,j})_{1\leqslant i,j\leqslant d}$, éléments de $\mathbf{GL}_d(\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^k)$, telles que l'on ait

$$\varphi(e_i) = \sum_{j=1}^{d} a'_{i,j}e_j \quad \text{et} \quad e_i = \sum_{j=1}^{d} b'_{i,j}\varphi(e_j), \quad \text{si } 1 \leqslant i \leqslant d.$$

On a $(\varphi(T)/T)^{p^k} = T^{(p-1)p^k}$ dans $\mathscr{O}_{\mathscr{E}}^{+}/\mathfrak{m}_L^k$; il existe donc $n \in \mathbf{N}$ tel que $(\varphi(T)/T)^{np^k}A'$ et $(\varphi(T)/T)^{np^k}B'$ soient à coefficients dans $T\mathscr{O}_{\mathscr{E}}^{+}/\mathfrak{m}_L^k$, et on peut prendre $n_0 = np^k$, $n_1 = -np^k$, $A = (\varphi(T)/T)^{np^k}A'$ et $B = (\varphi(T)/T)^{np^k}B'$.

Maintenant, les inclusions $\varphi(N_0) \subset TN_0$ et $N_1 \subset \mathscr{O}_{\mathscr{E}}^{+} \cdot \varphi(N_1)$ suivent de la construction de N_0 et N_1. On déduit de la première, par une récurrence immédiate, que l'on a $\varphi^n(N_0) \subset \varphi^n(T)N_0$, et comme $\varphi^n(T) \to 0$, cela montre que $N_0 \subset D^{++}$ (et donc, a fortiori, $TN_0 \subset D^{++}$). Enfin, si $n \in \mathbf{N}$, il existe $b_{i,j,n} \in \mathscr{O}_{\mathscr{E}}^{+}$ tels que $T^{n_1}e_i = \sum_{j=1}^{d} b_{i,j,n}\varphi^n(T^{n_1}e_j)$, si $1 \leqslant i \leqslant d$. On en déduit que si $x = \sum_{i=1}^{d} x_iT^{n_1}e_i \in D^{+}$, et si $\varphi^n(x) = \sum_{j=1}^{d} x_{i,n}T^{n_1}e_i$, alors $\varphi^n(x_i) = \sum_{j=1}^{d} b_{i,j,n}x_{j,n}$, et donc que la suite $\varphi^n(x_i)$ est bornée dans $\mathscr{O}_{\mathscr{E}}/\mathfrak{m}_L^{k_i}$. Ceci implique que $x_i \in \mathscr{O}_{\mathscr{E}}^{+}/\mathfrak{m}_L^{k_i}$, et donc que $x \in N_1$. On en déduit l'inclusion $D^{+} \subset N_1$ qui termine la démonstration du lemme.

Remarque II.3.3. — Si D n'est pas de torsion, D^{+} et D^{++} sont en général nuls. Il peut quand même arriver que D^{+} soit assez gros pour engendrer D, auquel cas on dit que D est *de hauteur finie*.

2. L'opérateur ψ. — Soit D un (φ, Γ)-module étale sur $\mathscr{O}_{\mathscr{E}}$. Comme les $(1+T)^i$, pour $0 \leqslant i \leqslant p-1$, forment une base de $\mathscr{O}_{\mathscr{E}}$ sur $\varphi(\mathscr{O}_{\mathscr{E}})$, on peut écrire tout élément x de D, de manière unique, sous la forme

$$x = \sum_{i=0}^{p-1}(1+T)^i\varphi(x_i),$$

ce qui nous permet de définir un opérateur $\psi : D \to D$ par la formule $\psi(x) = x_0$; c'est un inverse à gauche de φ (i.e. $\psi(\varphi(x)) = x$) qui va jouer un rôle primordial dans la suite.

L'action de Γ n'est pas utilisée dans la définition de ψ et cette définition est donc valable pour tout φ-module étale non nécessairement muni d'une action additionnelle de Γ. Dans le cas d'un

(φ,Γ)-module, ψ commute à l'action de Γ : en effet, si $a\in\mathbf{Z}_p^*$, on a

$$\sigma_a\big(\sum_{i=0}^{p-1}(1+T)^i\varphi(x_i)\big)=\sum_{i=0}^{p-1}(1+T)^{ai}\varphi(\sigma_a(x_i))=\varphi(\sigma_a(x_0))+\sum_{i=1}^{p-1}(1+T)^{j_i}\varphi((1+T)^{b_i}\sigma_a(x_i)),$$

où $j_i\in\{1,\dots,p-1\}$ et $b_i\in\mathbf{Z}_p$ sont définis par $ai=j_i+pb_i$; on a donc $\psi(\sigma_a(x))=\sigma_a(x_0)=\sigma_a(\psi(x))$.

3. ψ comme adjoint de φ. — Ce qui suit est à la base de la définition [?] de la dualité locale de Tate en termes de (φ,Γ)-modules.

Lemme II.3.4. — *Soient D,D_1,D_2 des (φ,Γ)-module étales sur $\mathscr{O}_{\mathscr{E}}$.*
(i) *Si $x\in\mathscr{O}_{\mathscr{E}}$ et si $y\in D$, alors $\psi(\varphi(x)y)=x\psi(y)$ et $\psi(x\varphi(y))=\psi(x)y$.*
(ii) *Si $x\in D_1$ et si $y\in D_2$, alors $\psi(\varphi(x)\otimes y)=x\otimes\psi(y)$.*
(iii) *Si $x\in\check{D}$ et $y\in D$, alors $\psi(\langle\varphi(x),y\rangle)=\langle x,\psi(y)\rangle$.*

Démonstration. — La démonstration étant la même dans les trois cas, nous nous contenterons de traiter le (ii). Si $y=\sum_{i=0}^{p-1}\varphi(y_i)(1+T)^i$, alors $\varphi(x)\otimes y=\sum_{i=0}^{p-1}\varphi(x\otimes y_i)(1+T)^i$ et donc

$$\psi(\varphi(x)\otimes y)=x\otimes y_0=x\otimes\psi(y).$$

Corollaire II.3.5. — *Si $x\in\check{D}$ et $y\in D$, alors*

$$\{x,\varphi(y)\}=\{\psi(x),y\}\quad\text{et}\quad\{\varphi(x),y\}=\{x,\psi(y)\}.$$

Démonstration. — C'est une conséquence immédiate du (ii) de la prop. I.4.2 et du (iii) du lemme II.3.4.

4. Les modules $D^\natural$ et $D^\sharp$. — On dit qu'un sous-ensemble M de D est *φ-saturé* s'il est stable par φ et si $\varphi(x)\in M$ implique $x\in M$. Il est immédiat, sur la définition, que D^+ et D^{++} sont φ-saturés.

Proposition II.3.6. — *Soient $D\in\Phi\Gamma^{\rm et}_{\rm tors}$ et M un treillis de D.*
(i) *Si M est stable par φ, alors $M\subset D^+$.*
(ii) *Si M est φ-saturé, alors $M\supset D^{++}$.*

Démonstration. — Si M est stable par φ et $x\in M$, on a $\varphi^n(x)\in M$ pour tout M, et donc la suite $(\varphi^n(x))_{n\in\mathbf{N}}$ est bornée. On en déduit le (i).

D^{++} est, comme tout treillis, de type fini sur $\mathscr{O}_{\mathscr{E}}^+$; on peut donc en choisir une famille génératrice finie $(e_i)_{i\in I}$. Maintenant, M étant ouvert, il résulte de la définition de D^{++} que $\varphi^n(e_i)\in M$, pour n assez grand ; on en déduit l'existence de n tel que $\varphi^n(D^{++})\subset M$, et M étant supposé saturé, cela implique que $D^{++}\subset M$. Ceci permet de conclure.

Lemme II.3.7. — *Soient $D\in\Phi\Gamma^{\rm et}_{\rm tors}$ et M un treillis de D.*

(i) *Les conditions « M est stable par φ » et « $M^\perp$ est stable par ψ » sont équivalentes ; les conditions « $M^\perp$ est stable par φ » et « M est stable par ψ » sont équivalentes.*

(ii) *Les conditions « M est φ-saturé » et « ψ induit une surjection de $M^\perp$ sur lui-même » sont équivalentes ; les conditions « $M^\perp$ est φ-saturé » et « ψ induit une surjection de M sur lui-même » sont équivalentes.*

Démonstration. — Le (i) est une conséquence formelle de ce que ψ est l'adjoint de ψ.

Le (ii) suit de ce que les conditions $x \in \psi(M^\perp)^\perp$ et $\varphi(x) \in (M^\perp)^\perp = M$ sont équivalentes.

- On définit $D^\natural$ et $D^\sharp$ comme les orthogonaux respectifs de $\check{D}^+$ et $\check{D}^{++}$.

Proposition II.3.8. — (i) *$D^\natural$ et $D^\sharp$ sont stables par ψ qui agit surjectivement.*

(ii) *$D^\natural$ est le plus petit treillis de D stable par ψ.*

(iii) *$D^\sharp$ est le plus grand treillis de D sur lequel ψ agit surjectivement.*

Démonstration. — Le (i) est une conséquence directe du lemme II.3.7 puisque $\check{D}^+$ et $\check{D}^{++}$ sont φ-saturés.

Maintenant, si M est stable par ψ, alors $M^\perp$ est stable par φ et donc est inclus dans $\check{D}^+$ d'après la prop. II.3.6 ; son orthogonal, qui n'est autre que M, contient donc $D^\natural$, ce qui démontre le (ii).

Enfin, si $\psi : M \to M$ est surjectif, alors $M^\perp$ est φ-saturé d'après le lemme II.3.7 et donc contient $\check{D}^{++}$ d'après la prop. II.3.6 ; son orthogonal, qui n'est autre que M, est donc contenu dans $D^\sharp$, ce qui démontre le (ii).

Proposition II.3.9. — *On a $D^{++} \subset D^+ \subset D^\natural \subset D^\sharp$.*

Démonstration. — La seule inclusion non triviale est $D^+ \subset D^\natural$. Soit donc $z \in D^+$. Alors $T\varphi(z) \in D^{++}$, et donc $\varphi^n(T\varphi(z)) \in D^\natural + p^kD$ pour n assez grand (dépendant de k). On en déduit que $y = \psi^{n+1}(\varphi^n(T\varphi(z)))$ appartient aussi à $D^\natural + p^kD$, et comme $y = \psi(T\varphi(z)) = \psi(T)z = -z$, on a $z \in D^\natural + p^kD$. Ceci étant vrai pour tout $k \in \mathbf{N}$, on a $z \in D^\natural$, ce qui permet de conclure.

Proposition II.3.10. — *Si M est un treillis, alors $\psi^n(M) \subset D^\sharp$ et $\psi^n(M) \supset D^\natural$, pour tout n assez grand.*

Démonstration. — On a $\varphi^n(\check{D}^{++}) \subset M^\perp$ et donc $\psi^n(M) \subset (\check{D}^{++})^\perp = D^\sharp$, pour tout n assez grand, d'où la première inclusion. Pour démontrer la seconde, on peut, quitte à diminuer M, supposer que $M = \varphi^n(T)D^+$. On a alors $\varphi(M) \subset M$, et donc $\psi(M) \supset M$, ce qui fait que la suite des $\psi^k(M)$ est une suite croissante de treillis de D inclus dans $D^\natural$ (puisque M l'est et que $D^\natural$ est stable par ψ). Le suite est donc stationnaire et la limite est un treillis de D stable par ψ, et qui, de ce fait, contient $D^\natural$ (prop. II.3.8). On en déduit l'inclusion $\psi^n(M) \supset D^\natural$, pour tout n assez grand, ce qui permet de conclure.

Proposition II.3.11. — *Si $f : D \to D_2$ est un morphisme surjectif d'éléments de $\Phi\Gamma^{\rm et}_{\rm tors}$, alors f induit des surjections de $D^\natural$ sur $D_2^\natural$ et de $D^\sharp$ sur $D_2^\sharp$.*

Démonstration. — Soit $D_1 = \operatorname{Ker} f$, et soit M l'image de $\check{D}^+$ dans $\check{D}_1$; c'est un treillis de $\check{D}_1$ car $\check{D}^+$ étant un $\mathscr{O}_{\mathscr{E}}^+$-module de type fini, il en est de même de son image par la surjection naturelle

$\check{D} \to \check{D}_1$. Dans le diagramme commutatif suivant, les deux lignes horizontales sont surjectives par définition de $D^\natural$, et les deux colonnes verticales de droite sont exactes par dualité de Pontryagin.

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & D_1 \arrow[r] \arrow[d] & M^\vee \arrow[d] & \\
0 \arrow[r] & D^\natural \arrow[r] \arrow[d] & D \arrow[r] \arrow[d] & (\check{D}^+)^\vee \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & D_2^\natural \arrow[r] & D_2 \arrow[r] \arrow[d] & (\check{D}_2^+)^\vee \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

Comme $D_1 \to M^\vee$ est surjective par dualité de Pontryagin, il résulte du lemme du serpent que $D^\natural \to D_2^\natural$ l'est aussi. Le raisonnement étant identique pour $D^\sharp \to D_2^\sharp$, cela permet de conclure.

Si $D \in \Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})$, on définit $D^\natural$ et $D^\sharp$ comme les limites projectives respectives des $(D/p^kD)^\natural$ et $(D/p^kD)^\sharp$.

Remarque II.3.12. — (i) Il résulte de la prop. II.3.11 que la réduction modulo p^k induit des surjections de $D^\natural$ sur $(D/p^kD)^\natural$ et de $D^\sharp$ sur $(D/p^kD)^\sharp$.

(ii) Il résulte de la prop. II.3.10 que, si M est un treillis de D, et si $k \in \mathbf{N}$, alors $\psi^n(M) \subset D^\sharp + p^kD$ et $\psi^n(M) + p^kD \supset D^\natural$, pour tout n assez grand.

5. Le module D^{nr}

Soit $D^{\mathrm{nr}} = \cap_{n\in\mathbf{N}}\varphi^n(D)$. Le (ii) de la prop. II.3.13 ci-dessous montre que D^{nr} est petit. Par exemple, $k_{\mathscr{E}}^{\mathrm{nr}} = k_L$ et $\mathscr{O}_{\mathscr{E}}^{\mathrm{nr}} = \mathscr{O}_L$.

Proposition II.3.13. — (i) D^{nr} *est inclus dans* D^+ *et* $D^+ = D^{\mathrm{nr}} \oplus D^{++}$.

(ii) $\dim_{k_L} D^{\mathrm{nr}}/\mathfrak{m}_L \leqslant \dim_{k_{\mathscr{E}}} D/\mathfrak{m}_L$.

Démonstration. — Si $x \in D^{\mathrm{nr}}$, on peut écrire x sous la forme $\varphi^n(x_n)$. On a alors $x_n = \psi^n(x)$, et donc $x_n \in D^\sharp$, pour tout n assez grand. Comme $D^\sharp/D^+$ est de longueur finie sur $\mathscr{O}_L$, et donc est un ensemble fini, il existe $a < b$ tels que $x_a - x_b \in D^+$. Il s'ensuit que $\varphi^b(x_a) - \varphi^a(x_a) \in D^+$, et donc que la suite $(\varphi^n(x_a))_{n\in\mathbf{N}}$ ne prend qu'un nombre fini de valeurs modulo D^+ ; elle est donc bornée, ce qui implique $x_a \in D^+$ et donc que x, qui est égal à $\varphi^a(x_a)$, appartient à D^+. D'où l'inclusion $D^{\mathrm{nr}} \subset D^+$.

Maintenant, si $x \in D^{\mathrm{nr}} \cap D^{++}$, on peut écrire x sous la forme $x = \varphi^n(x_n)$, avec $x_n \in D^{++}$, pour tout $n \in \mathbf{N}$. Comme l'intersection des $\varphi^n(D^{++})$ est réduite à 0, on en déduit que $D^{\mathrm{nr}} \cap D^{++} = 0$.

Enfin, $\varphi : D^+/D^{++} \to D^+/D^{++}$ est injective et donc aussi surjective puisque D^+/D^{++} est fini. Il en résulte que si $x \in D^+$, il existe, pour tout $n \in \mathbf{N}$, $x_n \in D^+$ tel que $x - \varphi^n(x_n) \in D^{++}$.

Soit alors y une valeur d'adhérence de la suite des $\varphi^n(x_n)$. Par construction, $y - x \in D^{++}$, et $\varphi^a(D^+)$ étant fermé (car compact), on a $y \in \varphi^a(D^+)$, pour tout $a \in \mathbf{N}$. On en déduit l'appartenance de y à D^{nr}, ce qui termine la démonstration du (i).

Passons à celle du (ii). Le $\mathscr{O}_L$-module D^{nr} est de rang fini puisque D^{nr} est un ensemble fini comme quotient D^+/D^{++} de deux treillis. Soit $e_1, \dots, e_r \in D^{\mathrm{nr}}$ tels que $D^{\mathrm{nr}} = \oplus_{i=1}^r (\mathscr{O}_L/\mathfrak{m}_L^{k_i})e_i$. Il s'agit de prouver que $e_1, \dots, e_d$ sont libres sur $\mathscr{O}_{\mathscr{E}}$ au sens qu'il n'existe pas de relation de la forme $\sum_{i=1}^r \lambda_i e_i = 0$ où un des λ_i est non nul modulo $\mathfrak{m}_L^{k_i}$.

Supposons le contraire, et choisissons une telle relation de longueur minimale. Quitte à permuter les e_i et à multiplier par une unité de $\mathscr{O}_{\mathscr{E}}$, on peut supposer que λ_1 est un élément non nul de $\mathscr{O}_L/\mathfrak{m}_L^{k_1}$. Maintenant, D^{nr} est stable par φ, et comme il est fini, il existe $n \in \mathbf{N}$ tel que φ^n soit l'identité de D^{nr}. On a alors $\sum_{i=1}^r \varphi^n(\lambda_i)e_i = 0$, et donc $\sum_{i=2}^r (\varphi^n(\lambda_i) - \lambda_i)e_i = 0$. Par minimalité de la relation initiale, cela implique que $\varphi^n(\lambda_i) - \lambda_i = 0$, pour tout i, et donc que $\lambda_i \in \mathscr{O}_L$, pour tout i. D'où une contradiction qui permet de conclure.

Remarque II.3.14. — $D^\sharp/D^\natural$ est le dual de de $\check{D}^+/\check{D}^{++} = \check{D}^{\mathrm{nr}}$, et donc est petit.

II.4. Les $P(\mathbf{Q}_p)$-modules $D \boxtimes \mathbf{Q}_p$, $D^\sharp \boxtimes \mathbf{Q}_p$ et $D^\natural \boxtimes \mathbf{Q}_p$

1. Définition. — Si D est un (φ, Γ)-module étale sur $\mathscr{O}_{\mathscr{E}}$, alors D et ses sous-modules $D^\sharp$ et $D^\natural$ sont naturellement des $(P(\mathbf{Z}_p), \psi)$-modules, l'action de ψ étant celle définie au § 2, et $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in P(\mathbf{Z}_p)$ agissant par $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z = (1+T)^b \sigma_a(z)$. On peut donc considérer le $P(\mathbf{Q}_p)$-module $D \boxtimes \mathbf{Q}_p$ et ses sous-$P(\mathbf{Q}_p)$-modules $D^\sharp \boxtimes \mathbf{Q}_p$ et $D^\natural \boxtimes \mathbf{Q}_p$. Les formules de la prop. I.6.1 peuvent se tr aduire en termes de (φ, Γ)-modules : si $z = (z^{(n)})_{n \in \mathbf{Z}} \in D \boxtimes \mathbf{Q}_p$, alors

$$\Big(\left(\begin{smallmatrix} p^k & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot z\Big)^{(n)} = z^{(n+k)} \text{ si } k \in \mathbf{Z}, \quad \text{en particulier, } \Big(\left(\begin{smallmatrix} p^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot z\Big)^{(0)} = z^{(-1)} = \psi(z^{(0)})\,;$$
$$\Big(\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot z\Big)^{(n)} = \sigma_a(z^{(n)}) \ \text{ si } a \in \mathbf{Z}_p^*\,;$$
$$\Big(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z\Big)^{(n)} = (1+T)^{bp^n} z^{(n)} \ \text{ si } b \in \mathbf{Q}_p \text{ et } n \geqslant -v_p(b).$$

Les modules $D^\sharp$ et $D^\natural$ étant compacts, il en est de même de $D^\sharp \boxtimes \mathbf{Q}_p$ et $D^\natural \boxtimes \mathbf{Q}_p$ qui, rappelons-le, sont munis de la topologie induite par la topologie produit.

Si D est un (φ, Γ)-module étale sur $\mathscr{E}$, on définit des sous-$P(\mathbf{Q}_p)$-modules $(D \boxtimes \mathbf{Q}_p)_b$, $(D^\natural \boxtimes \mathbf{Q}_p)_b$ et $(D^\sharp \boxtimes \mathbf{Q}_p)_b$ de $D \boxtimes \mathbf{Q}_p$, $D^\natural \boxtimes \mathbf{Q}_p$ et $D^\sharp \boxtimes \mathbf{Q}_p$ respectivement, par

$$(D \boxtimes \mathbf{Q}_p)_b = L \otimes_{\mathscr{O}_L} (D_0 \boxtimes \mathbf{Q}_p), \quad (D^\natural \boxtimes \mathbf{Q}_p)_b = L \otimes_{\mathscr{O}_L} (D_0^\natural \boxtimes \mathbf{Q}_p) \quad rmet \quad (D^\sharp \boxtimes \mathbf{Q}_p)_b = L \otimes_{\mathscr{O}_L} (D_0^\sharp \boxtimes \mathbf{Q}_p),$$

où D_0 est n'importe quel réseau de D stable par φ et Γ. On munit ces espaces de la topologie de la limite inductive, ce qui fait de $(D^\natural \boxtimes \mathbf{Q}_p)_b$ et $(D^\sharp \boxtimes \mathbf{Q}_p)_b$ des L-espaces vectoriels complets pour une topologie localement convexe et localement compacte.

Exemple II.4.1. — L'isomorphisme $\mathscr{O}_{\mathscr{E}}^\natural \cong \mathscr{D}_0(\mathbf{Z}_p, \mathscr{O}_L)$ de l'exemple **??** nous fournit un isomorphisme de $\mathscr{O}_L$-modules compacts $\mathscr{O}_{\mathscr{E}}^\natural \boxtimes \mathbf{Q}_p \cong \mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$, où $\mathscr{D}_0(\mathbf{Q}_p, \mathscr{O}_L)$ est muni de la topologie de la convergence faible.

En tensorisant par L, on en déduit un isomorphisme de L-espaces vectoriels topologiques $(\mathscr{E}^\natural \boxtimes \mathbf{Q}_p)_b \cong \mathscr{D}_0(\mathbf{Q}_p)$, où $\mathscr{D}_0(\mathbf{Q}_p)$ est muni de la topologie de la convergence faible. (Rappelons

[?] que $\mathscr{D}_0(\mathbf{Q}_p)$ désigne l'ensemble des distributions sur $\mathbf{Q}_p$ qui sont *globalement d'ordre* 0, et que l'on a $\mathscr{D}_0(\mathbf{Q}_p) = L\otimes_{\mathscr{O}_L}\mathscr{D}_0(\mathbf{Z}_p,\mathscr{O}_L)$; c'est le dual des fonctions continues sur $\mathbf{Q}_p$ tendant vers 0 à l'infini). L'espace $\mathscr{E}^\natural\boxtimes\mathbf{Q}_p$ est, quant à lui, l'espace des mesures sur $\mathbf{Q}_p$ (i.e. le dual des fonctions continues à support compact).

Remarque II.4.2. — (i) D est aussi muni d'une structure de $(P(\mathbf{Z}_p),\varphi,\psi)$-module ; on dispose donc, pour tout ouvert compact U de $\mathbf{Q}_p$, d'un sous-$\mathscr{O}_L$-module $D\boxtimes U$ de $D\boxtimes\mathbf{Q}_p$ et d'un projecteur $\mathrm{Res}_U : D\boxtimes\mathbf{Q}_p\to D\boxtimes U$, et d'un sous-$P(\mathbf{Q}_p)$-module $(D\boxtimes\mathbf{Q}_p)_c$ de $D\boxtimes\mathbf{Q}_p$.

(ii) Du point de vue de la correspondance de Langlands locale p-adique, le module le plus important est $D^\natural\boxtimes\mathbf{Q}_p$, mais le foncteur $D\mapsto D^\natural\boxtimes\mathbf{Q}_p$ jouit de propriétés moins agréables que le foncteur $D\mapsto D^\sharp\boxtimes\mathbf{Q}_p$ (cf. th. **??**). Comme $D^\sharp\boxtimes\mathbf{Q}_p/D^\natural\boxtimes\mathbf{Q}_p$ est petit (cor. **??**), on peut utiliser les bonnes propriétés du foncteur $D\mapsto D^\sharp\boxtimes\mathbf{Q}_p$ pour étudier le module $D^\natural\boxtimes\mathbf{Q}_p$.

(iii) On déduit de la propriété (iii) de $D^\sharp$ que si $z=(z^{(n)})_{n\in\mathbf{N}}\in D\boxtimes\mathbf{Q}_p$ est bornée (pour la topologie faible), alors $z^{(n)}\in D^\sharp$ pour tout $n\in\mathbf{N}$. Il en résulte que $D^\sharp\boxtimes\mathbf{Q}_p$ peut aussi être décrit comme l'ensemble des suites $z=(z^{(n)})_{n\in\mathbf{N}}$ de $D\boxtimes\mathbf{Q}_p$, bornées dans D pour la topologie faible.

(iv) Le module $D^{\psi=1}$ s'identifie naturellement à un sous-$\mathscr{O}_L$-module de $D^\sharp\boxtimes\mathbf{Q}_p$. Ce module joue un rôle très important en théorie d'Iwasawa.

Lemme II.4.3. — *Soit $M\subset D^\sharp\boxtimes\mathbf{Q}_p$ un sous-$\mathscr{O}_L$-module fermé, stable par $P(\mathbf{Q}_p)$, et, si $k\in\mathbf{Z}$, soit $M^{(k)}$ l'ensemble des $x\in D$ tels qu'il existe $z=(z^{(n)})_{n\in\mathbf{Z}}\in M$, avec $z^{(k)}=x$. Alors*

(i) $M^{(k)}=M^{(0)}$ *quel que soit* $k\in\mathbf{Z}$ *;*

(ii) $M^{(0)}$ *est un sous-$\mathscr{O}_{\mathscr{E}}^+$-module de $D^\sharp$ stable par ψ, qui agit surjectivement, et par Γ.*

(iii) $M=M^{(0)}\boxtimes\mathbf{Q}_p$.

Démonstration. — Les (i) et (ii) sont immédiats, ainsi que l'inclusion $M\subset M^{(0)}\boxtimes\mathbf{Q}_p$. Reste l'inclusion $M^{(0)}\boxtimes\mathbf{Q}_p\subset M$ à vérifier. Soit $z=(z^{(n)})_{n\in\mathbf{Z}}\in M^{(0)}\boxtimes\mathbf{Q}_p$. Si $k\in\mathbf{N}$, il existe $u_k=(u_k^{(n)})_{n\in\mathbf{Z}}\in M$ tel que $u_k^{(k)}=z^{(k)}$ car $M^{(k)}=M^{(0)}$. Par définition de la topologie sur $D^\sharp\boxtimes\mathbf{Q}_p$, la suite u_k tend vers z dans $D^\sharp\boxtimes\mathbf{Q}_p$ quand k tend vers $+\infty$, et M étant supposé fermé, cela implique $z\in M$, ce qui permet de conclure.

Remarque II.4.4. — Si M est un sous-$\mathscr{O}_L$-module compact de $D\boxtimes\mathbf{Q}_p$ stable par $P(\mathbf{Q}_p)$, alors $M^{(0)}=\mathrm{Res}_{\mathbf{Z}_p}M$ est un sous-$\mathscr{O}_{\mathscr{E}}^+$-module compact de D sur lequel ψ agit surjectivement ; on a donc $M^{(0)}\subset D^\sharp$ et $M\subset D^\sharp\boxtimes\mathbf{Q}_p$.

2. Dualité

Si $x\in(\check D\boxtimes\mathbf{Q}_p)_c$ et $y\in(D\boxtimes\mathbf{Q}_p)_c$, il existe $n\in\mathbf{N}$ tel que

$$x_n=\left(\begin{smallmatrix}p^n&0\\0&1\end{smallmatrix}\right)\cdot x\in\check D\boxtimes\mathbf{Z}_p=\check D\quad\text{et}\quad y_n=\left(\begin{smallmatrix}p^n&0\\0&1\end{smallmatrix}\right)\cdot y\in D\boxtimes\mathbf{Z}_p=D.$$

Comme $x_{n+1}=\varphi(x_n)$ et $y_{n+1}=\varphi(y_n)$, il résulte de la prop. II.2.1 que la quantité $\{x_n,y_n\}$ ne dépend pas du choix de n. Ceci nous fournit un accouplement sur $(\check D\boxtimes\mathbf{Q}_p)_c\times(D\boxtimes\mathbf{Q}_p)_c$ à valeurs dans $L/\mathscr{O}_L$ (resp. $\mathscr{O}_L$, resp. L), si $D\in\Phi\Gamma^{\mathrm{et}}_{\mathrm{tors}}$ (resp. $D\in\Phi\Gamma^{\mathrm{et}}(\mathscr{O}_{\mathscr{E}})$, resp. $D\in\Phi\Gamma^{\mathrm{et}}(\mathscr{E})$). On note

$\{\ ,\ \}_{\mathbf{Q}_p}$ cet accouplement. Sa restriction à $\check{D}\times D = (\check{D}\boxtimes \mathbf{Z}_p)\times(D\boxtimes\mathbf{Z}_p)$ est l'accouplement $\{\ ,\ \}$ défini précédemment.

Proposition II.4.5. — (i) *Si U,V sont des ouverts compacts disjoints de $\mathbf{Q}_p$, et si $x\in\check{D}\boxtimes U$ et $y\in D\boxtimes V$, alors $\{x,y\}_{\mathbf{Q}_p}=0$.*

(ii) *Si $g\in P(\mathbf{Q}_p)$, alors $\{g\cdot x, g\cdot y\}_{\mathbf{Q}_p}=\{x,y\}_{\mathbf{Q}_p}$.*

Démonstration. — Quitte à remplacer x et y par $\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)\cdot x$ et $\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)\cdot y$, ce qui, par construction, ne change pas la valeur de $\{x,y\}_{\mathbf{Q}_p}$, on peut supposer que U et V sont inclus dans $\mathbf{Z}_p$. On peut de plus partitionner U et V de manière à se ramener au cas $U=a+p^n\mathbf{Z}_p$, $V=b+p^n\mathbf{Z}_p$, et $a-b\notin p^n\mathbf{Z}_p$. Alors

$$\left(\begin{smallmatrix} -1 & 0\\ 0 & 1\end{smallmatrix}\right)x\in D\boxtimes(-a+p^n\mathbf{Z}_p)\quad\text{et}\quad z=\langle\left(\begin{smallmatrix} -1 & 0\\ 0 & 1\end{smallmatrix}\right)x,y\rangle\in\mathscr{O}_{\mathscr{E}}\frac{dT}{1+T}\boxtimes((b-a)+p^n\mathbf{Z}_p).$$

Comme $b-a\notin p^n\mathbf{Z}_p$, on a $\varphi^n(\psi^n(z))=\mathrm{Res}_{p^n\mathbf{Z}_p}(z)=0$, et donc $\psi^n(z)=0$. Par définition, on a $\{x,y\}=\mathrm{rés}_0(z)$, et comme $\mathrm{rés}_0(z)=\mathrm{rés}_0(\psi^n(z))$ d'après le (ii) de la prop. I.4.2, on obtient $\{x,y\}=0$, ce qui démontre le (i).

Pour démontrer le (ii), il suffit de prouver que $\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{x,y\}_{\mathbf{Q}_p}$, pour g de la forme $\left(\begin{smallmatrix} 1 & b\\ 0 & 1\end{smallmatrix}\right)$, avec $b\in\mathbf{Q}_p$, $\left(\begin{smallmatrix} p^k & 0\\ 0 & 1\end{smallmatrix}\right)$, avec $k\in\mathbf{Z}$, ou $\left(\begin{smallmatrix} a & 0\\ 0 & 1\end{smallmatrix}\right)$, avec $a\in\mathbf{Z}_p^*$. Si $n\in\mathbf{N}$, soient $x_n=\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)\cdot x$ et $y_n=\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)\cdot y$, de telle sorte que $\{x,y\}_{\mathbf{Q}_p}=\{x_n,y_n\}$, pour tout n assez grand.

• Si $g=\left(\begin{smallmatrix} 1 & b\\ 0 & 1\end{smallmatrix}\right)$, on a $\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)g=\left(\begin{smallmatrix} 1 & p^nb\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)$. On en déduit que

$$\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{(1+T)^{p^nb}x_n,(1+T)^{p^nb}y_n\},$$

si n est assez grand. Cette dernière quantité est égale à $\{x_n,y_n\}$ d'après la prop. II.2.1 ; on a donc bien $\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{x,y\}_{\mathbf{Q}_p}$.

• Si $g=\left(\begin{smallmatrix} p^k & 0\\ 0 & 1\end{smallmatrix}\right)$, alors $\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{x_{n+k},y_{n+k}\}$, si n est assez grand, et donc $\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{x,y\}_{\mathbf{Q}_p}$.

• si $g=\left(\begin{smallmatrix} a & 0\\ 0 & 1\end{smallmatrix}\right)$, on a $\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)g=g\left(\begin{smallmatrix} p^n & 0\\ 0 & 1\end{smallmatrix}\right)$, et donc $\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{\sigma_a(x_n),\sigma_a(y_n)\}$, si n est assez grand. Cette dernière quantité est égale à $\{x_n,y_n\}$ d'après la prop. II.2.1 ; on a donc bien $\{g\cdot x,g\cdot y\}_{\mathbf{Q}_p}=\{x,y\}_{\mathbf{Q}_p}$.

Ceci permet de conclure.

Si D est un (φ,Γ)-module étale sur $\mathscr{O}_{\mathscr{E}}$, soit $\widetilde{D}=\widetilde{\mathscr{O}}_{\mathscr{E}}\otimes_{\mathscr{O}_{\mathscr{E}}}D$. C'est un (φ,Γ)-module sur $\widetilde{\mathscr{O}}_{\mathscr{E}}$. Comme φ est bijectif sur $\widetilde{\mathscr{O}}_{\mathscr{E}}$ et D est étale sur $\mathscr{O}_{\mathscr{E}}$, l'action de φ est bijective sur $\widetilde{D}$. Un (φ,Γ)-module sur $\widetilde{\mathscr{O}}_{\mathscr{E}}$ ayant cette propriété est dit *étale*. Comme d'habitude, un (φ,Γ)-module sur $\widetilde{\mathscr{E}}$ est étale s'il possède un $\widetilde{\mathscr{O}}_{\mathscr{E}}$-réseau stable par φ et Γ qui est étale.

L'action de φ sur $\widetilde{D}$ étant bijective, cela permet de munir $\widetilde{D}$ d'une action de $P(\mathbf{Q}_p)$ en posant :

$$\left(\begin{smallmatrix} p^ka & b\\ 0 & 1\end{smallmatrix}\right)\cdot z=[(1+T)^b]\varphi^k(\sigma_a(z)),\quad \text{si } a\in\mathbf{Z}_p^*,\ b\in\mathbf{Q}_p \text{ et } k\in\mathbf{Z}.$$

Comme $\widetilde{D}$ est aussi égal à $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}\otimes_{\mathbf{A}_{\mathbf{Q}_p}}D$, il résulte de [?, prop. 8.5] que l'on a le résultat suivant :

Lemme II.4.6. — *Si $I\subset \mathbf{Q}_p$ est un système de représentants de $\mathbf{Q}_p/\mathbf{Z}_p$, tout élément z de $\widetilde{D}$ peut s'écrire, de manière unique, sous la forme*

$$z=\sum_{i\in I}[(1+T)^i]\,z_i,\quad \text{où } z_i\in D \text{ tend vers } 0 \text{ quand } i\to\infty \text{ dans } \mathbf{Q}_p.$$

Fixons un système $I\subset\mathbf{Q}_p$ de représentants de $\mathbf{Q}_p/\mathbf{Z}_p$, ce qui permet de décomposer tout élément de $\widetilde{D}$ sous la forme ci-dessus. Si $n\in\mathbf{N}$, on note I_n l'intersection de I et $p^{-n}\mathbf{Z}_p$, et donc I est la réunion croissante des I_n.

Lemme II.4.7. — *Si $z=\sum_{i\in I}[(1+T)^i]z_i\in\widetilde{D}$, alors $(\sum_{i\in I_n}[(1+T)^{p^n i}]\varphi^n(z_i))_{n\in\mathbf{N}}$ est un élément de $D\boxtimes\mathbf{Q}_p$, et l'application de $\widetilde{D}$ dans $D\boxtimes\mathbf{Q}_p$ ainsi définie ne dépend pas du choix de I et est $P(\mathbf{Q}_p)$-équivariante.*

Démonstration. — Si J est un autre système de représentants, et si $i\in I$, il existe $j(i)\in J$, unique, tel que $i-j(i)\in\mathbf{Z}_p$; de plus $j(i)\in J_n$ si $i\in I_n$, et $i\mapsto j(i)$ est une bijection de I_n sur J_n, pour tout $n\in\mathbf{N}$. On note $j\mapsto i(j)$ la bijection réciproque. Soit $z=\sum_{j\in J}[(1+T)^j]z'_j$ l'écriture de z utilisant le système de représentants J. Comme

$$\sum_{i\in I}[(1+T)^i]z_i=\sum_{i\in I}[(1+T)^{j(i)}]((1+T)^{i-j(i)}z_i),$$

l'unicité de l'écriture montre que $z'_j=(1+T)^{i(j)-j}z_{i(j)}$, et donc que $[(1+T)^i]z_i$ ne dépend que de z et de la classe de i modulo $\mathbf{Z}_p$, pas du choix de I. On en déduit que $\sum_{i\in I_n}[(1+T)^{p^n i}]\varphi^n(z_i)$ ne dépend pas du choix de I.

Maintenant, on a

$$\psi([(1+T)^{p^{n+1}i}]\varphi^{n+1}(z_i))=\begin{cases}[(1+T)^{p^n i}]\varphi^n(z), & \text{si } p^{n+1}i\in p\mathbf{Z}_p \text{ (i.e. si } i\in I_n),\\ 0, & \text{si } p^{n+1}i\in\mathbf{Z}_p^* \text{ (i.e., si } i\in I_{n+1}-I_n).\end{cases}$$

On en déduit l'appartenance de $(\sum_{i\in I_n}[(1+T)^{p^n i}]\varphi^n(z_i))_{n\in\mathbf{N}}$ à $D\boxtimes\mathbf{Q}_p$. L'injectivité de l'application ainsi définie suit de ce qu'un élément z du noyau doit vérifier $z_i=0$, pour tout i, d'après l'unicité de l'écriture, et donc est nul. Enfin, pour démontrer la $P(\mathbf{Q}_p)$-équivariance, il suffit de revenir aux formules, et de remarquer que :

- $\{ai,\ i\in I_n\}$ est un système de représentants de $p^{-n}\mathbf{Z}_p/\mathbf{Z}_p$, si $a\in\mathbf{Z}_p^*$ (équivariance de $\left(\begin{smallmatrix}a&0\\0&1\end{smallmatrix}\right)$),
- $\{a+i,\ i\in I_n\}$ est un système de représentants de $p^{-n}\mathbf{Z}_p/\mathbf{Z}_p$, si $b\in\mathbf{Q}_p$ et si n est assez grand (équivariance de $\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)$),
- $\{pi,\ i\in I_{n+1}-I_1\}\cup\{0\}$ est un système de représentants de $p^{-n}\mathbf{Z}_p/\mathbf{Z}_p$ (équivariance de $\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)$).

Le lemme II.4.7 permet d'identifier $\widetilde{D}$ à un sous-$P(\mathbf{Q}_p)$-module de $D\boxtimes\mathbf{Q}_p$, ce que nous ferons sans plus de commentaires. On remarquera que, si $z=\sum_{i\in I}[(1+T)^i]z_i\in\widetilde{D}$, alors :

- $\mathrm{Res}_{i+\mathbf{Z}_p}z=[(1+T)^i]z_i$, si $i\in I$, et $\mathrm{Res}_{p^{-n}\mathbf{Z}_p}z=\sum_{i\in I_n}[(1+T)^i]z_i$, si $n\in\mathbf{N}$,
- z est la limite des $\mathrm{Res}_{p^{-n}\mathbf{Z}_p}z$ dans $\widetilde{D}$.

Proposition II.4.8. — *Si $z \in D \boxtimes \mathbf{Q}_p$, les conditions suivantes sont équivalentes :*

(i) $z \in \widetilde{D}$;

(ii) $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z \to 0$ *dans* $D \boxtimes \mathbf{Q}_p$ *quand* $b \to \infty$ *dans* $\mathbf{Q}_p$;

(iii) $\mathrm{Res}_{\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z) \to 0$ *dans* D *quand* $b \to \infty$ *dans* $\mathbf{Q}_p$.

Démonstration. — L'implication (ii)$\Rightarrow$(iii) suit de la continuité de $\mathrm{Res}_{\mathbf{Z}_p}$. Maintenant, si (iii) est vérifiée, alors $\mathrm{Res}_{i+\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z)$, qui est égal à $[(1+T)]^i\mathrm{Res}_{\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b-i \\ 0 & 1 \end{smallmatrix}\right) \cdot z)$, tend vers 0 quand $b \to \infty$, pour tout $i \in I$. En sommant sur $i \in I_n$, on en déduit que $\mathrm{Res}_{p^{-n}\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z) \to 0$ et, ceci étant vrai pour tout n, que $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z \to 0$ dans $D \boxtimes \mathbf{Q}_p$. Ceci démontre que les propriétés (ii) et (iii) sont équivalentes.

Maintenant, si $z = \sum_{i \in I}[(1+T)^i]z_i \in \widetilde{D}$, et si $b \in \mathbf{Q}_p$, on a

$$\mathrm{Res}_{\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z) = [(1+T)^{i(-b)+b}]z_{i(-b)},$$

où $i(x)$ est l'unique élément de I vérifiant $x - i(x) \in \mathbf{Z}_p$. Comme $z_i \to 0$ quand $i \to \infty$, et comme $i(-b) \to \infty$ quand $b \to \infty$, on en déduit que $\mathrm{Res}_{\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z) \to 0$ dans D, ce qui prouve l'implication (i)$\Rightarrow$(iii). Enfin, si $\mathrm{Res}_{\mathbf{Z}_p}(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot z) \to 0$ dans D quand $b \to \infty$, alors z est la somme, dans $\widetilde{D}$, de la série $\sum_{i \in I}[(1+T)^i]\mathrm{Res}_{\mathbf{Z}_p}\big(\left(\begin{smallmatrix} 1 & -i \\ 0 & 1 \end{smallmatrix}\right) \cdot z\big)$, ce qui démontre l'implication (iii)$\Rightarrow$(i), et permet de conclure.

Corollaire II.4.9. — *$\widetilde{D}$ est le sous-module $(D \boxtimes \mathbf{Q}_p)_{\mathrm{pc}}$ de $D \boxtimes \mathbf{Q}_p$.*

Démonstration. — C'est une simple traduction de l'équivalence entre les (i) et (ii) de la proposition.

On note $\widetilde{D}^+$ (resp. $\widetilde{D}^{++}$) l'ensemble des $z \in \widetilde{D}$ tels que la suite $(\varphi^n(z))_{n \in \mathbf{N}}$ soit bornée (resp. tende vers 0) dans $\widetilde{D}$.

Lemme II.4.10. — (i) *Si $x \in \widetilde{D}^+$, alors* $\mathrm{Res}_{\mathbf{Z}_p}x \in D^\natural$.

(ii) $\widetilde{D} \cap (D^\natural \boxtimes \mathbf{Q}_p) = \widetilde{D}^+$.

(iii) $\widetilde{D}^+$ *est dense dans* $D^\natural \boxtimes \mathbf{Q}_p$.

Démonstration. — Si $x \in \widetilde{D}^+$, alors $x_n = \mathrm{Res}_{p^{-n}\mathbf{Z}_p}x \in \widetilde{D}^+ + p^k\widetilde{D}$, si n est assez grand. On en déduit que l'image y_n modulo p^k de $\varphi^n(x_n)$ appartient à $(D/p^kD)^+$, et donc que l'image modulo p^k de $\mathrm{Res}_{\mathbf{Z}_p}x$, qui n'est autre que $\psi^n(y_n)$, appartient à $(D/p^kD)^\natural$ puisque $(D/p^kD)^+ \subset (D/p^kD)^\natural$ et que $(D/p^kD)^\natural$ est stable par ψ. Ceci étant vrai pour tout k, cela démontre le (i).

Maintenant, on a $\widetilde{D}^+ \subset \widetilde{D} \cap (D^\natural \boxtimes \mathbf{Q}_p)$ d'après le (i) et la stabilité de $\widetilde{D}^+$ par $\left(\begin{smallmatrix} p^n & 0 \\ 0 & 1 \end{smallmatrix}\right)$. L'inclusion inverse suit de ce que $D^\natural \boxtimes \mathbf{Q}_p$ est compact et stable par $\left(\begin{smallmatrix} p^n & 0 \\ 0 & 1 \end{smallmatrix}\right)$, ce qui prouve que la suite des $\varphi^n(z) = \left(\begin{smallmatrix} p^n & 0 \\ 0 & 1 \end{smallmatrix}\right)z$, pour $n \in \mathbf{N}$, est bornée si $z \in \widetilde{D} \cap (D^\natural \boxtimes \mathbf{Q}_p)$. Ceci démontre le (ii).

Enfin, l'adhérence de $\widetilde{D}^+$ dans $D^\natural \boxtimes \mathbf{Q}_p$ est un sous-$P(\mathbf{Q}_p)$-module fermé de $D^\natural \boxtimes \mathbf{Q}_p$. Par ailleurs, 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 II.4.6 à $\mathscr{O}_{\mathscr{E}}$). On en déduit que $\mathscr{O}_{\mathscr{E}} \otimes_{\mathscr{O}_{\mathscr{E}}^+} \widetilde{D}^+$ est dense dans $\widetilde{D}$ qui est dense dans $D \boxtimes \mathbf{Q}_p$. Le lemme II.4.3 et le fait que $D^\natural$ est le plus petit treillis de D stable par ψ montrent que cette adhérence contient $D^\natural \boxtimes \mathbf{Q}_p$, ce qui permet de conclure.

Comme la topologie de $D^\natural \boxtimes \mathbf{Q}_p$ est induite par celle de $D \boxtimes \mathbf{Q}_p$, on déduit du (ii) du lemme II.4.10 et du cor. II.4.9 le résultat suivant.

Proposition II.4.11. — *$\widetilde{D}^+$ est le sous-module $(D^\natural \boxtimes \mathbf{Q}_p)_{\mathrm{pc}}$ de $D^\natural \boxtimes \mathbf{Q}_p$.*

III. Appendice

III.1. Vecteurs de Witt

1. Généralités sur les p-anneaux

Définition III.1.1. — *Si A est un anneau et I est un idéal de A, on dit que A est séparé et complet pour la topologie I-adique si l'application naturelle de A dans $\varprojlim (A/I^n A)$ est un isomorphisme. La topologie I-adique sur A est alors celle qui fait de l'isomorphisme précédent un isomorphisme d'anneaux topologiques, $\varprojlim (A/I^n A)$ étant muni de la topologie produit, chacun des $A/I^n A$ étant muni de la topologie discrète.*

Lemme III.1.2. — (i) *Si K est un corps complet pour une valuation v, et si $\pi \in K$ vérifie $v(\pi) > 0$, alors $\mathscr{O}_K$ est séparé et complet pour la topologie π-adique.*

(ii) *Si A est un anneau, si $\pi \in A$, si S est un et S est un système de représentants de $A/\pi A$ dans A, et si A est séparé et complet pour la topologie π-adique, alors tout élément de A peut s'écrire de manière unique sous la forme $\sum_{n=0}^{+\infty} s_n \pi^n$ avec $s_n \in S$.*

Démonstration. — (i) On note $\iota : \mathscr{O}_K \to \varprojlim (\mathscr{O}_K/\pi^n \mathscr{O}_K)$ l'application qui, à $x \in \mathscr{O}_K$, associe la suite des images de x modulo π^n. On a alors

- $\iota(x) = 0 \Leftrightarrow v(x) \geqslant nv(\pi)$ quel que soit $n \in \mathbf{N} \Leftrightarrow v(x) = +\infty \Leftrightarrow x = 0$, ce qui montre que ι est injective.
- Si $(x_n)_{n\in\mathbf{N}} \in \varprojlim (\mathscr{O}_K/\pi^n \mathscr{O}_K)$ et si $\hat{x}_n \in \mathscr{O}_K$ est un relêvement quelconque de x_n, alors $v(\hat{x}_{n+k} - \hat{x}_n) \geqslant nv(\pi)$ quels que soient $n, k \in \mathbf{N}$. Ceci montre que la suite $\hat{x}_n$ est de Cauchy, et sa limite x veŕifie $v(x - \hat{x}_n) \geqslant nv(\pi)$ quel que soit $n \in \mathbf{N}$. On en déduit que $\iota(x) = (x_n)_{n\in\mathbf{N}}$, ce qui prouve la surjectivité de ι.
- « $v(x - y) \geqslant nv(\pi)$ » $\Leftrightarrow$ « $x = y$ dans $\mathscr{O}_K/\pi^k \mathscr{O}_K$, quel que soit $i \leqslant n$ », ce qui montre que la topologie induite par v sur $\mathscr{O}_K$ correspond à la topologie produit sur $\varprojlim (\mathscr{O}_K/\pi^n \mathscr{O}_K)$, chaque $\mathscr{O}_K/\pi^n \mathscr{O}_K$ étant muni de la topologie discrète.

(ii) Soit $s : A \to S$ l'application qui à x associe l'unique élément $s(x)$ de S vérifiant $x - s(x) \in \pi A$. Si $x \in A$, on définit par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de A en posant $x_0 = x$ et, si $n \geqslant 1$, $x_n = \frac{1}{\pi}(x_{n-1} - s(x_{n-1}))$. On a alors $x = \sum_{i=0}^{n} s(x_i)\pi^i + \pi^{n+1} x_{n+1}$ quel que soit $n \in \mathbf{N}$, et donc $x = \sum_{n=0}^{+\infty} s(x_n)\pi^n$ ce qui prouve l'existence d'une écriture sous la forme mentionnée plus haut. D'autre part, si $\sum_{n=0}^{+\infty} s_n \pi^n = \sum_{n=0}^{+\infty} s'_n \pi^n$, alors réduisant modulo π, on obtient $s_0 = s'_0$ et une récurrence immédiate nous montre que $s_n = s'_n$ quel que soit $n \in \mathbf{N}$ d'où l'unicité de l'écriture.

Définition III.1.3. — *Un anneau R de caractéristique p est parfait si l'élévation à la puissance p est un isomorphisme. (Si R est un corps on retombe sur la définition usuelle.) Si R est un anneau parfait de caractéristique p, un idéal $\mathfrak{n}$ de R est parfait s'il est stable par extraction de racines p-ième, ce qui équivaut à ce que $R/\mathfrak{n}$ soit parfait.*

Définition III.1.4. — *Soient A un anneau et R un anneau de caractéristique p. On dit que A est un p-anneau d'anneau résiduel R s'il existe $\pi \in A$ tel que A soit séparé et complet pour la topologie π-adique et $R = A/\pi A$. Comme R est de caractéristique p, on a en particulier $p \in \pi A$. Un p-anneau est dit strict si $\pi = p$ et p n'est pas nilpotent dans A, et parfait s'il est strict et R est parfait.*

Exemple III.1.5. — (i) $\mathbf{Z}_p$ est un p-anneau parfait, car $\mathbf{F}_p$ est un corps parfait.

(ii) Si J est un ensemble quelconque, soit $W_J = \mathbf{Z}_p[X_j^{p^{-\infty}},\ j \in J] = \cup_{m\in\mathbf{N}}\mathbf{Z}_p[X_j^{p^{-m}},\ j \in J]$. On note $\widehat{W}_J$ le séparé complété de W_J pour la topologie p-adique (i.e $\widehat{W}_J = \varprojlim W_J/p^n W_J$), ce qui fait de $\widehat{W}_J$ un p-anneau strict d'anneau résiduel $\overline{W}_J = \mathbf{F}_p[X_j^{p^{-\infty}},\ j \in J]$ qui est parfait (on s'est clairement débrouillé pour).

Remarque III.1.6. — Soit R un anneau parfait de caractéristique p. Le morphisme naturel de $\overline{W}_R$ dans R qui à $X_x \in \overline{W}_R$ associe x est surjectif, ce qui permet de voir tout anneau parfait comme un quotient d'un anneau du type $\overline{W}_J$ par un idéal parfait. Ceci permet de ramener beaucoup de questions concernant les anneaux parfaits de caractéristique p au cas des anneaux du type $\overline{W}_J$.

Proposition III.1.7. — *Si A est un p-anneau d'anneau résiduel R et si $x \in A$, les deux conditions suivantes sont équivalentes :*

(i) x est inversible dans A ;

(ii) l'image $\overline{x}$ de x modulo π est inversible dans R.

Démonstration. — Si y est un inverse de x dans A, alors $\overline{y}$ est un inverse de $\overline{x}$ dans R. Réciproquement, si $\overline{y}$ est un inverse de $\overline{x}$ dans R, et si y est n'importe quel relèvement de $\overline{y}$ dans A, alors $z = 1 - xy \in \pi A$ et x admet comme inverse $y(\sum_{n=0}^{+\infty} z^n)$.

Corollaire III.1.8. — *Si A est un p-anneau strict dont l'anneau résiduel est un corps, alors $B = A[\frac{1}{p}]$ est un corps.*

Démonstration. — Si $x \in B - \{0\}$, il existe un unique entier $n \in \mathbf{Z}$ tel que $p^n x \in A - pA$ et la proposition précédente montre que $p^n x$ est inversible dans A, ce qui permet de conclure.

2. Représentants de Teichmüller. — Si A est un anneau, on note $\mathbb{R}(A)$ l'ensemble des suites $x = (x^{(n)})_{n\in\mathbf{N}}$ d'éléments de A telles que l'on ait $(x^{(n+1)})^p = x^{(n)}$ quel que soit $n \in \mathbf{N}$. Dans tout ce qui suit, A est un p-anneau.

Lemme III.1.9. — *Si x, y sont deux éléments de A vérifiant $x - y \in \pi A$, alors $x^{p^n} - y^{p^n} \in \pi^{n+1}A$ quel que soit $n \in \mathbf{N}$.*

Démonstration. — La formule du binôme montre que si $a \in A$ et $u \in \pi^n A$, alors $(a+u)^p - a^p \in \pi^{n+1}A$; on en déduit par récurrence sur n, le fait que si $a \in A$ et $u \in \pi A$, alors $(a+u)^{p^n} - a^{p^n} \in \pi^{n+1}A$, ce qui, appliqué à $a = x$ et $u = y - x$, permet de conclure.

Corollaire III.1.10. — *Si $x = (x^{(n)})_{n\in\mathbf{N}} \in \mathbb{R}(R)$ et $\tilde{x}^{(n)}$ est un relèvement de $x^{(n)}$, alors la suite de terme général $(\tilde{x}^{(n+m)})^{p^m}$ converge dans A vers une limite $\psi_A^{(n)}(x)$ qui ne dépend que de x et $\psi_A(x) = (\psi_A^{(n)}(x))_{n\in\mathbf{N}} \in \mathbb{R}(A)$. De plus, on a $\psi_A(xy) = \psi_A(x)\psi_A(y)$.*

Démonstration. — Par construction, $(\tilde{x}^{(n+m+1)})^p - \tilde{x}^{(n+m)} \in \pi A$, et donc $(\tilde{x}^{(n+m+1)})^{p^{m+1}} - (\tilde{x}^{(n+m)})^{p^m} \in \pi^{m+1}A$, ce qui montre que la suite de terme général $(\tilde{x}^{(n+m)})^{p^m}$ converge dans A. Le fait que la limite ne dépende pas du choix des $\tilde{x}^{(n)}$ suit du fait que si on a deux choix, on en fabrique un troisième en panachant et que les trois limites sont égales. On démontre que $(\psi_A^{(n+1)}(x))^p = \psi_A^{(n)}(x)$ par passage à la limite, ce qui prouve que $\psi_A(x) = (\psi_A^{(n)}(x))_{n\in\mathbf{N}} \in \mathbb{R}(A)$. Finalement, la multiplicativité de ψ_A suit de ce que l'on peut prendre $\tilde{x}^{(n)}\tilde{y}^{(n)}$ comme relèvement de $(xy)^{(n)}$ dans A.

Remarque III.1.11. — Si R est parfait, l'application qui à $x = (x^{(n)})_{n\in\mathbf{N}}$ associe $x^{(0)}$ est une bijection de $\mathbb{R}(R)$ sur R et l'application qui à $x \in R$ associe $[x] = \psi_A^{(0)}(x)$, (où x est considéré comme un élément de $\mathbb{R}(R)$) est multiplicative (i.e. $[xy] = [x][y]$ si $x, y \in R$) et l'image de $[x]$ dans $R = A/\pi A$ est x.

Définition III.1.12. — *L'élément $[x]$ de A est le représentant de Teichmüller de x dans A.*

Exercice 1. — (i) Montrer que, si A est de caractéristique p, alors $[x+y] = [x]+[y]$ quels que soient $x, y \in R$.

(ii) Montrer que, si F est un corps local de caractéristique p, et si k_F est parfait, alors $F \cong k_F((T))$.

3. L'anneau des vecteurs de Witt d'un anneau parfait de caractéristique p. — On a vu que l'on pouvait écrire tout élément de $\mathbf{Z}_p$ de manière unique sous la forme $\sum_{i=0}^{+\infty} p^i\omega_i$, où les ω_i sont des représentants de Teichmüller d'éléments de $\mathbf{F}_p$ (i.e. des racines de l'équation $X^p - X = 0$). On peut se demander s'il est possible de décrire les lois d'addition et multiplication en utilisant cette écriture. C'est le cas et cela va nous mener à introduire les vecteurs de Witt.

Théorème III.1.13. — *Si R est un anneau parfait de caractéristique p, il existe un p-anneau strict* $W(R)$ (anneau des vecteurs de Witt à coefficients dans R), *unique à isomorphisme unique près, dont l'anneau résiduel est R.*

De plus, $W(R)$ vérifie la propriété universelle suivante. Si A est un p-anneau d'anneau résiduel R', si $\overline{\theta} : R \to R'$ un morphisme d'anneaux, et si $\tilde{\theta} : R \to A$ est une application multiplicative relevant $\overline{\theta}$, il existe un unique morphisme d'anneau $\theta : W(R) \to A$ tel que si $x \in R$, alors $\theta([x]) = \tilde{\theta}(x)$.

Proposition III.1.14. — *Si A est un p-anneau parfait d'anneau résiduel R, alors tout élément de A s'écrit de manière unique sous la forme $\sum_{i=0}^{+\infty} p^i[x_i]$, où les x_i sont des éléments de R.*

Démonstration. — C'est vrai pour tout système de représentants de R dans A (lemme III.1.2).

Lemme III.1.15. — *Soit J un ensemble d'indices. Si A est un p-anneau d'anneau résiduel R, si $\overline{\theta} : \overline{W}_J \to R$ un morphisme d'anneaux, et si $\tilde{\theta} : \overline{W}_J \to A$ est une application multiplicative relevant $\overline{\theta}$, il existe un unique morphisme d'anneau $\theta : \widehat{W}_J \to A$ tel que si $x \in \overline{W}_J$, alors $\theta([x]) = \tilde{\theta}(x)$.*

Démonstration. — L'unicité est claire : on doit avoir $\theta(\sum_{i=0}^{+\infty} p^i[x_i]) = \sum_{i=0}^{+\infty} p^i\tilde{\theta}(x_i)$. Montrons l'existence. Soit $f : W_J \to A$ le morphisme d'anneaux défini par $f(X_j^{p^{-m}}) = \tilde{\theta}(X_j^{p^{-m}})$ si $j \in J$ et $m \in \mathbf{N}$. On prolonge f par continuité en un morphisme $\hat{f} : \widehat{W}_J \to A$ et pour conclure, il suffit de prouver que si $x \in \overline{W}_J$, alors $\hat{f}([x]) = \tilde{\theta}(x)$. Le morphisme $\overline{f} : \overline{W}_J \to R$ induit par $\hat{f}$ coïncide par construction avec $\overline{\theta}$ sur $X_j^{p^{-m}}$ si $j \in J$ et $m \in \mathbf{N}$ et comme ces éléments engendrent $\overline{W}_J$, on en déduit l'égalité de $\overline{f}$ et $\overline{\theta}$. Ceci implique en particulier que si $x \in \overline{W}_J$ et $n \in \mathbf{N}$, alors $\hat{f}([x^{p^{-n}}]) - \tilde{\theta}(x^{p^{-n}}) \in \pi A$ et donc, d'après le lemme III.1.9, que $\hat{f}([x]) - \tilde{\theta}(x) \in \pi^{n+1}A$ quel que soit $n \in \mathbf{N}$, et permet de conclure.

Soit $\mathbf{N} \amalg \mathbf{N}$ la réunion disjointe de deux copies de $\mathbf{N}$. Pour alléger un peu les notations, notons X_i et Y_i au lieu de $X_{1,i}$ et $X_{2,i}$ les variables de $W_{\mathbf{N}\amalg\mathbf{N}}$ Un élément $P(X, Y)$ de $\overline{W}_{\mathbf{N}\amalg\mathbf{N}}$ peut s'écrire de manière unique sous la forme

$$P(X,Y) = \sum_{\mathbf{r},\mathbf{s}} a_{\mathbf{r},\mathbf{s}}\Big(\prod_{i=0}^{+\infty} X_i^{r_i}\Big)\Big(\prod_{j=0}^{+\infty} Y_j^{s_j}\Big),$$

la somme portant sur les couples $(\mathbf{r}, \mathbf{s})$ de familles d'éléments de $\mathbf{Z}[\frac{1}{p}]$ n'ayant qu'un nombre fini de termes non nuls et les $a_{\mathbf{r},\mathbf{s}}$ étant des éléments de $\mathbf{F}_p$ presque tous nuls.

Soient $(S_i(X,Y))_{i\in\mathbf{N}}$ et $(P_i(X,Y))_{i\in\mathbf{N}}$ les suites d'éléments de $\overline{W}_{\mathbf{N}\amalg\mathbf{N}}$ définie par

$$\sum_{i=0}^{+\infty} p^i[X_i] + \sum_{i=0}^{+\infty} p^i[Y_i] = \sum_{i=0}^{+\infty} p^i[S_i(X,Y)] \quad \text{et} \quad \Big(\sum_{i=0}^{+\infty} p^i[X_i]\Big)\Big(\sum_{i=0}^{+\infty} p^i[Y_i]\Big) = \sum_{i=0}^{+\infty} p^i[P_i(X,Y)].$$

Les polynômes S_i et P_i sont des polynômes universels permettant de décrire les lois d'addition et multiplication dans un p-anneau parfait si on écrit les éléments sous la forme $\sum_{i=0}^{+\infty} p^i[x_i]$, où les x_i sont des éléments de l'anneau résiduel. De manière précise, on a la proposition suivante.

Proposition III.1.16. — *Si A est un p-anneau parfait d'anneau résiduel R, et si $x = (x_i)_{i\in\mathbf{N}}$ est une suite d'éléments de R, on note $\Sigma(x)$ l'élément $\sum_{i=0}^{+\infty} p^i[x_i]$ de A.*

Si $x = (x_i)_{i\in\mathbf{N}}$ et $y = (y_i)_{i\in\mathbf{N}}$ sont deux suites d'éléments de R, alors

$$\Sigma(x) + \Sigma(y) = \sum_{i=1}^{+\infty} p^i[S_i(x,y)] \quad \text{et} \quad \Sigma(x)\Sigma(y) = \sum_{i=1}^{+\infty} p^i[P_i(x,y)].$$

Démonstration. — Soit $\overline{\theta} : \overline{W}_{\mathbf{N}\amalg\mathbf{N}} \to R$ le morphisme défini par $\overline{\theta}(X_i) = x_i$ et $\overline{\theta}(Y_i) = y_i$ si $i \in \mathbf{N}$. Soit $\tilde{\theta} : \overline{W}_{\mathbf{N}\amalg\mathbf{N}} \to A$ l'application multiplicative définie par $\tilde{\theta}(x) = [\overline{\theta}(x)]$. D'après le lemme III.1.15, il existe une unique morphisme $\theta : \widehat{W}_J \to A$ tel que l'on ait $\theta([z]) = [\overline{\theta}(z)]$ quel que soit $z \in \overline{W}_{\mathbf{N}\amalg\mathbf{N}}$. Soient alors $X = (X_i)_i$ et $Y = (Y_i)_{i\in I}$ les deux suites naturelles d'éléments de $W_{\mathbf{N}\amalg\mathbf{N}}$. On a par construction $\Sigma(x) = \theta(\Sigma(X))$ et $\Sigma(y) = \theta(\Sigma(Y))$, ce qui nous donne les formules

$$\begin{aligned}\Sigma(x)+\Sigma(y) =&\theta(\Sigma(X))+\theta(\Sigma(Y)) = \theta(\Sigma(X)+\Sigma(Y))\\ =&\theta(\sum_{i=0}^{+\infty} p^i[S_i(X,Y)]) = \sum_{i=0}^{+\infty} p^i[\overline{\theta}(S_i(X,Y))] = \sum_{i=0}^{+\infty} p^i[S_i(x,y)],\end{aligned}$$

ce qui donne le résultat pour la somme ; le produit se traitant exactement de la même manière, cela permet de conclure.

Remarque III.1.17. — (i) La proposition III.1.14 décrit un anneau parfait d'anneau résiduel R de manière ensembliste, en fonction de R, et la prop. III.1.16 montre qu'il existe au plus une structure de p-anneau strict sur cet ensemble, qui fasse de R l'anneau résiduel. On en déduit l'unicité de $W(R)$.

(ii) Du fait de la distributivité de la multiplication par rapport à l'addition et de la continuité de l'addition, pour être capable de multiplier, additionner ou soustraire deux éléments de la forme $\Sigma(x)$ et $\Sigma(y)$, il suffit d'avoir une formule pour $[X]-[Y]$.

(iii) Comme $\Sigma(0) = 0$, on a $\Sigma(x)+\Sigma(y) = 0$, si $x = 0$ et $y = 0$; cela implique que les S_i, $i \in \mathbf{N}$, n'ont pas de terme constant. De même, $\Sigma(x)\Sigma(y) = 0$ si $x = 0$ ou $y = 0$, cela implique que les P_i n'ont pas de termes de degré 0 en les X_j ou en les Y_j.

Exercice 2. — Montrer que, si $i \in \mathbf{N}$, alors S_i (resp. P_i) est un polynôme homogène de degré 1 (resp. de degré 2) en $X_0,\dots,X_i,Y_0,\dots,Y_i$.

Lemme III.1.18. — *Soit A un p-anneau strict d'anneau résiduel R parfait et $\mathfrak{n}$ un idéal parfait de R distinct de R, l'ensemble $W(\mathfrak{n}) = \{\sum_{i=0}^{+\infty} p^i[x_i] \mid x_i \in \mathfrak{n}$ quel que soit $i \in \mathbf{N}\}$ est un idéal fermé de A et $A/W(\mathfrak{n})$ est un p-anneau parfait d'anneau résiduel $R/\mathfrak{n}$.*

Démonstration. — On déduit de la prop III.1.16 que $W(\mathfrak{n})$ est un sous-groupe additif de A, et qu'il est stable par multiplication par un élément de A car $v_X(P_i) = v_Y(P_i) > 0$ (rem. III.1.17). Par ailleurs, $W(\mathfrak{n})$ est fermé par construction, et l'anneau résiduel de $A/W(\mathfrak{n})$ est $A/W(\mathfrak{n})+pA = R/\mathfrak{n}$, ce qui termine la démonstration.

Revenons à la démonstration du théorème III.1.13. L'unicité a déjà été démontrée au (i) de la rem. III.1.17. Si R est parfait de caractéristique p, on peut l'écrire (de manière non unique) comme un quotient d'un $\overline{W}_J$ par un idéal parfait $\mathfrak{n}$. Le lemme précédent montre que $W(R) = \widehat{W}_J/W(\mathfrak{n})$ est un p-anneau parfait d'anneau résiduel R.

Il reste à prouver que $W(R)$ satisfait la propriété universelle demandée, mais cela se déduit du lemme III.1.15 en composant tout avec la projection de $\overline{W}_J$ sur R et en remarquant que le morphisme de $\widehat{W}_J$ dans A que l'on obtient se factorise à travers $W(R)$.

Exemple III.1.19. — (i) $W(\mathbf{F}_p) = \mathbf{Z}_p$.

(ii) Plus généralement, si K est un corps local de caractéristique 0 dont le corps résiduel k_K est parfait de caractéristique p, et dont p est une uniformisante, alors $K \cong W(k_K)[\frac{1}{p}]$.

Démonstration. — l'anneau des entiers de K est un p-anneau parfait d'anneau résiduel k_K, donc isomorphe à $W(k_K)$.

Exercice 3. — On définit par récurrence sur n, une suite $(U_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{Z}[\frac{1}{p}][X,Y]$, en posant

$$U_n(X,Y) = \frac{1}{p^n}\Big(X^{p^n} + Y^{p^n} - \Big(\sum_{i=0}^{n-1} p^i U_i(X,Y)^{p^{n-i}}\Big)\Big).$$

(i) Calculer U_0 et U_1 et vérifier que $U_0, U_1 \in \mathbf{Z}[X,Y]$.
(ii) On se place dans l'anneau $S_{X,Y} = \widehat{\mathbf{Z}[X^{p^{-\infty}}, Y^{p^{-\infty}}]}$ et on écrit $X+Y$ sous la forme

$$X+Y = \sum_{i=0}^{+\infty} p^i[V_i(X,Y)], \quad \text{avec } V_i \in \mathbf{F}_p[X^{p^{-\infty}}, Y^{p^{-\infty}}].$$

(a) Montrer que $X^{p^n} + Y^{p^n} = \sum_{i=0}^{+\infty} p^i[V_i(X,Y)^{p^n}]$.

(b) On suppose que, quel que soit $i \leqslant n-1$, $U_i \in \mathbf{Z}[X,Y]$ et que l'image $\overline{U}_i$ de U_i dans $\mathbf{F}_p[X,Y]$ vérifie $\overline{U}_i = V_i^{p^i}$. Montrer que

$$\sum_{i=0}^{n-1} p^i U_i(X,Y)^{p^{n-i}} \equiv \sum_{i=0}^{n-1} p^i[V_i(X,Y)^{p^n}] \mod p^{n+1}.$$

En déduire que $U_n \in \mathbf{Z}[X,Y]$ et que $\overline{U}_n = V_n^{p^n}$.
(iii) Montrer que V_n est un polynôme en $X^{p^{-n}}$ et $Y^{p^{-n}}$, puis que S_n et P_n, donnant l'addition et la multiplication des vecteurs de Witt, sont des polynômes en les $X_j^{p^{j-n}}, Y_j^{p^{j-n}}$, avec $j \leqslant n$.

Proposition III.1.20. — *Si R et R' sont deux anneaux parfaits de caractéristique p, l'application naturelle de* $\mathrm{Hom}(W(R), W(R'))$ *dans* $\mathrm{Hom}(R,R')$ *est une bijection.*

En particulier, le morphisme de Frobenius $x \to x^p$ sur R se relève en un automorphisme φ (de Frobenius) de $W(R)$.

Démonstration. — Si $\overline{\theta}$ est un morphisme de R dans R', on pose $\tilde{\theta}(x) = [\overline{\theta}(x)]$ et $\tilde{\theta}$ est une application multiplicative de R dans $W(R')$ relevant $\overline{\theta}$; on en déduit, utilisant la seconde partie du théorème, la surjectivité de l'application naturelle de $\mathrm{Hom}(W(R), W(R'))$ dans $\mathrm{Hom}(R,R')$.

Si θ est un morphisme de $W(R)$ dans $W(R')$, on a $\theta([x]) = \lim_{n\to+\infty} = \theta([x^{p^{-n}}])^{p^n} = [\overline{\theta}(x)]$ d'après le corollaire III.1.10 (et la remarque III.1.11), puisque $\theta([x^{p^{-n}}])$ est un relèvement dans $W(R')$ de $\overline{\theta}(x^{p^{-n}}) = (\overline{\theta}(x))^{p^{-n}}$, et l'injectivité suit de ce que $W(R)$ étant un p-anneau strict, la connaissance de $\theta([x])$ pour tout $x \in R$ est équivalente à la connaissance de θ d'après la proposition III.1.14.

Exercice 4. — Soit k un corps algébriquement clos de caractéristique p.

(i) Montrer que $\varphi - 1 : W(k) \to W(k)$ est surjectif. Quel est son noyau ?

(ii) Montrer que, si $u \in W(k)^*$, alors il existe $x \in W(k)^*$ tel que $\frac{\varphi(x)}{x} = u$.

Pierre Colmez, Institut de mathématiques de Jussieu, 4 place Jussieu, 75005 Paris, France
E-mail : colmez@math.jussieu.fr