DISTRIBUTIONS ET FONCTIONS ANALYTIQUES, NOTES DU COURS DE M2

par

Pierre Colmez

Table des matières

1. Fonctions analytiques

Dans tout ce qui suit, L est un sous-corps fermé de $\mathbf{C}_p$. L'application naturelle du groupe $\mathrm{Aut}_{\mathrm{cont}}(\mathbf{C}_p)$ des automorphismes continus (de corps) de $\mathbf{C}_p$ dans $\mathrm{G}_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ est un isomorphisme de groupes (l'injectivité suit de la densité de $\overline{\mathbf{Q}}_p$ dans $\mathbf{C}_p$, et la surjectivité, de ce qu'un élément de $\mathrm{G}_{\mathbf{Q}_p}$ agit par une isométrie sur $\overline{\mathbf{Q}}_p$ et donc s'étend par continuité à $\mathbf{C}_p$). Si on note G_L le sous-groupe de $\mathrm{Aut}_{\mathrm{cont}}(\mathbf{C}_p)$ des éléments fixant L, alors G_L est un sous-groupe fermé de $\mathrm{G}_{\mathbf{Q}_p}$ via l'identification précédente.

Par ailleurs, L contient $\mathbf{Q}_p$ et, comme $\mathbf{C}_p$ est algébriquement clos il contient une clôture algébrique $\overline{L}$ de L qui, elle-même, contient $\overline{\mathbf{Q}}_p$. En particulier, $\mathbf{C}_p$ est aussi le complété de la clôture algébrique de L, ce qui fait que, d'après le théorème d'Ax-Sen-Tate, G_L s'identifie à $\mathrm{Gal}(\overline{L}/L)$ et $\mathbf{C}_p^{\mathrm{G}_L} = L$. Comme $\mathbf{C}_p^{\mathrm{G}_L}$ est aussi, d'après le théorème d'Ax-Sen-Tate, le complété de $\overline{\mathbf{Q}}_p^{\mathrm{G}_L}$, cela permet de montrer le résultat suivant qui aurait plus sa place dans le chapitre "Les nombres p-adiques".

Proposition 1.1. — *Si L est un sous-corps fermé de $\mathbf{C}_p$, et si G_L est le sous-groupe de* $\mathrm{Aut}_{\mathrm{cont}}(\mathbf{C}_p)$ *des éléments fixant L, alors $L = \mathbf{C}_p^{\mathrm{G}_L}$ et $L \cap \overline{\mathbf{Q}}_p$ est dense dans L.*

1.1. Séries entières

1.1.1. Valuation de convergence raffinée d'une série entière. — Soit $\widetilde{\mathbf{R}} = \mathbf{R} \cup (\mathbf{R} \times \{-,+\}) \cup \{-\infty, +\infty\}$. Si $r \in \mathbf{R}$, on note simplement r^- [resp. r^+] l'élément $(r,-)$ [resp. $(r,+)$] de $\widetilde{\mathbf{R}}$. On munit $\widetilde{\mathbf{R}}$ de la relation d'ordre totale évidente définie par

(i) $-\infty \leqslant x$ et $x \leqslant +\infty$ quel que soit $x \in \widetilde{\mathbf{R}}$;

(ii) $r^- < r < r^+$ si $r \in \mathbf{R}$;

(iii) $r^+ < s^-$ si $r, s \in \mathbf{R}$ vérifient $r < s$.

Finalement, si $x \in \widetilde{\mathbf{R}}$, on définit $-x \in \widetilde{\mathbf{R}}$ de la manière habituelle si $x \in \mathbf{R}$ et par

$$-(-\infty) = +\infty \text{ et } -(+\infty) = -\infty; \quad -(r^-) = (-r)^+ \text{ et } -(r^+) = (-r)^- \text{ si } r \in \mathbf{R}.$$

Si $(x_k)_{k\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{R}$, on note $\operatorname{linf} x_k \in \mathbf{R} \cup \{-\infty, +\infty\}$ la limite inférieure de la suite $(x_k)_{k\in\mathbf{N}}$ et on définit la *limite inférieure raffinée* $\operatorname{linf}' x_k \in \widetilde{\mathbf{R}}$ de la suite $(x_k)_{k\in\mathbf{N}}$, par la formule

$$\operatorname{linf}' x_k = \begin{cases} -\infty & \text{si } \operatorname{linf} x_k = -\infty, \\ r^- & \text{si } \operatorname{linf} x_k = r \text{ et } \operatorname{linf} k\cdot(x_k - r) = -\infty, \\ r & \text{si } \operatorname{linf} x_k = r \text{ et } \operatorname{linf} k\cdot(x_k - r) \in \mathbf{R}, \\ r^+ & \text{si } \operatorname{linf} x_k = r \text{ et } \lim k\cdot(x_k - r) = +\infty, \\ +\infty & \text{si } \lim x_k = +\infty, \end{cases}$$

Si $f = \sum_{k=0}^{+\infty} a_k T^k \in L[[T]]$, on définit la *valuation de convergence* $\mathrm{Val}(f) \in \widetilde{\mathbf{R}}$ et la *valuation de convergence raffinée* $\mathrm{Val}'(f) \in \widetilde{\mathbf{R}}$ par les formules

$$\mathrm{Val}(f) = -\Big(\operatorname{linf} \frac{v_p(a_k)}{k}\Big) \quad \text{et} \quad \mathrm{Val}'(f) = -\Big(\operatorname{linf}' \frac{v_p(a_k)}{k}\Big).$$

Proposition 1.2. — *Si $f \in L[[T]]$, alors $f(T)$ converge si $v_p(T) > \mathrm{Val}(f)$ et $f(T)$ diverge si $v_p(T) < \mathrm{Val}(f)$. Plus précisément,*

$$\mathrm{Val}'(f) = \begin{cases} -\infty & \Leftrightarrow f \text{ est analytique sur } \mathbf{C}_p \text{ tout entier,} \\ r^- & \Leftrightarrow f \text{ est analytique sur } D(0,r) \text{ et ne converge pas si } v_p(T) < r, \\ r & \Leftrightarrow f \text{ est analytique bornée sur } D(0,r^+) \text{ et ne converge pas si } v_p(T) \leqslant r, \\ r^+ & \Leftrightarrow f \text{ est analytique non bornée sur } D(0,r^+) \text{ et ne converge pas si } v_p(T) \leqslant r, \\ +\infty & \Leftrightarrow f \text{ ne converge que pour } T = 0. \end{cases}$$

Démonstration. — Exercice

1.1.2. Le polygone de Newton d'une série entière. — Si $f = \sum_{k\in\mathbf{N}} a_k T^k \in L[[T]]$, soit $\mathrm{Newt}_f : \mathbf{R}_+ \to \mathbf{R} \cup \{\pm\infty\}$ la plus grande fonction convexe vérifiant $\mathrm{Newt}_f(k) \leqslant v_p(a_k)$ quel que soit $k \in \mathbf{N}$. Comme dans le cas d'un polynôme, cette fonction est affine par morceaux (et même affine sur chaque segment de la forme $[k, k+1]$, où $k \in \mathbf{N}$) et vaut $+\infty$ sur le segment $[0, v_T(f)]$; son graphe est *le polygone de Newton* de f, une *pente du polygone de Newton* est une valeur prise par la dérivée λ_f de Newt_f (qui est une fonction croissante puisque Newt_f est convexe). Par rapport au cas des polynômes, il peut se passer plusieurs phénomènes nouveaux.

• La fonction Newt_f peut ne prendre aucune valeur finie (même si $f \neq 0$) par exemple, si $f = \sum_{k=1}^{+\infty} p^{-k^2} T^k$, la fonction $\mathrm{Newt}_f(x)$ vaut $+\infty$ sur $[0,1[$ et $-\infty$ sur $[1,+\infty[$.

• Le polygone de Newton peut posséder une infinité de pentes : par exemple, si $f = \sum_{n=1}^{+\infty} p^{-n} T^{\frac{n(n+1)}{2}}$, la fonction $\mathrm{Newt}_f(x)$ vaut $-n - \frac{1}{n+1}(x - \frac{n(n+1)}{2})$ sur $[\frac{n(n+1)}{2}, \frac{(n+1)(n+2)}{2}]$ et la fonction λ_f prend donc les valeurs $-1, -\frac{1}{2}, -\frac{1}{3}, \dots$. Autre exemple, la fonction $\sum_{k=0}^{+\infty} p^{k^2} T^k$ dont les pentes sont $1, 3, 5, 7, \dots$ et tendent vers $+\infty$.

• Si le polygone de Newton ne possède qu'un nombre fini de pentes, alors le dernier « segment » est une demi-droite. Si cette demi-droite ne contient qu'un nombre fini de points de la forme $(k, v_p(a_k))$, on rajoute le dernier de ces points aux *sommets du polygone de Newton*, i.e. aux points de la forme $(k, v_p(a_k))$ appartenant au polygone de Newton en lesquels les dérivées à gauche et à droite ne sont pas les mêmes.

Proposition 1.3. — *La valuation de convergence de f est l'opposé de la limite de la fonction λ_f en $+\infty$.*

Démonstration. — Exercice

Exercice 1. — (i) Montrer que les sommets du polygone de Newton de $\log(1+T)$ sont les $(p^n, -n)$, pour $n \in \mathbf{N}$. Calculer ses pentes.

(ii) Montrer que le polygone de Newton de $\exp T$ est la droite $y = -\frac{x}{p-1}$.

1.1.3. Le théorème de préparation de Weierstrass. — Soit $L\{T\} = \mathrm{A}(D(0,0), L)$ l'anneau des séries convergeant sur la boule $\{v_p(x) \geqslant 0\}$; c'est aussi l'ensemble des séries $f = \sum_{k=0}^{+\infty} a_k T^k$ vérifiant $\lim_{k\to+\infty} v_p(a_k) = +\infty$; on l'obtient en complétant $L[T]$ pour la valuation de Gauss que l'on notera $v^{[0]}$ au lieu de v_G. On a aussi $v^{[0]} = v_{D(0,0)}$.

Proposition 1.4. — (Continuité de la division euclidienne) *Si $P \in \mathscr{O}_L[T]$ est un polynôme unitaire, alors tout élément f de $L\{T\}$ peut s'écrire de manière unique sous la forme $f = Pq(f) + r(f)$, où $q(f) \in L\{T\}$ et $r(f) \in L[T]$ est de degré $\leqslant \deg P - 1$. De plus, $v^{[0]}(q(f)) \geqslant v^{[0]}(f)$ et*

$v^{[0]}(r(f)) \geqslant v^{[0]}(f)$. (Le polynôme $r(f)$ est le *reste de la division euclidienne* de f par P, et $q(f)$ est le *quotient de la division euclidienne* de f par P.)

Démonstration. — Pour démontrer l'unicité, il suffit de vérifier que l'application $(g, R) \to Pg+R$ est injective et donc que si $Pg = -R$, alors $g = R = 0$. Or P, étant unitaire à coefficients entiers, a $\deg P$ zéros appartenant à la boule $\{v_p(x) \geqslant 0\}$, alors que R en a au plus $\deg P - 1$ s'il n'est pas nul ; ceci permet de conclure.

Pour démontrer l'existence, constatons que P étant unitaire à coefficients dans $\mathscr{O}_L$, le reste $r(Q)$ et le quotient $q(Q)$ de la division euclidienne d'un polynôme $Q \in \mathscr{O}_L[T]$ par P appartiennent aussi $\mathscr{O}_L[T]$; les applications r et q de $L[T]$ dans $L[T]$ vérifient donc $v^{[0]}(r(Q)) \geqslant v^{[0]}(Q)$ et $v^{[0]}(q(Q)) \geqslant v^{[0]}(Q)$, et elles s'étendent par continuité à $L\{T\}$ en des applications vérifiant les mêmes propriétés, ce qui permet de conclure.

Proposition 1.5. — (i) *$g = \sum_{k\in\mathbf{N}} b_kT^k \in L\{T\}$ est inversible dans $L\{T\}$ si et seulement si $b_0 \neq 0$ et $v_p(b_k) > v_p(b_0)$ si $k \geqslant 1$.*

(ii) *Si $f = \sum_{k\in\mathbf{N}} a_kT^k \in L\{T\}$ est non nul, alors f peut s'écrire de manière unique sous la forme $f = Pg$, où $P \in \mathscr{O}_L[T]$ est un polynôme unitaire, et $g = \sum_{k=0}^{+\infty} b_kT^k$ est une unité de $L\{T\}$*

Démonstration. — Soit $g \in L\{T\}$ inversible. Quitte à diviser g par un élément de L^*, on peut supposer que $v^{[0]}(g) = 0$. On a alors $v^{[0]}(g^{-1}) = 0$, ce qui permet de réduire l'identité $gg^{-1} = 1$ modulo $\mathfrak{m}_L$, et d'obtenir $\overline{g}\cdot\overline{g}^{-1} = 1$ dans $k_K[T]$. On en déduit que $\overline{g}$ est une constante non nulle, ce qui prouve l'implication « $g = \sum_{k\in\mathbf{N}} b_kT^k$ inversible »$\Rightarrow$« $b_0 \neq 0$ et $v_p(b_k) > v_p(b_0)$ si $k \geqslant 1$ ». Réciproquement, si $b_0 \neq 0$ et $v_p(b_k) > v_p(b_0)$ si $k \geqslant 1$, alors $v^{[0]}(b_0^{-1}g - 1) > 0$, ce qui implique que $b_0^{-1}g$ est inversible et donc que g est inversible. On en déduit le (i).

Passons au (ii). La suite $v_p(a_k)$ tendant vers $+\infty$, il existe $d \in \mathbf{N}$ tel que l'on ait $v_p(a_d) \leqslant v_p(a_k)$ (resp. $v_p(a_d) < v_p(a_k)$) si $k \in \mathbf{N}$ (resp. si $k > d$). Soient $\alpha_0 = a_d$ et $P_0 = \sum_{k=0}^{d} \frac{a_k}{a_d}T^k$. Nous allons prouver que l'on peut trouver $R \in \mathfrak{m}_L[T]$, de degré $\leqslant d-1$, et $u \in \mathfrak{m}_L\{T\}$, tels que l'on ait $\alpha_0^{-1}f = (P_0 + R)(1 + u)$, ce qui peut se réécrire sous la forme $P_0u + R = \alpha_0^{-1}f - P_0 - Ru$. Pour ce faire, considérons l'application θ qui à (u, R) associe le couple $\theta(u, R)$ obtenu en prenant le quotient et le reste de la division euclidienne de $\alpha_0^{-1}f - P_0 - Ru$ par P_0. Comme $\alpha_0^{-1}f - P_0 \in \mathfrak{m}_L\{T\}$ par construction de α_0 et P_0, l'application θ envoie $\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1}$ dans lui-même d'après la proposition précédente. D'autre part, cette même proposition montre que

$$\begin{aligned} v^{[0]}(\theta(u,R) - \theta(u'R')) = v^{[0]}(uR - u'R') &\geqslant \inf(v^{[0]}(u) + v^{[0]}(R - R'), v^{[0]}(R') + v^{[0]}(u - u')) \\ &\geqslant \inf(v^{[0]}(u - u'), v^{[0]}(R - R')) + \inf(v^{[0]}(u), v^{[0]}(R')), \end{aligned}$$

ce qui permet de prouver que θ est une application contractante de $\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1}$; son unique point fixe (u_0, R_0) répond à la question. Si $u_0 = \sum_{k=0}^{+\infty} c_kT^k$, il suffit alors de prendre $P = P_0 + R_0$ et $g = \alpha_0(1 + u_0)$.

Pour démontrer l'unicité d'une telle décomposition, remarquons que si $Pg = P'g'$, avec g, g' inversibles dans $L\{T\}$, la fraction rationnelle $\frac{P'}{P}$ n'a aucun zéro ni pôle sur la boule $\{v_p(x) \geqslant 0\}$ et, comme P et P' sont des polynômes unitaires dont tous les zéros appartiennent à cette boule (puisque P et P' sont à coefficients dans $\mathscr{O}_L$), on doit avoir $P = P'$, et donc aussi $g = g'$. Ceci permet de conclure.

Exercice 2. — Montrer que $\mathrm{Newt}_f - \mathrm{Newt}_P$ est constante sur $[0, \deg P]$, et que, si $x \in \mathbf{R}_+$, alors $\mathrm{Newt}_g(x) = \mathrm{Newt}_f(x + \deg P)$,

Corollaire 1.6. — *Si $f \in L[[T]]$ et $\lambda \in \mathbf{R}$, alors le nombre de zéros de F dans $\mathbf{C}_p$ (comptés avec multiplicité) de valuation λ est égal à la longueur du plus grand segment de pente $-\lambda$ dont les extrémités sont des sommets du polygone de Newton de f.*

Démonstration. — Si $\lambda \notin \mathbf{Q}$, il n'y a rien à prouver. Sinon, soit α un élément de $\overline{\mathbf{Q}}_p$ de valuation λ et soit $f_\lambda(T) = f(\frac{T}{\alpha})$. Le polygone de Newton de F et celui de f_λ sont reliés par la formule $\mathrm{Newt}_{f_\lambda}(x) = \mathrm{Newt}_f(x) - \lambda x$; ce qui permet de se ramener au cas $\lambda = 0$ qui suit immédiatement de la proposition précédente et de la théorie des polygones de Newton pour les polynômes.

Proposition 1.7. — *Soit $f \in L\{T\}$ ne s'annulant pas sur le cercle $\{x \in \mathbf{C}_p,\ v_p(x) = 0\}$ et vérifiant $v^{[0]}(f) = 0$. Soit $P \in \mathscr{O}_L[T]$ unitaire, non constant, ayant toutes ses racines de valuation 0. Alors il existe un unique couple (Q, g), avec $g \in L\{T\}$, et $Q \in L[T]$ de degré $< \deg P$, tel que l'on ait $fQ - Pg = 1$. De plus, $v^{[0]}(Q) = 0$.*

Démonstration. — L'unicité suit de ce que, si $f \cdot (Q_1 - Q_2) = P \cdot (g_1 - g_2)$, alors P divise $Q_1 - Q_2$ puisque f et P n'ont pas de zéros commun dans $D(0, 0)$ et que tous les zéros de P appartiennent à $D(0, 0)$. Comme $\deg(Q_1 - Q_2) < \deg P$, cela implique $Q_1 = Q_2$ et $g_1 = g_2$.

L'existence suit de ce que on peut écrire f sous la forme Rh, avec $R \in L[T]$ ayant toutes ses racines dans $D(0, 0)$, et h inversible dans $L\{T\}$. On a alors $(P, R) = 1$, et il existe Q_0 et Q_1 tels que $Q_0 R - Q_1 P = 1$. Il suffit de prendre pour Q le reste de la division de $h^{-1} Q_0$ par P pour assurer que Q est de degré $< \deg P$ et $Qf - 1$ est divisible par P dans $L\{T\}$.

Maintenant, soit $\alpha \in L$ avec $v_p(\alpha) = \inf(v^{[0]}(Q), v^{[0]}(g))$. Comme $v^{[0]}(P) \geqslant 0$ et $v^{[0]}(f) \geqslant 0$, la relation $Qf - Pg = 1$ implique $v_p(\alpha) \leqslant 0$. Si $v_p(\alpha) < 0$, on a $\overline{f}\overline{\alpha^{-1}Q} - \overline{P}\overline{\alpha^{-1}g} = 0$ dans $k_L[T]$, ce qui est impossible car $\overline{f}$ et $\overline{P}$ sont premiers entre eux et $\deg \overline{\alpha^{-1}Q} < \deg \overline{P}$. On a donc $v_p(\alpha) = 0$, ce qui fait qu'on peut prendre $\alpha = 1$. Comme $\overline{P}$ est de degré $\geqslant 1$, la relation $\overline{fQ} - \overline{Pg} = 1$ implique que $\overline{Q} \neq 0$, et donc $v^{[0]}(Q) = 0$. Ceci permet de conclure.

Exercice 3. — Soit L un sous-corps fermé de $\mathbf{C}_p$ tel que v_p soit discrète sur L.

(i) Montrer que $g = \sum_{k=0}^{+\infty} b_k T^k$ est inversible dans $\mathscr{O}_L[[T]]$ si et seulement si $v_p(b_0) = 0$.

(ii) Montrer que $P = X^n + c_{n-1} X^{n-1} + \cdots + c_0$ a toutes ses racines de valuation > 0 si et seulement si $v_p(c_i) > 0$ si $0 \leqslant i \leqslant n - 1$.

(iii) Soit $f \in \mathscr{O}_L[[T]]$ d'image non nulle dans $k_L[[T]]$. Montrer que f s'écrit de manière unique sous la forme $f = Pg$, où P est un polynôme unitaire ayant toutes ses racines de valuation > 0, et g est inversible dans $\mathscr{O}_L[[T]]$.

(iv) Montrer que ce dernier résultat est faux si L n'est pas de valuation discrète.

1.2. Fonctions analytiques sur le disque unité

1.2.1. Anneaux de fonctions analytiques. — Si $r \in \mathbf{R}$, on note $\mathscr{E}_L^{[r,+\infty]}$ l'ensemble des fonctions analytiques sur $D(0, r)$ définies sur L. On note $\mathscr{R}_L^+$ ou $\mathscr{E}_L^{]0,+\infty]}$ l'ensemble des fonctions analytiques sur $D(0, 0^+)$ définies sur L. On a donc $\mathscr{R}_L^+ = \cap_{r>0} \mathscr{E}_L^{[r,+\infty]}$. Finalement, on note $\mathscr{E}_L^+$ ou $\mathscr{E}_L^{(0,+\infty]}$ l'ensemble des fonctions analytiques bornées sur $D(0, 0^+)$ définies sur L. En termes de séries entières, on a les descriptions suivantes.

$$\begin{aligned}
\mathscr{E}_L^{[r,+\infty]} &= \Big\{\sum_{n=0}^{+\infty} a_nT^n,\ a_n \in L \text{ et } v_p(a_n) + rn \to +\infty \text{ quand } n \to +\infty\Big\},\\
\mathscr{E}_L^{+} &= \Big\{\sum_{n=0}^{+\infty} a_nT^n,\ a_n \in L \text{ et } \exists C \in \mathbf{R} \text{ tel que } v_p(a_n) \geqslant C \text{ quel que soit } n \in \mathbf{N}\Big\},\\
\mathscr{R}_L^{+} &= \Big\{\sum_{n=0}^{+\infty} a_nT^n,\ a_n \in L \text{ et } \forall r > 0,\ v_p(a_n) + rn \to +\infty \text{ quand } n \to +\infty\Big\}.
\end{aligned}$$

En particulier, $\mathscr{E}_L^{[0,+\infty]}$ n'est autre que l'anneau $L\{T\}$ considéré ci-dessus, et $\mathscr{E}_L^{[r,+\infty]}$ est aussi l'anneau $\mathrm{A}(D(0,r), L)$ du chapitre précédent. C'est donc un anneau de Banach pour la valuation $v_{D(0,r)}$ que nous noterons plus simplement $v^{[r]}$ (donc $v^{[r]}(\sum_{n=0}^{+\infty} a_nT^n) = \inf_{n\in\mathbf{N}} v_p(a_n) + rn$).

On munit $\mathscr{R}_L^+$ de la topologie définie par la famille de valuations $v^{[r]}$, $r > 0$. Une base de voisinage d'ouverts est constituée des $U_{f,r,C} = \{g \in \mathscr{R}_L^+,\ v^{[r]}(g - f) > C\}$, pour $f \in \mathscr{R}_L^+$, $r > 0$, et $C \in \mathbf{R}$. Une suite f_n tend vers f dans $\mathscr{R}_L^+$ si et seulement si $v^{[r]}(f_n - f)$ tend vers $+\infty$ quand n tend vers $+\infty$, quel que soit $r > 0$ (i.e. si et seulement si f_n tend vers f dans $\mathscr{E}_L^{[r,+\infty]}$, quel que soit $r > 0$). Comme $v^{[r]}(f) < v^{[s]}(f)$ si $r < s$, on peut se contenter de ne considérer que les $v^{[r_h]}$, où r_h est une suite de réels > 0 tendant vers 0, pour définir la topologie de $\mathscr{R}_L^+$. En résumé, $\mathscr{R}_L^+$ est la limite projective (l'intersection) d'une famille dénombrable d'espaces de Banach ; c'est donc un Fréchet. En particulier (ceci ne nous servira pas dans ce cours, mais est quand-même très utile), les théorèmes de Baire (une intersection dénombrable d'ouverts denses est dense) et de Banach-Steinaus (une limite simple de formes linéaires continues est une forme linéaire continue) sont valables pour $\mathscr{R}_L^+$.

Exercice 4. — Soit $f \in \mathscr{R}_L^+$, et soit $r > 0$. Montrer que si f ne s'annule pas sur le cercle $\{x \in \mathbf{C}_p,\ v_p(x) = r\}$, alors $v_p(f(x))$ est constant, égal à $v^{[r]}(f)$, sur ce cercle.

Exercice 5. — Soit $f \in \mathscr{R}_L^+$.

(i) Montrer que la fonction $r \mapsto v^{[r]}(f)$ est une fonction croissante, affine par morceaux, concave sur $]0, +\infty[$.

(ii) Montrer qu'il existe $a \in \mathbf{N}$, $b \in \mathbf{Q}$ et $r_0 > 0$ tels que $v^{[r]}(f) = ar + b$ si $r \geqslant r_0$.

(iii) Soit ρ la limite de $v^{[r]}(f)$ en $r = 0^+$. Montrer que $\rho \neq -\infty$ si et seulement si $f \in \mathscr{E}_L^+$.

(iv) Montrer que, si $f(0) = 0$ et $f \neq 0$, alors $f : D(0, 0^+) \to D(0, \rho^+)$ est surjective.

(v) Montrer que, quel que soit $a \in \mathbf{C}_p$, l'équation $\log(1 + x) = a$ a une solution dans $\mathbf{C}_p$. Quel est l'ensemble des valuations des solutions de cette équation ?

Proposition 1.8. — *Soit $r \in \mathbf{Q}$.*

(i) *Si $f \in \mathscr{E}_L^{[r,+\infty]}$, alors f n'a qu'un nombre fini de zéros dans $D(0, r)$. De plus, si $P = \prod_{x\in D(0,r)}(T - x)^{v_x(f)}$, où $v_x(f)$ est l'ordre d'annulation de f en x, alors $P \in L[T]$, et $P^{-1}f$ est inversible dans $\mathscr{E}_L^{[r,+\infty]}$.*

(ii) *$\mathscr{E}_L^{[r,+\infty]}$ est un anneau principal.*

Démonstration. — alors, quel que soient $n \in \mathbf{N}$ et $x \in D(0, r)$, on a $f^{(n)}(\sigma(x)) = \sigma(f^{(n)}(x))$ puisque $f^{(n)}$ est une série à coefficients dans L convergeant sur $D(0, r)$, et que l'action de $\mathrm{G}_{\mathbf{Q}_p}$ est continue. Ceci implique que $v_{\sigma(x)}(f) = v_x(f)$, et donc que, si f a un nombre fini de zéros dans $D(0, r)$, alors $P = \prod_{x\in D(0,r)}(T - x)^{v_x(f)}$ est invariant par G_L. On en déduit (cf. prop. 1.1) l'appartenance de P à $L[T]$.

Maintenant, comme $r \in \mathbf{Q}$, on peut trouver $\alpha \in \overline{\mathbf{Q}}_p$ avec $v_p(\alpha) = r$, et on peut appliquer la prop. 1.5 à $g(T) = f(\alpha T)$ pour en déduire le reste du (i) [On a $g \in L\{T\}$ par construction].

Le (ii), quant à lui, est une conséquence immédiate du (i) et du fait que $L[T]$ est un anneau principal.

1.2.2. Diviseurs et fonctions. — On supose dorénavant que L est une extension finie de $\mathbf{Q}_p$ (ou, plus généralement, un sous-corps fermé de $\mathbf{C}_p$ tel que la restriction de v_p à L soit *discrète*). Soit $\mathscr{P}_L$ l'ensemble des *diviseurs localement finis, définis sur* L, c'est-à-dire l'ensemble des sommes formelles $D = \sum_{x \in D(0,0^+)} n_D(x)[x]$ telles que

- $n_D(x) \in \mathbf{N}$ si $x \in D(0, 0^+)$ et $\sum_{x \in D(0,r)} n_D(x) < +\infty$ quel que soit $r > 0$;
- $n_D(\sigma(x)) = n_D(x)$ si $\sigma \in \mathrm{G}_L$ et $x \in D(0, 0^+)$.

Si $D_1, D_2 \in \mathscr{P}_L$, on dit que $D_1 \leqslant D_2$ si $n_{D_1}(x) \leqslant n_{D_2}(x)$ quel que soit $x \in D(0, 0^+)$. On note $\min(D_1, D_2)$ le diviseur D défini par $n_D(x) = \min(n_{D_1}(x), n_{D_2}(x))$ quel que soit $x \in D(0, 0^+)$. C'est le plus grand élément de $\mathscr{P}_L$ pour la relation d'ordre ci-dessus qui est inférieur à D_1 et D_2. On dit que D_1 et D_2 sont *étrangers* si $\min(D_1, D_2) = 0$.

Si $P \in L[T]$, on note $[P] \in \mathscr{P}_L$ son diviseur ; il est défini par $n_{[P]}(x) = v_x(P)$, où $v_x(P)$ est l'ordre du zéro de P en x. C'est un diviseur fini (la somme des $n_{[P]}(x)$ est finie). Il est plus ou moins évident sur la définition qu'un élément de $\mathscr{P}_L$ peut s'écrire de manière unique sous la forme $\sum_{i \in I(D)}[P_i]$, où $I(D)$ est un intervalle de $\mathbf{N}$ contenant 0 s'il est non vide, et où $P_i \in L[T]$ est un polynôme unitaire ayant toutes ses racines de valuation r_i, et $r_0 > r_1 > \cdots > r_i > \cdots$, et $\lim_{i \to +\infty} r_i = 0$ si $I(D) = \mathbf{N}$. Cette décomposition est *la décomposition par valuations* de D.

Proposition 1.9. — (i) *Si* $f \in \mathscr{R}_L^+$, *alors* $[f] = \sum_{x \in D(0,0^+)} v_x(f)[x] \in \mathscr{P}_L$.

(ii) f *est inversible dans* $\mathscr{R}_L^+$ *si et seulement si* $[f] = 0$. *Plus généralement,* f *divise* g *dans* $\mathscr{R}_L^+$ *si et seulement si* $[f] \leqslant [g]$.

(iii) *Si* $D \in \mathscr{P}_L$, *alors il existe* $f \in \mathscr{R}_L^+$ *tel que l'on ait* $D = [f]$, *et l'idéal* (f) *de* $\mathscr{R}_L^+$ *engendré par* f *ne dépend que de* D.

Démonstration. — Le (i) est une conséquence immédiate du cor. 1.6 et de la prop. 1.8. Maintenant, si $f \in \mathscr{R}^+$ vérifie $[f] = 0$, alors f n'a aucun zéro sur sur le disque $D(0, r)$, quel que soit $r > 0$. D'après la prop. 1.8, cela implique que f a un inverse dans $\mathscr{E}_L^{[r,+\infty]}$, quel que soit $r > 0$, et donc que l'inverse f^{-1} de f dans $L((T))$ appartient à $\cap_{r>0}\mathscr{E}_L^{[r,+\infty]} = \mathscr{R}_L^+$. Plus généralement, si $[f] \leqslant [g]$, alors, d'après la prop. 1.8, f divise g dans $\mathscr{E}_L^{[r,+\infty]}$, quel que soit $r > 0$. On en déduit l'appartenance de $f^{-1}g \in L((T))$ à $\mathscr{E}_L^{[r,+\infty]}$, quel que soit $r > 0$, et donc l'appartenance de $f^{-1}g$ à $\mathscr{R}_L^+$, ce qui démontre le (ii).

Passons à la démonstration du (iii). Soit $D \in \mathscr{P}_L$, et soit $\sum_{i \in I(D)}[P_i]$ la décomposition par valuations de D. Si $P_i(0) = 0$ (ce qui ne peut se produire que pour $i = 0$), soit $Q_i = P_i$; sinon, soit $Q_i = \frac{P_i}{P_i(0)} = 1 + a_{i,1}T + \cdots + a_{i,n_i}T^{n_i} \in L[T]$. C'est un polynôme ayant toutes ses racines de valuation r_i, et $(r_i)_{i \in \mathbf{N}}$ est une suite strictement décroissante tendant vers 0. Soit $e = e(L/\mathbf{Q}_p)$ l'indice de ramification absolu de L, et, si $i \in \mathbf{N}$, soit $j(i)$ le plus grand entier j tel que $jr_i < \frac{1}{e}$. Comme r_i tend vers 0, $j(i)$ tend vers $+\infty$ quand i tend vers $+\infty$. De plus, comme $v_p(a_{i,j})$ est un multiple de $\frac{1}{e}$, et comme $v_p(a_{i,j}) \geqslant -jr_i$ quel que soit $j \leqslant n_i$, on a $v_p(a_{i,j}) \geqslant 0$ si $j \leqslant j(i)$.

Soit alors $g_i = 1 + \sum_{1 \leqslant j \leqslant j(i)} a_{i,j}T^j$, et soit $f_i = g_i^{-1}Q_i = \sum_{j=0}^{+\infty} b_{i,j}T^j$. Comme g_i est à coefficients dans $\mathscr{O}_L$, et comme son terme constant est 1, cela implique que g_i^{-1} est à coefficients dans $\mathscr{O}_L$, et que $v_p(b_{i,j}) \geqslant -r_i \inf(j, n_i)$. Par ailleurs, on a $b_{i,0} = 1$ et $b_{i,j} = 0$, si $1 \leqslant j \leqslant j(i)$. Soit alors $r > 0$, et soit $i(r)$ tel que l'on ait $r_i < r$ si $i \geqslant i(r)$. Si $s = \sup_{i > i(r)} r_i$, on a $s < r$ et $v_p(b_{i,j}) \geqslant -js$ quels que soient $i \geqslant i(r)$ et $j \in \mathbf{N}$. Cette minoration et la nullité de $b_{i,j}$ si $1 \leqslant j \leqslant j(i)$ impliquent que l'on a $v^{[r]}(f_i - 1) \geqslant (j(i)+1)(r-s)$, si $i \geqslant i(r)$. Comme $(j(i)+1)(r-s)$ tend vers $+\infty$ quand i tend vers $+\infty$, cela implique que le produit $f = \prod_{i \in I(D)} f_i$ converge dans $\mathscr{E}_L^{[s,+\infty]}$, et que son diviseur sur $D(0,s)$ est le même que $\prod_{i=0}^{i(r)-1} f_i$, c'est-à-dire $\sum_{i=0}^{i(r)-1} [P_i]$. Comme ceci est vrai quel que soit $s > 0$, cela montre que le produit $\prod_{i \in I(D)} f_i$ converge dans $\mathscr{R}_L^+$ et que, si $f = \prod_{i \in I(D)} f_i$, alors $[f] = \sum_{i \in I(D)} [P_i] = D$. Ceci permet de conclure.

Remarque 1.10. — Le fait que L est de valuation discrète a joué un rôle essentiel dans la démonstration précédente. De fait, on peut montrer que le résultat est faux pour $\mathbf{C}_p$, mais qu'il est vrai pour un corps algébriquement clos *sphériquement complet* (l'intersection d'une suite de boules fermées emboitées est non vide) ; la démonstration est nettement plus délicate.

Exercice 6. — Montrer que $\mathscr{R}_L^+$ n'est pas un anneau principal.

Exercice 7. — Montrer que $(\mathscr{R}_L^+)^* = (\mathscr{E}_L^+)^*$

Exercice 8. — Si $n \geqslant 1$, on note Φ_n le polynôme $\frac{(1+T)^{p^n}-1}{(1+T)^{p^{n-1}}-1}$.

(i) Montrer que $\log(1+T) = \lim_{n \to +\infty} \frac{(1+T)^{p^n}-1}{p^n}$ dans $\mathscr{R}_L^+$.

(ii) Montrer que l'on a $\log(1+T) = T \prod_{n=1}^{+\infty} \frac{\Phi_n}{p}$ dans $\mathscr{R}_L^+$.

(iii) Montrer que, quelle que soit la suite $(k_n)_{n \in \mathbf{N}}$ d'éléments de n, le produit $T^{k_0} \prod_{n=1}^{+\infty} \left(\frac{\Phi_n}{p}\right)^{k_n}$ converge dans $\mathscr{R}_L^+$.

Exercice 9. — (i) Montrer que $\overline{\mathbf{Q}}$ est dense dans $\mathbf{C}_p$; en déduire que l'ensemble des boules fermées (de valuation rationnelle) de $\mathbf{C}_p$ est dénombrable.
(ii) Soit $r \notin \mathbf{Q}$; soit $(r_n)_{n \in \mathbf{N}}$ une suite strictement croissante d'éléments de $\mathbf{Q}$ dont la limite est r et, si $n \in \mathbf{N}$, soit $\alpha_n \in \mathbf{C}_p$, avec $v_p(\alpha_n) = r_n$. Si $\varepsilon = (\varepsilon_k)_{k \in \mathbf{N}} \in \{0,1\}^{\mathbf{N}}$, soit $D_{\varepsilon,n} = D(\sum_{k=0}^{n} \varepsilon_k \alpha_k, r_{n+1})$.

(a) Montrer que $D_{\varepsilon,n+1} \subset D_{\varepsilon,n}$.

(b) Montrer que, si $\varepsilon, \varepsilon' \in \{0,1\}^{\mathbf{N}}$, et si $\varepsilon_n \neq \varepsilon'_n$, alors $D_{\varepsilon,n} \cap D_{\varepsilon',n} = \emptyset$.

(c) En déduire que $\cap_{n \in \mathbf{N}} D_{\varepsilon,n} = \emptyset$ pour ε dans un sous-ensemble non dénombrable de $\{0,1\}^{\mathbf{N}}$, et que $\mathbf{C}_p$ n'est pas sphériquement complet.

1.2.3. Structure algébrique de l'anneau $\mathscr{R}_L^+$. — Le résultat ci-dessous est une généralisation à l'anneau $\mathscr{R}_L^+$ du théorème des restes chinois.

Théorème 1.11. — (i) *Si P est un polynôme ayant toutes ses racines dans $D(0,0^+)$, alors l'application naturelle $L[T]/(P) \to \mathscr{R}_L^+/(P)$ est un isomorphisme.*

(ii) *Si $f \in \mathscr{R}_L^+$, et si $\sum_{i \in I(f)} [P_i]$ est la décomposition par valuations du diviseur de f, alors l'application naturelle $\mathscr{R}_L^+/(f) \to \prod_{i \in I(f)} \mathscr{R}_L^+/(P_i)$ est un isomorphisme.*

Démonstration. — (i) Soit r_0 le minimum des valuations des racines de P. On a $r_0 > 0$ par hypothèse, et d'après la prop. 1.4 (modulo un changement de variable $T \mapsto \alpha T$), si $0 < r \leqslant r_0$ appartient à $\mathbf{Q}$, tout élément f de $\mathscr{E}_L^{[r,+\infty]}$ peut s'écrire de manière unique sous la forme $f =$

$Pg_r + Q_r$, avec $g_r \in \mathscr{E}_L^{[r,+\infty]}$ et $Q_r \in L[T]$ de degré $< \deg P$. Maintenant, si $f \in \mathscr{R}_L^+$, alors Q_r (et donc aussi g_r) ne dépend pas de $r < r_0$, et on a $g \in \cap_{r>0}\mathscr{E}_L^{[r,+\infty]} = \mathscr{R}_L^+$. On en déduit le (i).

Passons au (ii). L'application de $\mathscr{R}_L^+/(f) \to \prod_{i\in I(f)} \mathscr{R}_L^+/(P_i)$ est injective car un élément du noyau a son diviseur $\geqslant \sum_{i\in I(f)}[P_i] = [f]$ et donc est divisible par f, d'après la prop.1.9. Pour démontrer la surjectivité, nous aurons besoin du lemme suivant.

Lemme 1.12. — *Quel que soit $i \in I(f)$, il existe $g_i \in \mathscr{R}_L^+$, vérifiant :*
- *$v^{[r_i]}(g_i) = 0$, où r_i est la valuation des racines de P_i,*
- *$g_i \equiv 1$ mod P_i, et $g_i \equiv 0$ mod P_j si $j \neq i$.*

Démonstration. — Soit $f_i \in \mathscr{R}_L^+$ de diviseur $\sum_{j\neq i}[P_j]$. Quitte à multiplier f_i par une constante, on peut s'arranger pour que $v^{[r_i]}(f_i) = 0$. Il résulte alors de la prop. 1.7, qu'il existe un unique couple (F_i, h_i), avec $h_i \in \mathscr{E}_L^{[r_i,+\infty]}$ et $F_i \in L[T]$ de degré $< \deg P_i$, tel que l'on ait $F_i f_i - h_i P_i = 1$, et que l'on a de plus $v^{[r_i]}(F_i) = 0$. Il est clair que $g_i = F_i f_i$ satisfait aux exigences du lemme.

Lemme 1.13. — *Soit $g \in \mathscr{E}_L^{[r,+\infty]}$, ayant une racine de valuation $s_0 > r$, et soit $s \geqslant r$. Alors $v^{[s]}(g) \geqslant v^{[r]}(g) + \inf(s - r, s_0 - r)$.*

Démonstration. — On peut écrire g sous la forme $\alpha u \prod_{i=1}^d (X - x_i)$, où les x_i sont des éléments de $D(0, r)$, $\alpha \in L^*$, et $v^{[r]}(u - 1) > 0$. Si $s \geqslant r$, on a alors

$$v^{[s]}(g) = \inf_{x\in D(0,s)} v_p(g(x)) = v_p(\alpha) + \sum_{i=1}^d \inf(s, v_p(x_i)) = v^{[r]}(g) + \sum_{i=1}^d \inf(s - r, v_p(x_i) - r).$$

On en déduit le résultat.

Revenons à la démonstration de la surjectivité de $\mathscr{R}_L^+/(f) \to \prod_{i\in I(f)} \mathscr{R}_L^+/(P_i)$. Soit $(Q_i)_{i\in I(f)}$ une suite d'éléments de $L[T]$. Si $i \geqslant 1$, si $r \geqslant r_i$ et si $k_i \in \mathbf{N}$, on a, d'après le lemme 1.13,

$$v^{[r]}(Q_i g_i^{k_i}) = v^{[r]}(Q_i) + k_i v^{[r]}(g_i) \geqslant v^{[0]}(Q_i) + k_i \inf(r_0 - r_i, r - r_i).$$

Prenons alors $k_i = \sup(i, |v^{[0]}(Q_i)|)^2$ de telle sorte que $v^{[0]}(Q_i) + k_i \inf(r_0 - r_i, r - r_i)$ tende vers $+\infty$ quand i tend vers $+\infty$, quel que soit $r > 0$ (on a $r > r_i$ si i est assez grand). La série $\sum_{i\in I(f)} Q_i g_i^{k_i}$ converge alors dans $\mathscr{E}_L^{[r,+\infty]}$ pour tout $r > 0$; elle converge donc aussi dans $\mathscr{R}_L^+$, et par construction sa somme g a même image que Q_i dans $L[T]/(P_i)$. La suite $(Q_i)_{i\in I(f)}$ étant arbitraire, cela permet de conclure.

Corollaire 1.14. — *L'anneau $\mathscr{R}_L^+$ est un anneau de Bézout* (tout idéal engendré par un nombre fini d'éléments est principal).

Démonstration. — Il suffit de montrer qu'un idéal engendré par deux éléments f et g est principal (une récurrence immédiate permet d'en déduire le cas général). Soit $h \in \mathscr{R}_L^+$ de diviseur $\min([f], [g])$. Alors h divise f et g, et il s'agit de prouver que h est dans l'idéal engendré par f et g. Quitte à diviser f et g par h, on est ramené à prouver que, si les diviseurs de f et g sont étrangers, alors l'idéal de $\mathscr{R}_L^+$ engendré par f et g contient 1. Soit $\sum_{i\in I(f)}[P_i]$ la décomposition par valuations de $[f]$. Comme $[f]$ et $[g]$ sont étrangers, g est inversible dans $L[T]/(P_i)$ quel que soit $i \in I$, et donc aussi dans $\mathscr{R}_L^+/(f)$ d'après le th. 1.11. Il existe donc $a \in \mathscr{R}_L^+$ tel que $ag - 1 \in (f)$, ce qui permet de conclure.

1.2.4. Éléments d'ordre r. — Si $h \in \mathbf{N}$, soit $v_h = \frac{1}{(p-1)p^h} = v_p(\zeta_{p^{h+1}} - 1)$. Comme v_h tend vers 0, la topologie de $\mathscr{R}_L^+$ est aussi la topologie (de Fréchet) définie par la famille de valuations $v_{D(0,v_h)}$, $h \in \mathbf{N}$.

Un élément $f = \sum_{n=0}^{+\infty} b_n T^n$ de $\mathscr{R}_L^+$ est *d'ordre r*, si $v_p(b_n) + r\ell(n)$ est borné inférieurement quand n tend vers $+\infty$. On note $\mathscr{R}_{L,r}^+$ le sous-ensemble de $\mathscr{R}_L^+$ des éléments d'ordre r, et on munit $\mathscr{R}_{L,r}^+$ de la valuation v_r définie par $v_r(f) = \inf_{n\in\mathbf{N}} v_p(b_n) + r\ell(n)$, ce qui en fait un L-banach.

L'espace $\mathscr{R}_{L,0}^+$ des séries à coefficients bornés n'est autre que $\mathscr{E}_L^+$.

Lemme 1.15. — *La valuation v_r est équivalente à la valuation v_r' définie par*
$$v_r'(f) = \inf_{h\in\mathbf{N}} \big(v_{D(0,v_h)}(f) + rh\big).$$

Démonstration. — Si $f(T) = \sum_{n\in\mathbf{N}} a_n T^n \in \mathscr{R}_{L,r}^+$, on a
$$v_r'(f) = \inf_{h\in\mathbf{N}} \Big(\inf_{n\in\mathbf{N}} \Big(v_p(a_n) + \frac{n}{(p-1)p^h} + rh\Big)\Big) = \inf_{n\in\mathbf{N}} \Big(v_p(a_n) + \inf_{h\in\mathbf{N}} \Big(\frac{n}{(p-1)p^h} + rh\Big)\Big).$$
Si $n = 0$, le minimum ci-dessus vaut 0. Si $n \geqslant 1$, La fonction $x \mapsto \frac{n}{(p-1)p^x} + rx$ atteint son minimum en $\frac{1}{\log p} \log\big(\frac{n\log p}{(p-1)r}\big)$, et en prenant $h = \big[\frac{\log n}{\log p}\big] = \ell(n) - 1 \geqslant \frac{\log n}{\log p} - 1$, on obtient l'encadrement
$$r(\ell(n)-1) + \frac{r}{\log p}(1 + \log\frac{\log p}{(p-1)r}) \leqslant \inf_{h\in\mathbf{N}} \Big(\frac{n}{(p-1)p^h} + rh\Big) \leqslant \frac{p}{p-1} + r(\ell(n)-1).$$
On en déduit le résultat.

1.2.5. Actions de $\mathbf{Z}_p^*$, φ et ψ

• Actions de $\mathbf{Z}_p^*$ et φ.

Si $x \in L^*$, alors $(1+T)^x - 1 = \sum_{n=1}^{+\infty} \binom{x}{n} T^n$ est une uniformisante de $L((T))$. Ceci permet de définir un automorphisme continu (pour la valuation v_T) $f \mapsto f \star x$ de $L[[T]]$, en envoyant $\sum_{n=0}^{+\infty} a_n T^n$ sur $\sum_{n=0}^{+\infty} a_n((1+T)^x - 1)^n$. Comme
$$((1+T)\star x)\star y = ((1+T)^x)\star y = ((1+T)^y)^x = (1+T)^{xy},$$
on a $(f\star x)\star y = f\star xy$ quel que soit $f \in L[[T]]$; on a donc défini une action de groupe de L^* sur $L[[T]]$.

Lemme 1.16. — (i) *Si $a \in \mathbf{Z}_p^*$, et si $r \geqslant 0$, alors $v^{[r]}((1+T)^a - 1) = v^{[r]}(T)$.*

(ii) *Si $r \geqslant 0$ et si $s = \inf(r+1, pr)$, alors $v^{[r]}((1+T)^p - 1) = v^{[s]}(T)$.*

Démonstration. — Le (i) suit de ce que $\binom{a}{n} \in \mathbf{Z}_p$ si $a \in \mathbf{Z}_p^*$, et le (ii) est un calcul immédiat.

On note $f \mapsto \varphi(f)$ l'application $f \mapsto f \star p$. D'après ce qui précède, les actions de φ et $\mathbf{Z}_p^*$ commutent entre elles sur $L[[T]]$.

Proposition 1.17. — (i) *Si $r \geqslant 0$ et si $a \in \mathbf{Z}_p^*$, alors $f \mapsto f \star a$ est une isométrie de $\mathscr{E}_L^{[r,+\infty]}$ dans lui-même.*

(ii) *Si $r \geqslant 0$, si $r' = \sup(r-1, \frac{r}{p})$ et si $f \in \mathscr{E}_L^{[r,+\infty]}$, alors $\varphi(f) \in \mathscr{E}_L^{[r',+\infty]}$, et $v^{[r']}(\varphi(f)) = v^{[r]}(f)$. En particulier, $f \mapsto \varphi(f)$ est continue de $\mathscr{E}_L^{[r,+\infty]}$ dans $\mathscr{E}_L^{[r',+\infty]}$.*

Démonstration. — Soit $f = \sum_{n=0}^{+\infty} a_n T^n \in \mathscr{E}_L^{[s,+\infty]}$. Si $s' \in \mathbf{R}$ et $x \in L$, on a

$$v^{[s]}(f) = \inf_{n\in\mathbf{N}} v^{[s]}(a_n T^n) = \inf_{n\in\mathbf{N}} v_p(a_n) + v^{[s]}(T)$$
$$v^{[s']}(f \star x) \geqslant \inf_{n\in\mathbf{N}} v^{[s']}(a_n((1+T)^x - 1))^n) \geqslant \inf_{n\in\mathbf{N}} v_p(a_n) + nv^{[s']}((1+T)^x - 1).$$

En appliquant ceci à $s = s' = r$, et $x = a \in \mathbf{Z}_p^*$, cela permet de montrer, en utilisant le (i) du lemme précédent, que $v^{[r]}(f \star a) \geqslant v^{[r]}(f)$. On en déduit le (i) en appliquant l'inégalité ci-dessus à $f \star a^{-1}$.

Passons à la démonstration du (ii). Le fait que $\varphi(f) \in \mathscr{E}_L^{[r',+\infty]}$ si $f \in \mathscr{E}_L^{[r,+\infty]}$ se démontre en prenant $s' = r$, $s = r'$, et en utilisant le (ii) du lemme 1.16. Finalement, $z \mapsto (1+z)^p - 1$ induit une surjection de $D(0,r')$ sur $D(0,r)$. On en déduit la formule

$$v^{[r]}(f) = \inf_{z\in D(0,r)} (v_p(f(z))) = \inf_{z\in D(0,r')} v_p(f((1+z)^p - 1) = \inf_{z\in D(0,r')} v_p(\varphi(f)(z)) = v^{[r']}(\varphi(f)),$$

ce qui permet de conclure.

Corollaire 1.18. — *Les actions de $\mathbf{Z}_p^*$ et φ laissent stable $\mathscr{R}_L^+$ et sont continues sur $\mathscr{R}_L^+$.*

- L'opérateur ψ.

Lemme 1.19. — (i) *Si $0 \leqslant r \leqslant \frac{1}{p-1}$, et si $\zeta^p = 1$, alors $v^{[r]}((1+T)\zeta - 1) = v^{[r]}(T)$.*

(ii) *L'application $f \mapsto f * \zeta$, où $(f * \zeta)(T) = f((1+T)\zeta - 1)$, est une isométrie de $\mathscr{E}_L^{[r,+\infty]}$ si $0 \leqslant r \leqslant \frac{1}{p-1}$, et ceci définit une action de groupe continue de $\boldsymbol{\mu}_p$ sur $\mathscr{E}_L^{[r,+\infty]}$ et $\mathscr{R}_L^+$ si $\boldsymbol{\mu}_p \subset L$.*

Démonstration. — Le (i) suit de ce que $v_p(\zeta - 1) \geqslant \frac{1}{p-1}$. Le (ii) se démontre à partir du (i) comme le (i) de la prop. 1.17.

Lemme 1.20. — *Soit $n \in \mathbf{N}$.*

(i) *Il existe un unique $Q_n \in \mathbf{Q}_p[T]$ tel que $Q_n((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p=1}((1+T)\zeta - 1)^n$.*

(ii) *Si $0 \leqslant r \leqslant \frac{p}{p-1}$, alors $v^{[rp]}(Q_n) \geqslant nv^{[r]}(T) - 1$*

Démonstration. — Soit $R_n(T) = \frac{1}{p}\sum_{\zeta^p=1}((1+T)\zeta - 1)^n$. Comme $\sum_{\zeta^p=1}\zeta^i = 0$ si i n'est pas un multiple de p, cela implique que R_n est un polynôme en $(1+T)^p$. On en déduit le (i).

Pour démontrer le (ii), commençons par remarquer que, d'après le lemme 1.19, l'on a $v^{[r]}(R_n) \geqslant nv^{[r]}(T) - 1$, si $0 \leqslant r \leqslant \frac{1}{p-1}$. On conclut via l'identité $v^{[rp]}(R_n) = v^{[r]}(Q_n)$ de la prop. 1.17.

Proposition 1.21. — (i) *Si $0 \leqslant r \leqslant \frac{1}{p-1}$, et si $f \in \mathscr{E}_L^{[r,+\infty]}$, il existe $\psi(f) \in \mathscr{E}_L^{[r/p,+\infty]}$ unique tel que $\psi(f)((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p=1} f((1+T)\zeta - 1)$. De plus, $\psi : \mathscr{E}_L^{[r,+\infty]} \to \mathscr{E}_L^{[r/p,+\infty]}$ est continue, et ψ laisse stable $\mathscr{R}_L^+$ et est continue sur $\mathscr{R}_L^+$.*

(ii) *ψ commute à $\mathbf{Z}_p^*$ sur $\mathscr{R}_L^+$ et sur $\mathscr{E}_L^{[r,+\infty]}$, si $0 \leqslant r \leqslant \frac{1}{p-1}$.*

(iii) *$\psi \circ \varphi = \mathrm{id}$, et plus généralement, $\psi(\varphi(f)g) = f\psi(g)$, si $f, g \in \mathscr{E}_L^{[r,+\infty]}$, et $0 \leqslant r \leqslant \frac{1}{p-1}$.*

Démonstration. — Si $f = \sum_{n=0}^{+\infty} a_n T^n$, soit $\psi(f) = \sum_{n=0}^{+\infty} a_n Q_n$. Le lemme précédent montre que $\psi : \mathscr{E}_L^{[r,+\infty]} \to \mathscr{E}_L^{[r/p,+\infty]}$ est continue si $0 \leqslant r \leqslant \frac{p}{p-1}$. Par ailleurs, si f est un polynôme, on a $\psi(f)((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p=1} f((1+T)\zeta - 1)$. Or l'application $f \mapsto \frac{1}{p}\sum_{\zeta^p=1} f((1+T)\zeta - 1)$ est continue sur $\mathscr{E}_L^{[r,+\infty]}$ d'après le lemme 1.19 ; On en déduit le (i).

Le (ii) et le (iii) sont immédiats pour $f = (1+T)^n$ (resp. $f = (1+T)^n$, $g = (1+T)^m$) ; le cas général s'en déduit par linéarité et continuité.

Exercice 10. — (i) Montrer que $\mathbf{Z}_p^*$ agit par des isométries sur $\mathscr{R}_{L,r}^+$ muni de v_r'.

(ii) Montrer que ϕ et ψ laissent stables $\mathscr{R}_{L,r}^+$ et sont continus sur $\mathscr{R}_{L,r}^+$.

Exercice 11. — Soit L une extension non ramifiée de $\mathbf{Q}_p$. Soit $I \neq 0$ un idéal de type fini de $\mathscr{R}_L^+$, et soit Φ_n, pour $n \in \mathbf{N}$, le polynôme défini à l'exercice 8.

(i) Montrer que, si I est stable par $\mathbf{Z}_p^*$, alors il existe une suite $(k_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{N}$, telle que I soit engendré par $X^{k_0}\prod_{n=1}^{+\infty}\left(\frac{\Phi_n}{p}\right)^{k_n}$.

(ii) Montrer que, si I est stable par φ, alors il existe une suite décroissante $(k_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{N}$, telle que I soit engendré par $X^{k_0}\prod_{n=1}^{+\infty}\left(\frac{\Phi_n}{p}\right)^{k_n}$.

2. Distributions p-adiques

2.1. Distributions continues

On appelle distribution continue sur $\mathbf{Z}_p$ une forme linéaire continue sur $\mathrm{LA}(\mathbf{Z}_p, L)$, c'est-à-dire une forme linéaire sur $\mathrm{LA}(\mathbf{Z}_p, L)$ dont la restriction à chaque $\mathrm{LA}_h(\mathbf{Z}_p, L)$ est continue. En particulier, si μ est une distribution continue, on peut considérer μ comme un élément du dual de $\mathrm{LA}_h(\mathbf{Z}_p, L)$, et donc définir sa valuation $v_{\mathrm{LA}_h}(\mu) = \inf_{\phi\in\mathrm{LA}_h(\mathbf{Z}_p,L)-\{0\}}(v_p(\mu(\phi)) - v_{\mathrm{LA}_h}(\phi))$.

On note $\mathscr{D}(\mathbf{Z}_p, L)$ l'ensemble des distributions continues sur $\mathbf{Z}_p$, à valeurs dans L, et on munit $\mathscr{D}(\mathbf{Z}_p, L)$ de la topologie de Fréchet définie par la famille de valuations v_{LA_h}, $h \in \mathbf{N}$.

Si $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$, on écrira en général $\mu(\phi)$ sous la forme plus parlante $\int_{\mathbf{Z}_p}\phi(x)\,\mu(x)$ ou simplement sous la forme $\int_{\mathbf{Z}_p}\phi\,\mu$.

A une distribution continue μ, on associe la série formelle

$$\mathscr{A}_\mu(T) = \int_{\mathbf{Z}_p}(1+T)^x\mu(x) = \sum_{n=0}^{+\infty} T^n \int_{\mathbf{Z}_p}\binom{x}{n}\mu(x),$$

appelée *transformée d'Amice* de μ.

Lemme 2.1. — *Si $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$, et si $z \in D(0, 0^+)$, alors $\int_{\mathbf{Z}_p}(1+z)^x\mu(x) = \mathscr{A}_\mu(z)$.*

Démonstration. — Il existe $h \in \mathbf{N}$ tel que $v_p(z) > v_h$, ce qui implique que la série $\sum_{n=0}^{+\infty}\binom{x}{n}z^n$ converge vers $(1+z)^x$ dans $\mathrm{LA}_h(\mathbf{Z}_p, \mathbf{C}_p)$ car $\frac{z^n}{[\frac{n}{p^h}]!}$ tend vers 0. On en déduit le résultat.

Théorème 2.2. — *L'application $\mu \mapsto \mathscr{A}_\mu$ est un isomorphisme d'espaces de Fréchet de $\mathscr{D}(\mathbf{Z}_p, L)$ sur $\mathscr{R}_L^+$. De plus, si $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$, et si $h \in \mathbf{N}$, on a*

$$v_{D(0,v_h)}(\mathscr{A}_\mu) \geqslant v_{\mathrm{LA}_h}(\mu) \geqslant v_{D(0,v_{h+1})}(\mathscr{A}_\mu) - 1.$$

Démonstration. — Soit μ une distribution et $\mathscr{A}_\mu(T) = \sum_{n=0}^{+\infty} b_n T^n$ sa transformée d'Amice. En utilisant le théorème d'Amice, on montre que, quel que soient $h \in \mathbf{N}$ et $n \in \mathbf{N}$,

$$v_p(b_n) \geqslant v_{\mathrm{LA}_h}(\mu) + v_{\mathrm{LA}_h}\left(\binom{x}{n}\right) = v_{\mathrm{LA}_h}(\mu) - v_p\left([\frac{n}{p^h}]!\right) \geqslant v_{\mathrm{LA}_h}(\mu) - nv_h.$$

Ceci permet de montrer que $\mathscr{A}_\mu$ converge sur $D(0,v_h^+)$ pour tout h, et donc appartient à $\mathscr{R}_L^+$, et aussi que $v_{D(0,v_h)}(\mathscr{A}_\mu) \geqslant v_{\mathrm{LA}_h}(\mu)$.

Réciproquement, si $= \sum_{n=0}^{+\infty} b_n T^n \in \mathscr{R}_L^+$, alors pour tout $h \in \mathbf{N}$ et tout $n \in \mathbf{N}$,

$$v_p\Big(\big[\frac{n}{p^h}\big]!b_n\Big) \geqslant v_p(b_n) + \big[\frac{n}{p^{h+1}}\big] \geqslant v_p(b_n) + nv_{h+1} - 1 \geqslant v_{D(0,v_{h+1})}(\mathscr{A}_\mu) - 1,$$

et tend vers $+\infty$ quand n tend vers $+\infty$. Ceci montre que l'on peut définir une distribution continue μ sur $\mathbf{Z}_p$, en posant $\int_{\mathbf{Z}_p} \phi\,\mu = \sum_{n=0}^{+\infty} b_n a_n(\phi)$. De plus, on a

$$v_{\mathrm{LA}_h}(\mu) = \inf_{n\in\mathbf{N}} v_p\Big(\big[\frac{n}{p^h}\big]!b_n\Big) \geqslant v_{D(0,v_{h+1})}(\mathscr{A}_\mu) - 1.$$

Ceci permet de conclure.

Exercice 12. — (i) Montrer que $\frac{1}{p^n}\sum_{i=0}^{p^n-1}(1+T)^i$ tend vers $\frac{\log(1+T)}{T}$ dans $\mathscr{R}_L^+$.

(ii) Montrer que, si $\phi \in \mathrm{LA}(\mathbf{Z}_p, L)$, alors $\frac{1}{p^n}\sum_{i=0}^{p^n-1}\phi(i)$ a une limite dans L.

2.2. Distributions tempérées et mesures

2.2.1. Transformées d'Amice des distributions tempérées. — Soit $r \geqslant 0$. Une distribution continue μ sur $\mathbf{Z}_p$ est dite *d'ordre* r si elle s'étend par continuité à $\mathscr{C}^r$. On note $\mathscr{D}_r(\mathbf{Z}_p, L)$ l'ensemble des distributions d'ordre r que l'on munit de la valuation $v'_{\mathscr{D}_r}$ définie par

$$v'_{\mathscr{D}_r} = \inf_{\phi\in\mathscr{C}^r(\mathbf{Z}_p,L)-\{0\}} \Big(v_p\Big(\int_{\mathbf{Z}_p}\phi\,\mu\Big) - v_{\mathscr{C}^r}(\phi)\Big),$$

ce qui fait de $\mathscr{D}_r(\mathbf{Z}_p, L)$ le dual topologique de $\mathscr{C}^r(\mathbf{Z}_p, L)$.

Une distribution est dite *tempérée*, s'il existe $r \in \mathbf{R}_+$ telle qu'elle soit d'ordre r. On note $\mathscr{D}_{\mathrm{temp}}$ l'espace des distributions tempérées.

Proposition 2.3. — *L'application $\mu \mapsto \mathscr{A}_\mu$ induit une isométrie de $\mathscr{D}_r(\mathbf{Z}_p, L)$ sur $\mathscr{R}_{L,r}^+$.*

Démonstration. — C'est immédiat à partir de la définition de $v_{\mathscr{C}^r}$.

Exercice 13. — (i) Montrer que la suite de terme général $\frac{1}{p^n}\sum_{i=0}^{p^n-1}(1+T)^i$ est bornée dans $\mathscr{R}_{L,1}^+$, mais qu'elle ne converge pas pour la valuation v_1.

(ii) Montrer que, si $\phi \in \mathscr{C}^1(\mathbf{Z}_p, L)$, alors $\frac{1}{p^n}\sum_{i=0}^{p^n-1}\phi(i)$ a une limite dans L. Quelle est cette limite ? (On commencera par regarder $\phi = \binom{x}{n}$, et on utilisera le (i)).

(iii) Montrer qu'il existe $\phi \in \mathscr{C}^0(\mathbf{Z}_p, L)$ tel que $\frac{1}{p^n}\sum_{i=0}^{p^n-1}\phi(i)$ n'ait pas de limite dans L. (On ne demande pas de construire un tel ϕ explicitement.)

2.2.2. Mesures. — Une distribution d'ordre 0 est aussi appelée *une mesure*. Par définition, l'espace $\mathscr{D}_0(\mathbf{Z}_p, L)$ des mesures est donc le dual topologique de l'espace des fonctions continues. La prop. 2.3 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 $\mathscr{C}^0(\mathbf{Z}_p,L)$.

Exercice 14. — Soit $z\in\mathbf{C}_p-D(1,0^+)$.

(i) Montrer qu'il existe une unique mesure μ_z sur $\mathbf{Z}_p$ telle que l'on ait $\mu_z(a+p^n\mathbf{Z}_p)=\frac{z^a}{1-z^{p^n}}$ si $0\leqslant a\leqslant p^n-1$.

(ii) Montrer que la transformée d'Amice de μ_z est $\frac{1}{1-(1+T)z}$.

2.2.3. Distributions tempérées et sommes de Riemann. — La prop. 2.3 caractérise les distributions tempérées en termes de leurs transformées d'Amice, ce qui permet de construire une distribution tempérée à partir d'une série entière de rayon de convergence 1, vérifiant des conditions de croissance. La connaissance de la transformée d'Amice d'une distribution est équivalente à la connaissance des $\int_{\mathbf{Z}_p}x^i\mu(x)$ pour $i\in\mathbf{N}$. Le théorème suivant permet de construire une distribution d'ordre fini en ne connaissant que les intégrales du type $\int_{a+p^n\mathbf{Z}_p}x^i\mu(x)$ pour $a\in\mathbf{Z}_p$, $n\in\mathbf{N}$ et $0\leqslant i\leqslant N$. Cette construction généralise celle des mesures donnée au n$^{\text{o}}$ précédent et est très importante pour les applications arithmétiques (par exemple pour construire les fonctions L p-adiques attachées aux formes modulaires).

Si I est une partie de $\mathbf{N}$, on note $\mathscr{D}^I_{\mathrm{alg}}(\mathbf{Z}_p,L)$ l'ensemble des distributions algébriques sur $\mathbf{Z}_p$ (de degré $\in I$), c'est-à-dire l'ensemble des formes linéaires sur $\mathrm{LP}^I(\mathbf{Z}_p,L)$. Un élément μ de $\mathscr{D}^I_{\mathrm{alg}}(\mathbf{Z}_p,L)$ est donc équivalent à la donnée des valeurs $\int_{a+p^n\mathbf{Z}_p}x^i\mu(x)$ pour $i\in I$, $a\in\mathbf{Z}_p$ et $n\in\mathbf{N}$, avec les relations de compatibilité évidentes

$$\int_{a+p^n\mathbf{Z}_p}x^i\mu(x)=\sum_{k=0}^{p-1}\int_{a+kp^n+p^{n+1}\mathbf{Z}_p}x^i\mu(x).$$

On a une application naturelle de $\mathscr{D}(\mathbf{Z}_p,L)$ dans $\mathscr{D}^I_{\mathrm{alg}}(\mathbf{Z}_p,L)$ quel que soit $I\subset\mathbf{N}$.

Si I est une partie de $\mathbf{R}$, on pose $\mathscr{D}^I_{\mathrm{alg}}(\mathbf{Z}_p,L)=\mathscr{D}^{I\cap N}_{\mathrm{alg}}(\mathbf{Z}_p,L)$

Théorème 2.4. — (i) *Si $\mu\in\mathscr{D}_r(\mathbf{Z}_p,L)$, il existe $C\in\mathbf{R}$ tel que, quels que soient $a\in\mathbf{Z}_p$, $k\in\mathbf{N}$ et $n\in\mathbf{N}$, on ait*

$$v_p\Big(\int_{a+p^n\mathbf{Z}_p}\big(\frac{x-a}{p^n}\big)^k\mu\Big)\geqslant C-rn.$$

(ii) *Réciproquement, si* $N \in \mathbf{N} \cup \{+\infty\}$ *est* $\geqslant [r]$, *si* $\mu \in \mathscr{D}_{\mathrm{alg}}^{[0,N]}(\mathbf{Z}_p, L)$ *est telle qu'il existe* $C \in \mathbf{R}$ *tel que, quels que soient* $a \in \mathbf{Z}_p$, $k \leqslant N$ *et* $n \in \mathbf{N}$, *on ait*

$$v_p\Big(\int_{a+p^n\mathbf{Z}_p} \big(\frac{x-a}{p^n}\big)^k \mu\Big) \geqslant C - rn,$$

alors μ *se prolonge de manière unique en une distribution d'ordre* r *sur* $\mathbf{Z}_p$.

Démonstration. — (i) La fonction $\phi_{a,n,k}$, définie par $\phi_{a,n,k}(x) = \mathbf{1}_{a+p^n\mathbf{Z}_p}(x)\big(\frac{x-a}{p^n}\big)^k$ appartient à $\mathrm{LA}_n(\mathbf{Z}_p, L)$ et on a $v_{\mathrm{LA}_n}(\phi_{a,n,k}) = 0$. Comme $v_{\mathscr{C}^r}(\phi) \geqslant v_{\mathrm{LA}_n}(\phi) - nr - C_1(r)$, si $\phi \in \mathrm{LA}_n(\mathbf{Z}_p, L)$ (cf. chapitre précédent), on en déduit la minoration

$$v_p\Big(\int_{a+p^n\mathbf{Z}_p} \big(\frac{x-a}{p^n}\big)^k \mu\Big) \geqslant v'_{\mathscr{D}_r}(\mu) + v_{\mathscr{C}^r}(\phi_{a,n,k}) \geqslant v'_{\mathscr{D}_r}(\mu) + v_{\mathrm{LA}_n}(\phi_{a,n,k}) - nr - C_1(r),$$

ce qui démontre le (i) avec $C = v'_{\mathscr{D}_r}(\mu) - C_1(r)$.

(ii) Pour démontrer le (ii), introduisons le sous-espace $\mathscr{D}_r^{[0,N]}(\mathbf{Z}_p, L)$ des éléments $\mu \in \mathscr{D}_{\mathrm{alg}}^{[0,N]}(\mathbf{Z}_p, L)$ tels que la quantité

$$v_{\mathscr{D}_r,N}(\mu) = \inf_{a\in\mathbf{Z}_p,\, k\leqslant N,\, n\in\mathbf{N}} \Big(v_p\Big(\int_{a+p^n\mathbf{Z}_p} \big(\frac{x-a}{p^n}\big)^k \mu\Big) + rn\Big)$$

soit finie. D'après le (i), l'application naturelle ι de $\mathscr{D}(\mathbf{Z}_p, L)$ dans $\mathscr{D}_{\mathrm{alg}}^{[0,N]}$ envoie $\mathscr{D}_r(\mathbf{Z}_p, L)$ dans $\mathscr{D}_r^{[0,N]}(\mathbf{Z}_p, L)$, et on est ramené à démontrer que la restriction de ι à $\mathscr{D}_r(\mathbf{Z}_p, L)$ induit un isomorphisme de $\mathscr{D}_r(\mathbf{Z}_p, L)$ sur $\mathscr{D}_r^{[0,N]}(\mathbf{Z}_p, L)$.

La restriction de ι à $\mathscr{D}_r(\mathbf{Z}_p, L)$ est injective puisque $\mathrm{LP}^{[0,N]}(\mathbf{Z}_p, L)$ est dense dans $\mathscr{C}^r(\mathbf{Z}_p, L)$. Il ne reste donc que la surjectivité à prouver. Soit $\mu \in \mathscr{D}_r^{[0,N]}(\mathbf{Z}_p, L)$. Si $i \in \mathbf{N}$, et si $k \in \{0, 1, \ldots, [r]\}$, soit $e_{i,k,r}$ l'élément de la base de vaguelettes définie au chapitre précédent. Posons

$$b_{i,k} = \int_{\mathbf{Z}_p} e_{i,k,r}\, \mu = \int_{i+p^{\ell(i)}\mathbf{Z}_p} p^{[r\ell(i)]}\big(\frac{x-a}{p^{\ell(i)}}\big)^k \mu.$$

On a donc $v_p(b_{i,k}) \geqslant v_{\mathscr{D}_r,N}(\mu) - 1$ quels que soient $i \in \mathbf{N}$ et $k \in \{0, 1, \ldots, [r]\}$. Il existe donc, puisque les $e_{i,k,r}$ forment une base de Banach de $\mathscr{C}^r(\mathbf{Z}_p, L)$, un unique élément $\tilde\mu$ de $\mathscr{D}_r(\mathbf{Z}_p, L)$ tel que, quels que soient $i \in \mathbf{N}$ et $k \in \{0, 1, \ldots, [r]\}$, on ait $\int_{\mathbf{Z}_p} e_{i,k,r}\, \tilde\mu = b_{i,k}$.

Soit alors $\lambda = \iota(\tilde\mu) - \mu$. C'est un élément de $\mathscr{D}_r^{[0,N]}(\mathbf{Z}_p, L)$ dont la restriction à $\mathrm{LP}^{[0,r]}(\mathbf{Z}_p, L)$ est identiquement nulle par construction. Maintenant, si $k \leqslant N$, et si $m \in \mathbf{N}$, on peut écrire $\int_{a+p^n\mathbf{Z}_p} x^k \lambda$ sous la forme

$$\sum_{i=0}^{p^m-1} \Big(\sum_{j=0}^{k} \binom{k}{j} (a+ip^n)^{k-j} \int_{a+ip^n+p^{n+m}\mathbf{Z}_p} (x-(a+ip^n))^j \lambda\Big).$$

Comme les termes avec $j \leqslant r$ sont nuls, et ceux avec $j > r$ ont une valuation $\geqslant \big(\inf_{r<j\leqslant k}(j-r)(n+m)\big) + v_{\mathscr{D}_r,N}(\lambda)$, et comme cette dernière quantité tend vers $+\infty$ quand m tend vers $+\infty$, cela permet de montrer que $\int_{a+p^n\mathbf{Z}_p} x^k \lambda = 0$ quels que soient $a \in \mathbf{Z}_p$, $k \leqslant N$ et $n \in \mathbf{N}$. On en déduit l'égalité $\mu = \iota(\tilde\mu)$, ce qui prouve que ι est surjective est permet de conclure.

2.2.4. Autres valuations naturelles sur $\mathscr{D}_r(\mathbf{Z}_p, L)$. — La valuation $v'_{\mathscr{D}_r}$ dont nous avons muni $\mathscr{D}_r$ n'est pas toujours très commode. La valuation $v_{\mathscr{D}_r}$ définie ci-dessous est, en général, nettement plus agréable.

Proposition 2.5. — *Si on définit $v_{\mathscr{D}_r}(\mu)$, pour $\mu \in \mathscr{D}_r(\mathbf{Z}_p, L)$ par la formule*

$$v_{\mathscr{D}_r}(\mu) = \inf_{n\in\mathbf{N}} v_{\mathrm{LA}_n}(\mu) + rn = \inf_{a\in\mathbf{Z}_p,\, k\in\mathbf{N},\, n\in\mathbf{N}} \Big(v_p\Big(\int_{a+p^n\mathbf{Z}_p} (\frac{x-a}{p^n})^k\,\mu\Big) + rn\Big),$$

alors $v_{\mathscr{D}_r}(\mu)$ est une valuation sur $\mathscr{D}_r(\mathbf{Z}_p, L)$ équivalente à la valuation $v'_{\mathscr{D}_r}$.

Démonstration. — C'est une conséquence immédiate du th. 2.4 et du théorème de l'image ouverte.

Exercice 15. — (i) Montrer que, si $N \in \mathbf{N}$ est $\geqslant [r]$, et si

$$v_{\mathscr{D}_r,N}(\mu) = \inf_{a\in\mathbf{Z}_p,\, k\leqslant N,\, n\in\mathbf{N}} \Big(v_p\Big(\int_{a+p^n\mathbf{Z}_p} (\frac{x-a}{p^n})^k\,\mu\Big) + rn\Big),$$

alors $v_{\mathscr{D}_r,N}(\mu)$ est une valuation sur $\mathscr{D}_r(\mathbf{Z}_p, L)$ équivalente à la valuation $v'_{\mathscr{D}_r}$.

(ii) Montre que, si $N \in \mathbf{N}$ est $\geqslant [r]$, et si

$$v'_{\mathscr{D}_r,N}(\mu) = \inf_{a\in\mathbf{Z}_p,\, n\in\mathbf{N}} \Big(v_p\Big(\int_{a+p^n\mathbf{Z}_p} (\frac{x-a}{p^n})^N\,\mu\Big) + rn\Big),$$

alors $v'_{\mathscr{D}_r,N}(\mu)$ est une valuation sur $\mathscr{D}_r(\mathbf{Z}_p, L)$ équivalente à la valuation $v_{\mathscr{D}_r,N}$.

2.3. Opérations sur les distributions

2.3.1. Masses de Dirac. — si $a \in \mathbf{Z}_p$, soit δ_a la masse de Dirac en a, c'est-à-dire la mesure qui à ϕ associe $\phi(a)$. Sa transformée d'Amice est $(1+T)^a$; en particulier $\mathscr{A}_{\delta_0} = 1$.

Comme les polynômes sont denses dans $\mathscr{R}_L^+$, et $\mathscr{R}_{L,r}^+$, si $r \geqslant 0$, 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 $\mathscr{D}(\mathbf{Z}_p, L)$ et $\mathscr{D}_r(\mathbf{Z}_p, L)$, si $r \geqslant 0$.

2.3.2. Multiplication par une fonction. — Si μ est une distribution sur $\mathbf{Z}_p$ et f est une fonction localement analytique sur $\mathbf{Z}_p$, on définit la distribution $f\mu$ par la formule $\int_{\mathbf{Z}_p} \phi\,(f\mu) = \int_{\mathbf{Z}_p} (f\phi)\,\mu$. On peut de même multiplier une mesure par une fonction continue ou, plus généralement, une distribution d'ordre r par une fonction de classe $\mathscr{C}^r$.

• 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

$$\mathscr{A}_{x\mu}(T) = (1+T)\frac{d}{dT}\mathscr{A}_\mu(T).$$

Cette formule est plus agréable sur la *transformée de Laplace* $\mathscr{L}_\mu$ de μ : c'est la série entière définie par

$$\mathscr{L}_\mu(t) = \mathscr{A}_\mu(e^t - 1) = \int_{\mathbf{Z}_p} e^{tx}\,\mu.$$

Comme $(1+T)\frac{d}{dT} = \frac{d}{dt}$, on obtient,

$$\int_{\mathbf{Z}_p} x^n e^{tx}\,\mu = (\frac{d}{dt})^n\mathscr{L}_\mu(t), \quad \text{et} \quad \int_{\mathbf{Z}_p} x^n\,\mu = (\frac{d}{dt})^n\mathscr{L}_\mu(t)_{|t=0}.$$

• Multiplication par z^x si $v_p(z-1)>0$. D'après le lemme 2.1, si $v_p(y-1)>0$, et si λ est une distribution continue 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 $y\in D(0,0^+)$. On en déduit la formule

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

• Division par x. Le résultat n'est bien défini qu'à addition d'un multiple de la masse de Dirac en 0. La transformée d'Amice de $x^{-1}\mu$ est alors une primitive de $(1+T)^{-1}\mathscr{A}_\mu(T)$, le choix de la constante d'intégration correspondant à l'indétermination mentionnée ci-dessus.

Exercice 16. — (i) Soit μ une mesure sur $\mathbf{Z}_p$ telle que $v_{\mathscr{D}_0}(\mu)\geqslant 0$. Montrer que, si $k\geqslant 1$, et si n_1,n_2 sont deux entiers $\geqslant k$ vérifiant $n_1\equiv n_2 \bmod (p-1)p^{k-1}$, alors $v_p(\int_{\mathbf{Z}_p} x^{n_1}\mu-\int_{\mathbf{Z}_p} x^{n_2}\mu)\geqslant k$.

(ii) Soit $F\in\mathbf{Z}_p[[T]]$, et soit $f(t)=F(e^t-1)=\sum_{n=0}^{+\infty}a_n\frac{t^n}{n!}\in\mathbf{Q}_p[[t]]$. Montrer que, si $k\geqslant 1$, et si n_1,n_2 sont deux entiers $\geqslant k$ vérifiant $n_1\equiv n_2 \bmod (p-1)p^{k-1}$, alors $v_p(a_{n_1}-a_{n_2})\geqslant k$ (congruences de Kummer).

2.3.3. 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

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

Si $k\geqslant 1$ et $F\in\mathscr{R}_L^+$, notons $\partial^{-k}F$ une solution G de l'équation différentielle $\partial^k G=F$, ce qui fait que $\partial^{-k}F$ n'est bien déterminé qu'à addition près d'un polynôme de degré $\leqslant k-1$ en $\log(1+T)$.

Proposition 2.6. — *Soient $n\in\mathbf{N}$, $b\in\mathbf{Z}_p$ et $k\in\mathbf{Z}$. On a alors*

$$\int_{b+p^n\mathbf{Z}_p}x^k\,\mu=p^{-n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{-b}\partial^k\mathscr{A}_\mu(\eta-1),$$

si $k\geqslant 0$ ou si $k\leqslant -1$ et $b\notin p^n\mathbf{Z}_p$.

Démonstration. — C'est une conséquence immédiate des discussions précédentes. Si $k\leqslant -1$, l'indépendance du membre de droite par rapport au choix de $\partial^k\mathscr{A}_\mu$ suit de ce que $\log\eta=0$ si $\eta\in\boldsymbol{\mu}_{p^n}$ et de ce que $\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{-b}=0$ si $b\notin p^n\mathbf{Z}_p$.

Exercice 17. — On définit les polynômes de Bernoulli $B_k(X)$, $k\in\mathbf{N}$, par la formule

$$\frac{te^{tX}}{e^t-1}=\sum_{k=0}^{+\infty}B_k(X)\frac{t^k}{k!}.$$

On a en particulier $B_0(X)=1$, $B_1(X)=X-\frac12$.

(i) Montrer que, si $k\geqslant 1$, alors B_k est l'unique polynôme de degré k vérifiant

$$B_k(X+1)-B_k(X)=kX^{k-1}\quad\text{et}\quad\sum_{i=0}^{d-1}B_k(X+i/d)=d^{1-k}B_k(dX),\ \text{si } d\geqslant 1.$$

(ii) Si $x \in \mathbf{Q}_p$, on définit $\{x\}$ comme l'unique élément de $\mathbf{Z}[\frac{1}{p}] \cap [0,1[$ tel que $x - \{x\} \in \mathbf{Z}_p$. Montrer que, si $a \in \mathbf{Z}_p^*$, il existe une unique mesure μ_a telle que, quels que soient $n \in \mathbf{N}$, et $i \in \mathbf{Z}_p$, on ait

$$\mu_a(i + p^n\mathbf{Z}_p) = B_1\big(\{\frac{i}{p^n}\}\big) - aB_1\big(\{\frac{a^{-1}i}{p^n}\}\big).$$

(iii) Montrer que, si $a \in \mathbf{Z}_p^*$, il existe une mesure λ_a de transformée d'Amice $\frac{1}{T} - \frac{a}{(1+T)^a-1}$.

(iv) Montrer que $\lambda_a = \mu_a$.

(v) Montrer que, quel que soient $k \in \mathbf{N}$, $n \in \mathbf{N}$, et $i \in \mathbf{Z}_p$, on a

$$\int_{i+p^n\mathbf{Z}_p} x^k\,\mu_a = \frac{p^{nk}}{k+1}\Big(B_{k+1}\big(\{\frac{i}{p^n}\}\big) - a^{k+1}B_{k+1}\big(\{\frac{a^{-1}i}{p^n}\}\big)\Big).$$

(vi) Exprimer $\int_{\mathbf{Z}_p^*} x^k\,\mu_a$ en termes du nombre de Bernoulli $B_k(0)$. En déduire l'existence de congrences (de Kummer) entre les nombres de Bernoulli.

2.3.4. Dérivée d'une distribution. — Si $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$, on définit sa dérivée $\mathrm{d}\mu$ par :

$$\int_{\mathbf{Z}_p} \phi(x)\,\mathrm{d}\mu = \int_{\mathbf{Z}_p} \phi'(x)\,\mu \quad \text{et donc} \quad \mathscr{A}_{\mathrm{d}\mu}(T) = \log(1+T)\cdot\mathscr{A}_\mu(T).$$

On remarquera qu'en p-adique, il n'est en général pas possible de définir la primitive d'une distribution, car au niveau des transformées d'Amice, cette opération correspondrait à la division par $\log(1+T)$, mais cette série a une infinité de zéro sur $D(0,0^+)$.

2.3.5. Actions de $\mathbf{Z}_p^*$, φ et ψ. — Ces actions permettent de faire le lien entre la théorie des (φ,Γ)-modules et celles des distributions.

- On fait agir $a \in \mathbf{Z}_p^*$ sur une distribution μ par :

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

et donc $\mathscr{A}_{\mu\star a} = \mathscr{A}_\mu \star a$.

- On fait agir φ sur une distribution μ par :

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

- Si μ est une distribution sur $\mathbf{Z}_p$, on note $\psi(\mu)$ la distribution 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 $\mathscr{A}_{\psi(\mu)} = \psi(\mathscr{A}_\mu)$.

Les actions de $\mathbf{Z}_p^*$, φ et ψ vérifient les relations suivantes :

(a) $\psi\circ\varphi = \mathrm{id}$;

(b) $\psi(\mu)\star a = \psi(\mu\star a)$ et $\varphi(\mu)\star a = \varphi(\mu\star a)$, si $a \in \mathbf{Z}_p^*$.

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

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

Exercice 18. — Montrer que, si $\mu \in \mathscr{D}_0(\mathbf{Z}_p, L)$, alors

$$v_{\mathscr{D}_0}(\mu \star a) = v_{\mathscr{D}_0}(\mu), \quad v_{\mathscr{D}_0}(\varphi(\mu)) = v_{\mathscr{D}_0}(\mu) \quad \text{et} \quad v_{\mathscr{D}_0}(\psi(\mu)) \geqslant v_{\mathscr{D}_0}(\mu).$$

2.3.6. Convolution des distributions. — Si λ et μ sont deux distributions, on définit leur convolée $\lambda * \mu$ par

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

En prenant pour ϕ la fonction $x \mapsto z^x$, avec $v_p(z-1) > 0$, on démontre que l'on a $\mathscr{A}_{\lambda*\mu}(z) = \mathscr{A}_\lambda(z)\mathscr{A}_\mu(z)$ quel que soit $z \in D(0, 0^+)$, et donc que $\mathscr{A}_{\lambda*\mu} = \mathscr{A}_\lambda \mathscr{A}_\mu$.

Pour donner un sens à l'intégrale double ci-dessus, nous aurons besoin du lemme suivant.

Lemme 2.7. — *Si $\phi \in \mathrm{LA}_h(\mathbf{Z}_p, L)$, alors la dérivée n-ième de ϕ appartient à $\mathrm{LA}_h(\mathbf{Z}_p, L)$. De plus, $v_{\mathrm{LA}_h}\big(\frac{p^{nh}\phi^{(n)}}{n!}\big) \geqslant v_{\mathrm{LA}_h}(\phi)$ quel que soit $n \in \mathbf{N}$ et la suite de terme général $v_{\mathrm{LA}_h}\big(\frac{p^{nh}\phi^{(n)}}{n!}\big)$ tend vers $+\infty$ quand n tend vers $+\infty$.*

Démonstration. — Soit S un système de représentants de $\mathbf{Z}_p$ modulo $p^h\mathbf{Z}_p$. Si $x_0 \in S$, alors $\frac{p^{nh}\phi^{(n)}(x)}{n!} = \sum_{k=0}^{+\infty} \binom{n+k}{n} a_{n+k}(\phi, x_0)(\frac{x-x_0}{p^h})^k$. Comme $\binom{n+k}{n}$ est entier, on en déduit l'inégalité

$$v_{D(x_0,h)}\big(\frac{p^{nh}\phi^{(n)}}{n!}\big) \geqslant \inf_{k\geqslant n} v_p(a_k(\phi, x_0)) \geqslant \inf_{k\geqslant 0} v_p(a_k(\phi, x_0)) \geqslant v_{D(x_0,h)}(\phi).$$

On en déduit la minoration voulue, et le fait que la suite de terme général $v_{\mathrm{LA}_h}\big(\frac{p^{nh}\phi^{(n)}}{n!}\big)$ tend vers $+\infty$ est une conséquence du fait que la suite $v_p\big(a_k(\phi, x_0)\big)$ tend vers $+\infty$.

Pour prouver que l'intégrale double définissant $\lambda * \mu$ converge, il suffit d'écrire $\phi(x+y)$, pour $x \in x_0 + p^h\mathbf{Z}_p$, sous la forme

$$\phi(x+y) = \sum_{n=0}^{+\infty} \frac{p^{nh}\phi^{(n)}(x_0+y)}{n!} (\frac{x-x_0}{p^h})^n.$$

Comme $v_p\big(\int_{x_0+p^h\mathbf{Z}_p} \big(\frac{x-x_0}{p^h}\big)^n \lambda\big) \geqslant v_{\mathrm{LA}_h}(\lambda)$, la série

$$\sum_{x_0\in S} \sum_{n=0}^{+\infty} \Big(\int_{x_0+p^h\mathbf{Z}_p} (\frac{x-x_0}{p^h})^n\ \lambda\Big) \cdot \frac{p^{nh}\phi^{(n)}(x_0+y)}{n!}$$

converge dans $\mathrm{LA}_h(\mathbf{Z}_p, L)$ d'après le lemme 2.7, ce qui permet de conclure.

Proposition 2.8. — (i) *La convolée de deux mesures est une mesure.*

(ii) *Plus généralement, si λ est d'ordre r et μ est d'ordre s, alors $\lambda * \mu$ est d'ordre $r+s$.*

Démonstration. — C'est, modulo le lemme 1.15 et la formule $v_{D(0,v_h)}(fg) = v_{D(0,v_h)}(f) + v_{D(0,v_h)}(g)$, immédiat sur les transformées d'Amice.

Remarque 2.9. — 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 $\mu = 0$. Il n'y a donc pas de distribution continue sur $\mathbf{Z}_p$, invariante par translation ; autrement dit, *il n'y a pas de mesure de Haar p-adique.*

Exercice 19. — Si $\phi \in \mathrm{LA}(\mathbf{Z}_p, L)$ et si $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$, on définit la fonction $\mu * \phi : \mathbf{Z}_p \to L$ par la formule

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

(i) Montrer que, $\mu * \phi \in \mathrm{LA}(\mathbf{Z}_p, L)$, et que, si $\lambda \in \mathscr{D}(\mathbf{Z}_p, L)$, alors

$$\int_{\mathbf{Z}_p} (\mu * \phi)\, \lambda = \int_{\mathbf{Z}_p} \phi\, (\lambda * \mu).$$

(ii) Soit $\mu_{\mathrm{KL}} \in \mathscr{D}(\mathbf{Z}_p, L)$ dont la transformée d'Amice est $\frac{\log(1+T)}{T}$ et, si $\phi \in \mathrm{LA}(\mathbf{Z}_p, L)$, soit $\tilde{\phi} = \mu_{\mathrm{KL}} * \phi$. Montrer que l'on a $\tilde{\phi}(x+1) - \tilde{\phi}(x) = \phi'(x)$, quel que soit $x \in \mathbf{Z}_p$.

(iii) Si $z \in \mathbf{C}_p - \mathbf{Z}_p$, soit $G_p(z) = \int_{\mathbf{Z}_p} ((x+z)\log(x+z) - (x+z))\ \mu_{\mathrm{KL}}(x)$ (où l'on a choisi une branche du logarithme sur $\mathbf{C}_p^*$). Montrer que G_p est une fonction localement analytique sur $\mathbf{C}_p - \mathbf{Z}_p$, et que l'on a $G_p(z+1) - G_p(z) = \log z$, quel que soit $z \in \mathbf{C}_p - \mathbf{Z}_p$.

(iv) Montrer que $G_p(z) + G_p(1-z) = 0$ quel que soit $z \in \mathbf{C}_p - \mathbf{Z}_p$. (On pourra commencer par montrer que $\int_{\mathbf{Z}_p} \phi\, \mu_{\mathrm{KL}} = \lim_{n\to+\infty} p^{-n} \sum_{i=0}^{p^n-1} \phi(i)$, si $\phi \in \mathrm{LA}(\mathbf{Z}_p, L)$.)

(v) Dans cette question, on suppose que $\log p = 0$. Soit $H_p : \mathbf{Z}_p \to L$, définie par $H_p(x) = \sum_{0\leqslant i<p,\, p\nmid x+i} G_p(\frac{x+i}{p})$. Montrer que H_p est une fonction localement analytique sur $\mathbf{Z}_p$, et que l'on a $H_p(n) = \log(\Gamma^*(n))$, avec $\Gamma^*(n) = \prod_{1\leqslant i\leqslant n-1,\, p\nmid n} i$, quel que soit $n \in \mathbf{N}$. (La fonction G_p est la *fonction log gamma* de Diamond.)

Exercice 20. — Si X est un fermé de $\mathbf{Z}_p$, une distribution μ sur $\mathbf{Z}_p$ est *à support dans* X, si on a $\int_{\mathbf{Z}_p} \phi\, \mu = 0$ pour tout $\phi \in \mathrm{LA}(\mathbf{Z}_p, L)$ nulle dans un ouvert contenant X.

(i) Montrer que, si $r \geqslant 0$, une distribution d'ordre r, à support dans $\{0\}$ est une combinaison linéaire des dérivées $\mathrm{d}^i\delta_0$, $i \leqslant r$, de la masse de Dirac en 0.

(ii) Montrer que, si a_n, $n \in \mathbf{N}$, est une suite d'éléments de L telle que la série $\sum_{n=0}^{+\infty} a_n X^n$ converge sur tout $\mathbf{C}_p$, alors la série $\sum_{n=0}^{+\infty} a_n \mathrm{d}^n\delta_0$ converge dans $\mathscr{D}(\mathbf{Z}_p, L)$ vers une distribution de support $\{0\}$.

(iii) Montrer que, réciproquement, si $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$ est une distribution de support $\{0\}$, il existe une suite d'éléments de L telle que la série $\sum_{n=0}^{+\infty} a_n X^n$ converge sur tout $\mathbf{C}_p$ et telle que $\mu = \sum_{n=0}^{+\infty} a_n \mathrm{d}^n\delta_0$.

Pierre Colmez