École Normale Supérieure de Rennes

Rapport de stage 1A

Introduction aux L fonctions p-adiques

Antoine Meddane Cauchy

Encadré par *Denis Benoit*

17 Mai 2016 — 10 Juillet 2016

Table des matières

Introduction

Cet article traite principalement de la construction des L fonctions p-adiques par une méthode dite d'interpolation.
Historiquement, la théorie algébrique des nombres a pris son essence dans les travaux de Pierre de Fermat, et plus précisément dans son célèbre dernier théorème. Mais cette théorie s'est réellement développée seulement à partir de 1801 grâce au mathématicien Carl Friedrich Gauss dans son livre intitulé *Disquisitiones Arithmeticae*, qui a permis d'ouvrir la voie à d'autres mathématiciens. Un grand acteur et un pionnier de cette théorie récente fut Ernst Kummer qui, dans un article publié en 1857, réussi a résoudre un cas particulier de l'hypothèse de Fermat (pour p premier régulier) en introduisant le concept de nombre idéaux. L'idée principal fut de transporter le théorème fondamental de l'arithmétique dans des corps de nombres *i.e des extensions finies de* $\mathbb{Q}$. Egalement, le théorème de Kronecker-Weber, énonçant que toute extension abélienne de $\mathbb{Q}$ (*i.e de groupe de Galois abélien*) est inclus dans une extension cyclotomique, nous invite à regarder un certain type de corps de nombre, que sont les corps cyclotomiques.
A la fin de XIX^{eme} siècle, une nouvelle théorie à vue le jour, celle des nombres p-adiques. Plus précisément, c'est dans un article publié en 1897, que le mathématicien Kurt Hensel, donna pour la première fois une définition des nombres p-adiques. La première motivation de telle structure algébrique a été celle généralisée plus tard pour les corps locaux, qui est d'utiliser les techniques des séries entières en théorie des nombres. Aujourd'hui, la théorie des nombres p-adiques dépassent largement ce cadre et peut-être vue comme un monde parallèle au monde réel (associé à $\mathbb{R}$). Cette dichotomie entre le monde réel et p-adique a été révélée grâce au théorème d'Ostrowsky. Cependant, contrairement à $\mathbb{R}$, le corps des nombres p-adiques $\mathbb{Q}_p$ (où p est nombre premier quelconque) possède une topologie totalement dicrète, au sens que les composantes connexes sont réduites aux singletons. Ceci laisse tendre à penser que les théorèmes homologues p-adiques seront des versions algébriques de leur semblable réel, comme par exemple la substitution du théorème de prolongement analytique par le théorème de préparation de Weierstass.
Les L fonctions, qui sont des généralisations de la fonction Zêta, sont des outils au cœur de l'arithmétique. Il est donc légitime de construire leur homologue p-adique. De manière surprenante, les L fonctions p-adiques ressemblent bien plus à leur homologue définit dans $\mathbb{C}$ que ce dont laissait imaginer leur construction. Et, comble de l'imagination, les L fonctions p-adiques recèlent une mine d'information arithmétique bien plus importante que les L fonctions classiques, notamment en ne décrivant non plus seulement les cardinaux des groupes de classes mais en décrivant la structure algébrique d'un objet similaire, purement arithmétique.

La section 1 est fondamentale, elle introduit les concepts à savoir sur les nombres p-adiques (même si certains résultats sont assez anecdotiques). La section 2 est la moins importante de ce rapport, elle donne une construction peu généralisable. Cependant, certains résultats fondamentaux y ont été introduits. La section 3 ne sert qu'à la compréhension de la section 4 dans laquelle se trouve une jolie construction des L fonctions p-adiques.

1 A propos des nombres p-adiques

1.1 Corps normés, Corps valués

Dans cette partie, nous allons introduire quelques résultats généraux sur les corps normés et valués qui nous serviront par la suite.

1.1.1 Corps normés

Définition 1.1.1. *(Corps normé)*
Soit K un corps. Une norme sur K est une application qui à tout $x \in K$ associe un réel positif $|x|$ de telle sorte que, pour tous x et y de K :
- $|x| = 0 \Leftrightarrow x = 0_K$ *(axiome de séparation)*
- $|xy| = |x||y|$
- $|x + y| \leq |x| + |y|$

Une norme sur K est dite ultramétrique si elle vérifie la condition suivante :
- *pour tous x et y de K, $|x + y| \leq max\{|x|, |y|\}$*

La similarité avec la définition d'une norme d'espace vectoriel vient du fait qu'un corps peut être vu comme un espace vectoriel sur lui-même.
La proposition suivante est une caractérisation des normes ultramétriques.

Proposition 1.1.1. *Soit K un corps et $|.|$ une norme sur K. Les conditions suivantes sont équivalentes :*
(i) $|.|$ *est ultramétrique*
(ii) $|.|$ *est bornée sur* $\mathbb{Z}$
(iii) $\forall x \in \mathbb{Z}, |x| \leq 1$

Démonstration. On a de manière évidente $(i) \Rightarrow (iii) \Rightarrow (ii)$ comme $|1| = 1$.
Montrons que $(ii) \Rightarrow (i)$. Soit $x, y \in K$ tel que $|x| \leq |y|$,
$|.|$ est bornée sur $\mathbb{Z}$ donc $\exists M \in \mathbb{R}_+$ tel que $\forall x \in \mathbb{Z}, |x| \leq M$. Or,

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Donc, par inégalité triangulaire $|x+y|^n \leq M(n+1)|y|$, et donc en prenant la racine n-ième, puis la limite quand n tend vers $+\infty$, on obtient le résultat. □

Corollaire 1.1.1. *Toute norme sur un corps de caractéristique $p \neq 0$ est ultramétrique.*

Exemple 1.1.1.
1. *<u>Norme triviale</u> : On peut munir un corps K d'une norme dite triviale définie par $|x| = 1, \forall x \in K^*$*
2. *<u>Norme induite</u> : Soit L un sous-corps d'un corps normé K, on peut munir L de la norme définie sur K restreinte à L.*
3. *<u>Norme sur $\mathbb{C}$</u> : Le module définie sur $\mathbb{C}$ définie une norme sur $\mathbb{C}$.*

Une norme sur un corps K induit une distance qui induit une topologie sur K. Regardons à présent quelques propriétés topologique des corps ultramétriques.

Lemme 1.1.1. *Si K est un corps muni d'une norme ultramétrique $|.|$. soient $x, y \in K$ tels que $|x| \neq |y|$, alors $|x+y| = \sup(|x|, |y|)$.*

Démonstration. On a $|x+y| \leq \sup(|x|, |y|)$ par propriété de la norme ultramétrique. On peut supposer $|x| < |y|$ quitte à permuter x et y. Or $|y| = |(x+y) - x| \leq \sup(|x+y|, |x|)$, donc $|x+y| = |y|$. □

1.1.2 Corps valués

Définition 1.1.2. *(Corps valué)*
Soit K un corps. Une valuation sur K est une application de K dans $\mathbb{R} \cup \{+\infty\}$, $x \mapsto v(x)$ qui vérifie :
- $v(x) = +\infty \Leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x+y) \geq \inf\{v(x), v(y)\}$

Remarque 1.1.1. *Soit K un corps muni d'une valuation v, si $0 < \lambda < 1$ alors $|.| : x \mapsto \lambda^{-v(x)}$ définit une norme ultramétrique sur K.*
Réciproquement, si K est un corps muni d'une norme ultramétrique $|.|$. Alors, si $\lambda < 0$, $v : x \mapsto \lambda \log |x|$ définie une valuation sur K.
Par conséquent, il résulte du lemme 1.1.1 que si $v(x) \neq v(y)$ alors $v(x+y) = \inf(v(x), v(y))$.

Définition 1.1.3. *On dit qu'une valuation est discrète si $v(K^*)$ est un sous-groupe discret de $\mathbb{R}$ (i.e de la forme $a\mathbb{Z}$), et qu'elle est normalisée si $v(K^*) = \mathbb{Z}$.*

Soit K est un corps valué discret muni d'une valuation v. Si v est normalisée, un élément $\pi \in \mathscr{O}^*$ tel que $v(\pi) = 1$ est appelée uniformisante et tout élément $x \in \mathbb{K}^*$ se décompose de manière unique sous la forme $x = up^n$ où $u \in \mathscr{O}^*$ et $n \in \mathbb{Z}$.

On peut constater qu'il y a équivalence entre les notions de corps ultramétriques et de corps valués.

Définition 1.1.4. *(Norme sur $\mathbb{Q}$)*
Si $n \in \mathbb{N}$, on définit la valuation p-adique de n, $v_p(n)$, comme étant la plus grande puissance de p qui divise n. Si $r = \frac{a}{b} \in \mathbb{Q}$, on définit la valuation p-adique de r par : $v_p(r) = v_p(a) - v_p(b)$.

On peut remarquer que la définition de la valuation p-adique d'un nombre rationel ne dépend pas du représentant (ce qui est nécessaire à la définition de v_p sur $\mathbb{Q}$).

Proposition 1.1.2. *$|.|_p : \mathbb{Q} \to \mathbb{R}_+, x \mapsto p^{-v_p(x)}$ définit une norme ultramétrique sur $\mathbb{Q}$, appelée norme p-adique.*

Démonstration. La preuve repose principalement sur la décomposition en facteurs premiers. □

Nous allons fournir quelques exemples fondamentaux de valuations que l'on utilisera fréquemment dans la partie 3 ou bien dans l'étude des extension finie de $\mathbb{Q}_p$.

Exemple 1.1.2. *Soit K un corps, on peut munir $K(X)$, le corps des fractions rationnelles à coefficients dans K, d'une valuation $val_X : \frac{P}{Q} \mapsto val_X(P) - val_X(Q)$ où $P, Q \in K[X], Q \neq 0$ et telle que $\forall P \in K[X], val_X(P) = \inf\{n \in \mathbb{N} \mid P^{(n)}(0) \neq 0\}$ où $P^{(n)}$ est la dérivée n-ième algébrique de P.*

Définition 1.1.5. *(Norme de Gauss)*
Soit K un corps ultramétrique muni d'une norme $|.|$. Soit $P \in K[X]$, on définit la norme de Gauss $|.|_G$ de $P(X) = \sum_{i=0}^{n} a_i X^i$ par $|P|_G = \sup(|a_0|, ..., |a_n|)$

Lemme 1.1.2. *Si P et Q sont deux éléments de $K[X]$, alors $|PQ|_G = |P|_G|Q|_G$*

Démonstration. La norme de Gauss étant ultramétrique, l'inégalité $|PQ|_G \leq |P|_G|Q|_G$ est évidente.
Montrons l'autre sens de l'inégalité. Posons $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{i=0}^{m} b_i X^i$, soit $i_0 = \inf\{i||a_i| = |P|_G\}$ et $j_0 = \inf\{j||b_j| = |Q|_G\}$. Soit $k_0 = i_0 + j_0$, alors $PQ(X) = \sum_{k=0}^{m+n} c_k X^k$, où

$$c_{k_0} = a_{i_0} b_{j_0} + \sum_{i<i_0} a_i b_{k_0-i} + \sum_{j<j_0} a_{k_0-j} b_j$$

avec $a_k = 0$ si $k > n$ et $b_k = 0$ si $k > m$. Donc, d'après le lemme 1.1.1 $|c_{k_0}| = |P|_G|Q|_G$ car tous les autres termes sont de norme strictement inférieurs. D'où le résultat. □

De plus, on peut prolonger $|.|_G$ sur $K(X)$ de manière évidente. Le seul axiome non trivial à vérifier à été prouver dans le lemme précédent. Il nous reste juste à montrer que la norme de Gauss est ultramétrique sur $K(X)$. Il suffit de montrer que si $f = \frac{P}{Q} \in K(X)$ tel que $|f|_G \leq 1$ alors $|f+1|_G \leq 1$. Quitte à diviser P et Q par un élément de norme $|Q|_G$, on peut supposer $|Q|_G = 1$, et se ramener à montrer que si $|P|_G \leq 1$ alors $|P+Q|_G \leq 1$ ce qui est immédiat. Donc $|.|_G$ définit bien une norme ultramétrique sur $K(X)$.

1.1.3 Propriétés topologiques

Définition 1.1.6. *Deux normes sur un corps K sont dites équivalentes si elles définissent la même topologie.*

Proposition 1.1.3. *Soit K un corps. Deux normes $|.|_1$ et $|.|_2$ sont équivalentes si et seulement si il existe $s \in \mathbb{R}_+^*$ tel que $|x|_1 = |x|_2, \forall x \in K$*

Démonstration. Soit $|.|$ une norme sur K. Alors on a $x^n \underset{n\to+\infty}{\longrightarrow} 0$ ssi $|x| < 1$. Donc, si $|.|_1$ et $|.|_2$ sont équivalentes, alors

$$\{x \in K||x|_1 < 1\} = \{x \in K||x|_2 < 1\}$$

. Si ce dernier ensemble est réduit à $\{0\}$, alors $|x|_1 = |x|_2 = 1, \forall x \in K^*$. Sinon, soit $x \in K^*$ tel que $|x|_1 < 1$, alors $\forall y \in K^*, \forall a \in \mathbb{Z} et b \in \mathbb{N}$ on a :

$$|y^b x^{-a}|_1 < 1 \Leftrightarrow |y^b x^{-a}|_2 < 1$$

Donc

$$\{r \in \mathbb{Q} | r < \frac{\log |y|_1}{\log |x|_1}\} = \{r \in \mathbb{Q} | r < \frac{\log |y|_2}{\log |x|_2}\}$$

Donc les réels $\frac{\log |y|_1}{\log |x|_1}$ et $\frac{\log |y|_2}{\log |x|_2}$ définissent la même coupure de Dedekind, donc sont égaux. On conclut que $x \longmapsto \frac{\log |x|_1}{\log |x|_2}$ est constante sur K^*, d'où le résultat. □

Théorème 1.1.1. *(Ostrowsky)*
Une norme sur Q est équivalente soit à la norme triviale, soit à la norme usuelle $|.|_{+\infty}$ ou soit à la norme $|.|_p$ pour un nombre premier p.

Démonstration. Soit $|.|$ une norme non triviale sur $\mathbb{Q}$. Supposons tout d'abord qu'il existe $k \in \mathbb{N}$ tel que $|k| > 1$. Or $|1| = 1$, donc par inégalité triangulaire on a $|k| \leq k$. Donc il existe $\alpha \in]0, 1]$ tel que $|k| = k^\alpha$. L'idée ensuite va être de montrer que $|m| = m^\alpha, \forall m \in \mathbb{N}$. Pour cela, effectuons une décomposition en base k. Soit $m = \sum_{i=0}^{n} a_i k^i$, où $a_i \in \{0, ..., k-1\} \forall i$, et $a_n \neq 0$. On a, comme $k^n \leq m$,

$$|m| \leq (k-1) \sum_{i=0}^{n} |k|^i \leq \frac{(k-1)}{k^\alpha - 1}(k^{\alpha(n+1)} - 1) \leq \frac{k(k-1)}{k^\alpha - 1} k^{\alpha n} \leq C m^\alpha$$

où $C = \frac{k(k-1)}{k^\alpha - 1}$. En remplaçant m par m^s, où $s \in \mathbb{N}$, en prenant la racine s-ième puis la limite quand s tend vers $+\infty$, on obtent l'inégalité $|m| \leq m^\alpha$. Pour montrer l'inégalité dans l'autre sens, nous allons raisonner par symétrie.
Supposons $|m| > 1$, alors par le même raisonnement que précédemment en inversant les rôles de k et m, on ontient que $\frac{\log |m|}{\log m} = \frac{\log |k|}{\log k}$ et donc que $|m| = m^\alpha$.
Supposont $|m| \leq 1$, alors $\exists l \in \mathbb{N}$ tel que $|k^l m| > 1$. Donc, en appliquant le résultat à $k^l m$ on obtient finalement que $|m| = m^\alpha, \forall m \in \mathbb{N}$. Or une norme étant à valeur positive et par multiplicativité, on a $|-1| = 1$, ce qui nous donne l'égalité précédente sur $\mathbb{Z}$. Donc $\forall m \in \mathbb{Q}, |m| = |m|_\infty^\alpha$, en passant au corps des fractions. Et donc, d'après la proposition 1.1.3, $|.|$ est équivalente à $|.|_\infty$.
Supposons à présent que pour tous $k \in \mathbb{N}$, $|k| \leq 1$. Il existe un nombre premier p qui atteint $\sup\{|n|| \ \ |n| < 1, n \in \mathbb{N}\}$. Supposons qu'il existe un autre nombre premier q distinct de p tel que $|q| < 1$. Alors p^n et q^n sont premiers entre eux quelque soit $n \in \mathbb{N}$. Donc, d'après l'identité de Bézout, $\exists u, v \in \mathbb{N}$ tels que $p^n u + q^n v = 1$. Donc, par inégalité triangulaire, $1 \leq |p|^n + |q|^n, \forall n \in \mathbb{N}$, absurde. Donc, p est l'unique nombre premier à avoir une norme strictement inférieure à 1. En utilisant la décomposition en facteurs premiers, puis en étendant à $\mathbb{Z}$, et finalement à $\mathbb{Q}$, on obtient que $|.|$ est équivalente à la norme p-adique $|.|_p$. □

1.2 Construction de $\mathbb{Z}_p$ et $\mathbb{Q}_p$

1.2.1 Complétion

Si K est un corps normé, on notera $\widetilde{K}$ l'ensemble des suites de Cauchy de K.
On notera $I \subset \widetilde{K}$ l'ensemble des suite de Cauchy qui tendent vers 0.

Lemme 1.2.1. *(i) Si $(a_n) \in \widetilde{K}$, alors $(|a_n|)$ converge dans $\mathbb{R}_+$.*
(ii) Si $|.|$ est ultramétrique et $(a_n) \in \widetilde{K} \setminus I$, alors $(|a_n|)$ est constante à partir d'un certain rang.
(iii) Si $(a_n) \equiv (b_n) \mod I$, alors $\lim\limits_{n\to+\infty} |a_n| = \lim\limits_{n\to+\infty} |b_n|$.

Démonstration. (i) découle de l'inégalité triangulaire $|\ |a_{n+p}| - |a_n|\ | \leq |a_{n+p} - a_n|$, et de la complétude de $\mathbb{R}$
(ii) Si $(a_n) \in \widetilde{K} \setminus I$, alors $\exists \delta > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, |a_n| > \frac{2\delta}{3}$. Comme (a_n) est de Cauchy, $\exists n_1, \forall n \geq n_1, \forall p \in \mathbb{N}, |a_{n+p} - a_n| < \frac{2\delta}{3}$.
Donc $\forall n \geq n_2 = \max(n_0, n_1), \forall p \in \mathbb{N}, |a_{n+p} - a_n| < |a_n|$
Donc $\forall p \in \mathbb{N}, \forall n \geq n_2, |a_{n+p}| = |a_n|$.
(iii) est obtenue grâce à l'inégalité triangulaire $|\ |a_n| - |b_n|\ | \leq |a_n - b_n|$, et à $(a_n - b_n) \in I$. □

Lemme 1.2.2. *$\widetilde{K}$ est un anneau et I un idéal maximal de $\widetilde{K}$*

Démonstration. On montre sans difficultée que $\widetilde{K}$ est un anneau et I un idéal.
Si $(a_n) \in \widetilde{K} \setminus I$, alors $\lim\limits_{n\to+\infty} |a_n| = \alpha \in \mathbb{R}_+^*$. De plus, $\exists \delta > 0, \exists N \in \mathbb{N}, \forall n \geq N, |a_n| \geq \delta$, donc posons $b_n = a_n^{-1}$ si $n \geq N$ et $b_n = 0$ si $0 \leq n < N$. On a bien $(b_n) \in \widetilde{K}$ car $\forall n \geq N, \forall p \in \mathbb{N}, a_{n+p}^{-1} - a_n^{-1} = \frac{1}{a_n a_{n+p}}(a_n - a_{n+p})$, Donc $|a_{n+p}^{-1} - a_n^{-1}| \leq \frac{1}{\delta^2}|a_n - a_{n+p}|$. On a alors $(a_n)(b_n) - 1 \in I$, donc (a_n) est inversible dans $\widetilde{K}/I$. Donc $\widetilde{K}/I$ est un corps. □

Posons $\widehat{K} = \widetilde{K}/I$. Il résulte du lemme précédent que $\widehat{K}$ est un corps.

Proposition 1.2.1. *$|.|$ est une norme sur $\widehat{K}$, et $\widehat{K}$ est complet pour cette norme. De plus, K (identifié aux classes des suites constantes dans $\widehat{K}$) est dense dans $\widehat{K}$.*

Démonstration. L'inégalité triangulaire, ultramétrique et la multiplicativité de la norme passent bien à la limite. Egalement, on a pour $a \in \widehat{K}$, $|a| = 0 \leftrightarrow \lim\limits_{n\to+\infty} |a_n| = 0 \leftrightarrow a = 0$.
Donc $|.|$ est une norme sur $\widehat{K}$, ultramétrique si $|.|$ est ultramétrique sur K.
Soit $(a_n) \in \widehat{K}$, on a $|(a_n)_{n\in\mathbb{N}} - (a_p)_{n\in\mathbb{N}}| \leq \sup\limits_{n\geq 1} |a_{n+p} - a_p|$ qui tend vers 0 quand p tend vers $+\infty$ puisque la suite (a_n) est de Cauchy. Donc K est bien dense dans $\widehat{K}$.
Soit $(a^{(n)})_{n\in\mathbb{N}}$ une suite de Cauchy dans $\widehat{K}$. Comme K est dense dans $\widehat{K}$, $\forall n \in \mathbb{N}, \exists b_n \in K, |a^{(n)} - b_n| \leq 2^{-n}$. On a ainsi construit une suite (b_n) d'éléments de K. Montrons que cette suite est de Cauchy. On a $\forall n, p \in \mathbb{N}$,

$$|b_{n+p} - b_n| = |(b_{n+p} - a^{(n+p)}) + (a^{(n+p)} - a^{(n)}) + (a^{(n)} - b_n)| \leq 2^{-(n+p)} + |a^{(n+p)} - a^{(n)}| + 2^{-n}$$

qui tend bien vers 0 quand n tend vers $+\infty$, car $(a^{(n)})_{n\in\mathbb{N}}$ est de Cauchy. Donc (b_n) est une suite de Cauchy dans K, donc converge dans $\widetilde{K}$ et $\widehat{K}$, par définition. Finalement, $(a^{(n)})$ possède une limite dans $\widehat{K}$ égale à la limite de (b_n). Donc $\widehat{K}$ est complet. □

Définition 1.2.1. *Le corps $\widehat{K}$ muni de la norme $|.|$ s'appelle le complété de K pour la norme $|.|$.*

Exemple 1.2.1. *(i) $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la valeur absolue.*
(ii) $\mathbb{C}$ est le complété de $\mathbb{Q}(i)$ pour la norme $|.| : a + ib \mapsto \sqrt{a^2 + b^2}$.
(iii) Si K est un corps complet et L un sous-corps dense de K alors K est le complété de L pour la norme induite.
(iv) $K((X))$, corps des séries de Laurent à coefficients dans K, est le complété du corps des fractions rationnelles $K(X)$ pour la norme $|.|_X$.

Remarque 1.2.1. *On peut constater d'après le lemme 1.2.1 que si K est un corps muni d'une valuation v, alors $v(\widehat{K}^*) = v(K^*)$. En particulier, si K est un corps valué discret (i.e muni d'une valuation discrète) alors $\widehat{K}$ est également un corps valué discret.*

Définition 1.2.2. *Soit $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la norme p-adique. On appelle $\mathbb{Q}_p$ le corps des nombres p-adiques.*

Définitions 1.2.1. *(i) Un anneau local est un anneau commutatif possédant un unique idéal maximal*
(ii) Un anneau intègre $\mathscr{O}$ est un anneau de valuation si pour tous $x \in K = Frac(\mathscr{O})$, le corps des fractions de $\mathscr{O}$, on a $x \in \mathscr{O}$ où $x^{-1} \in \mathscr{O}$.

Définition 1.2.3. *Soit $\mathbb{K}$ un corps muni d'une norme ultramétrique $|.|$. On définit :*

$$\mathscr{O} := \{x \in K, v_p(x) \geq 0\}$$

$$\mathfrak{m} = \{x \in K, v_p(x) > 0\}$$

$$k = \mathscr{O}/\mathfrak{m}$$

On appelle $\mathscr{O}$ l'anneau des entiers ou l'anneau de valuation K, $\mathfrak{m}$ son unique idéal maximal et k le corps résiduel de K.

Remarque 1.2.2. *L'unicité de l'idéal maximal vient du fait que $\mathscr{O}$ est un anneau local. En effet, soit I un idéal de $\mathscr{O}$, supposons qu'il existe $x \in \mathscr{O}$ tel que $v_p(x) = 0$, alors x est inversible et $I = \mathscr{O}$, donc $I \subset \mathfrak{m}$.*
De plus, un anneau de valuation est toujours intégralement clos. En effet, soit $x \in K$ entier sur $\mathscr{O}$, alors il existe $n \in \mathbb{N}$ et $a_0, ..., a_{n-1} \in \mathscr{O}$ tels que

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$$

Supposons $x \notin \mathscr{O}$, alors $x^{-1} \in \mathscr{O}$ et donc $x = -a_{n-1} - ... - a_0(x^{-1})^{n-1} \in \mathscr{O}$, ce qui est absurde.

Définition 1.2.4. *On appelle $\mathbb{Z}_p$ l'anneau des entiers de $\mathbb{Q}_p$.*

On peut remarquer de manière assez évidente que $\mathbb{Z}_p$ est l'anneau des entiers de $\mathbb{Q}_p$ puisque $\mathbb{Z}$ est l'anneau des entiers de $\mathbb{Q}$.

1.2.2 Autres définitions de $\mathbb{Z}_p$ et $\mathbb{Q}_p$

Dans ce paragraphe, nous allons donner quelques définitions équivalentes de $\mathbb{Z}_p$ et $\mathbb{Q}_p$, afin d'avoir une compréhension plus étaillée de ces objets abstraits. Commençons par donner une définition de $\mathbb{Z}_p$ en terme de limite projective.

Définition 1.2.5. *(Groupe profini)*
Un groupe profini est un groupe topologique G qui est compact (et séparé) et a une base de voisinnages ouverts de 1 constitués de sous-groupes distingués.

La définition suivante est celle de limite projective dans la catégorie des ensembles. Cette définition peut-être facilement adaptée aux catégories des groupes et anneaux, etc.

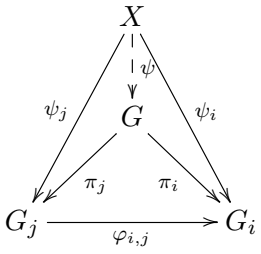
Définition 1.2.6. *Un ensemble dirigé I est un ensemble ordonné tel que $\forall i, j \in I, \exists k \in I, i, j \leq k$*
Un système projectif d'ensembles sur un ensemble dirigé I est une famille

$$\{G_i, \varphi_{i,j} \mid i, j \in I, i \leq j\}$$

où $(G_i)_{i\in I}$ est une famille d'ensemble et $(\varphi_{i,j})_{i\leq j}$ est une famille d'application vérifiant : $\varphi_{i,j} : G_j \mapsto G_i$ et si $i, j, k \in I$ tels que

1. *$\varphi_{i,i} = Id_{G_i}, \forall i \in G_i$*
2. *Si $i \leq j \leq k$, alors $\varphi_{i,k} = \varphi_{i,j} \circ \varphi_{j,k}$.*

Un ensemble G muni d'une famille d'applications $\pi_i : G \mapsto G_i$ telles que $\pi_i = \varphi_{i,j} \circ \pi_j$ si $i \leq j$ est appelée la limite projective du système projectif $(G_i, \varphi_{i,j})_{i,j\in I}$ si la propriété universelle suivante est satisfaite :
Soient X un ensemble et $(\psi_i : X \mapsto G_i)_{i\in I}$ une famille d'applications telles que $\psi_i = \varphi_{i,j} \circ \psi_j$ si $i \leq j$. Il existe alors une unique application $\psi : X \mapsto G$ rendant commutatif le diagramme suivant :



$$i \leq j$$

On note $G = \varprojlim G_i$ la limite projective du système $(G_i, \varphi_{i,j})_{i,j\in I}$.

Remarque 1.2.3.

$$G = \{\prod_{i\in I} \sigma_i \in \prod_{i\in I} G_i \mid \varphi_{i,j}(\sigma_j) = \sigma_i, i \leq j\}$$

et par conséquent, si $(G_i)_{i\in I}$ est une famille d'espaces topologiques et si les $\varphi_{i,j}$ sont continues, alors G est un fermé de l'espace topologique produit $\prod_{i\in I} G_i$.

Proposition 1.2.2. *Si G est un groupe profini, et N parcours les sous-groupes distingués ouverts de G, alors (en tant qu'ensemble et groupe topologique)*

$$G = \varprojlim G/N$$

Réciproquement, si $G_i, \varphi_{i,j}$ est un système projectif de groupes finis G_i, alors $G = \varprojlim G_i$ est un groupe profini.

C'est un résultat assez connu sur les groupes profini.

Exemple 1.2.2. $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$

Théorème 1.2.1. *(Théorème de Représentation)*
Soient K un corps ultramétrique complet et $\mathscr{O}$ son anneau maximal. Choisissons un élément ξ tel que $|\xi| < 1$ et S une famille de représentants des classes de $\mathscr{O}/\xi\mathscr{O}$ contenant 0. Alors, tout élément $x \in K^*$ peut s'écrire :

$$x = \sum_{i \geq m} a_i \xi^i \text{ avec } m \in \mathbb{Z},\ a_i \in S,\ a_m \neq 0$$

avec $m \geq 0$ si et seulement si $x \in \mathscr{O}$ et l'application $\mathscr{O} \longrightarrow \varprojlim_n \mathscr{O}/\xi^n\mathscr{O}$ est un

$$x \longmapsto (\pi_n(\textstyle\sum_{i=0}^{n} a_i \xi^i))_{n \in \mathbb{N}}$$

isomorphisme, où π_n est la projection canonique de $\mathscr{O}$ sur $\mathscr{O}/\xi^n\mathscr{O}$.

La preuve s'effectue en construisant (a_i) par récurrence puis en montrant que $x - \sum_{i \leq n} a_i \xi^i$ tend vers 0 quand n tend vers $+\infty$.

Proposition 1.2.3. *L'application naturelle de $\mathbb{Z}/p^n\mathbb{Z}$ dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$ est un isomorphisme.*

Démonstration. $\mathbb{Z}_p$ étant le complété de $\mathbb{Z}$ pour la norme p-adique, le morphisme d'anneau $i : \mathbb{Z} \to \mathbb{Z}_p$ est bien défini car le morphisme de corps $\mathbb{Q}$ dans $\mathbb{Q}_p$ est bien défini, et en utilisant le fait que pour tout $x \in \mathbb{Z}$, $v_p(x) \geq 0$. Soit $\pi : \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ la projection canonique, $\pi \circ i$ définit donc bien un morphisme d'anneau de $\mathbb{Z}$ dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$. Soit $x \in \mathbb{Z} \cap p^n\mathbb{Z}_p$, alors $v_p(x) \geq n$ et donc $x \in p^n\mathbb{Z}$, donc $Ker(\pi \circ i) \subset p^n\mathbb{Z}$. Or, l'autre inclusion est évidente, donc $Ker(\pi \circ i) = p^n\mathbb{Z}$. Donc, le morphisme de $\mathbb{Z}/p^n\mathbb{Z}$ dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$ est injectif.
Soit $z \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, donc il existe $y \in \mathbb{Z}_p$ tel que $\pi(y) = z$. Comme $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$, il existe $r \in \mathbb{Q}$ tel que $v_p(y - r) \geq n$, et en particulier on a $v_p(r) \geq 0$. Ecrivons r sous la forme $r = \frac{a}{b}$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, comme $v_p(a) \geq v_p(b)$, quitte à diviser par $p^{v_p(b)}$, on peut supposer $pgcd(b, p) = 1$. Donc $\bar{b}$ est inversible dans $\mathbb{Z}/p^n\mathbb{Z}$. Soit $\bar{c} = \bar{b}^{-1}$ dans $\mathbb{Z}/p^n\mathbb{Z}$, où $c \in \mathbb{Z}$, alors $v_p(r - ac) = v_p(a) + v_p(1 - bc) \geq n$ et donc $v_p(y - ac) \geq n$. Donc ac a pour image z dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$. □

Corollaire 1.2.1. *Le corps résiduel k de $\mathbb{Q}_p$ est isomorphe à $\mathbb{F}_p$.*

Corollaire 1.2.2. *Appliquons le théorème de représentation à $\mathbb{Q}_p$ avec $\xi = p$, on obtient que tout élément de $\mathbb{Q}_p$ peut s'écrire de manière unique sous la forme $\sum_{i \geq k} a_i p^i$ où $a_i \in \{0, 1, ..., p-1\}$ et $k \in \mathbb{Z}$. De plus, d'après la proposition précédente, on a*

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

.

Théorème 1.2.2. *(i) $\mathbb{Z}_p$ est compact et $\mathbb{Q}_p$ est localement compact.*
(ii) $\mathbb{N}$ est dense dans $\mathbb{Z}_p$, et plus généralement, si $b \in \mathbb{Z}$ est premier à p et $a \in \mathbb{Z}$, $a + b\mathbb{N}$ est dense dans $\mathbb{Z}_p$.

Démonstration. (i) Cela vient de la représentation de $\mathbb{Z}_p$ sous forme de série qui implique que $\mathbb{Z}_p$ (muni de v_p) est topologiquement isomorphe à $\prod_{n\in\mathbb{N}}\{0, 1, ..., p-1\}$ muni de la topologie produit des topologies discrètes sur $\{0, 1, ..., p-1\}$ qui compact d'après le théorème de Tychonoff. (ii) Soit $x \in \mathbb{Z}_p$, $x = \sum_{k=0}^{+\infty} a_k p^k$, où $a_k \in \{0, 1, ..., p-1\}, \forall k$. Posons $x_n = \sum_{k=0}^{n} a_k p^k \in \mathbb{N}$, on a $v_p(x - x_n) \geq n, \forall n \in \mathbb{N}$. Donc (x_n) est de Cauchy dans $\mathbb{Z}_p$ qui est complet car compact d'après le (i), donc (x_n) converge vers x dans $\mathbb{Z}_p$. Donc $\mathbb{N}$ est dense dans $\mathbb{Z}_p$.
si $b \in \mathbb{Z}$ est premier à p et $a \in \mathbb{Z}$, alors $x \mapsto bx + a$ est une isométrie de $\mathbb{Z}_p$. □

1.3 Lemme de Hensel

Nous allons à présent découvrir un résultat analogue à la méthode de Newton dans les corps complets ultramétriques. Nous prendrons K un corps valué complet à valuation discrète, $\mathscr{O}$ son anneau de valuation, $\mathfrak{m}$ son idéal maximal et $k = \mathscr{O}/\mathfrak{m}$ son corps résiduel.

Définition 1.3.1. *Un polynôme $P \in \mathscr{O}[X]$ est dit primitif si $|P|_G = 1$, i.e $P(X) \not\equiv 0 mod \wp$.*

Théorème 1.3.1. *(Lemme de Hensel)*
Si un polynôme $P \in \mathscr{O}[X]$ se décompose modulo $\mathfrak{m}$ en deux polynômes premiers entre eux $\bar{g}, \bar{h} \in k[X]$:

$$P(x) \equiv \bar{g}(x)\bar{h}(x) \, mod \, \mathfrak{m}$$

Alors P se factorise dans $\mathscr{O}[X]$ sous la forme

$$P(x) = g(x)h(x)$$

où $g(x) \equiv \bar{g}(x) \, mod \, \mathfrak{m}$ et $h(x) \equiv \bar{h}(x) \, mod \, \mathfrak{m}$ avec $\deg(g) = \deg(\bar{g})$

Une preuve de ce théorème est fournie dans le livre de Hasse [2].

Une version plus forte du lemme de Hensel existe dans le cas où K n'est pas à valuation discrète. Celle-ci se démontre non plus par une simple récurrence, mais en utilisant le théorème de point fixe de Picard.

1.4 Extensions finies de $\mathbb{Q}_p$

Dans cette partie, nous allons étendre notre valuation p-adique aux extensions finies de $\mathbb{Q}_p$ et montrer quelques résultats les caractérisant.

1.4.1 Extension de la valuation p-adique

La proprosition suivante est un résultat général concernant l'équivalence des normes en dimension finie.

Proposition 1.4.1. *Soit K un corps normé complet et V un espace vectoriel de dimension finie sur K, toutes les normes sur V (compatibles avec la norme sur K, i.e vérifiant $||\lambda x|| = |\lambda|||x|| \ \forall \lambda \in K, \forall x \in V$) sont équivalentes et V est complet pour n'importe laquelle d'entre elles.*

Démonstration. Il suffit de prouver que toutes les normes sont équivalentes à la norme sup. Montrons cela par récurrence sur la dimension de V. Si $\dim_K V = 1$, alors il n'y a rien à faire.
Si $\dim_K V = n$, supposons que tout sous-espace de V de dimension $n-1$ soit complet. Soit $e_1, ..., e_n$ une base de V, alors

$$||x_1 e_1 + ... + x_n e_n|| \leq (||e_1|| + ... + ||e_n||) \sup(|x_1|, ..., |x_n|)$$

. Pour montrons l'autre égalité, nous raisonnerons par l'absurde. Quitte à diviser par $\sup(|x_1|, ..., |x_n|)$, on peut se ramener au cas où $|x|_\infty = 1$. Supposons que $\forall \varepsilon > 0, \exists x \in V, |x|_\infty = 1, ||x|| < \varepsilon$. Donc il existe une suite $x^{(k)} = x_1^{(k)} e_1 + ... + x_n^{(k)} e_n$ telle que $|x^{(k)}|_\infty = 1$ et $||x^{(k)}|| \leq 2^{-k}, \forall k$. Ainsi, il existe $\phi : \mathbb{N} \to \mathbb{N}$ injection croissante, $i \in [\![1, n]\!]$ et $C \in \mathbb{R}_+^*$ tels que $|x_i^{\phi(k)}| \geq C$. Or $||x^{\phi(k)}|| \leq 2^{-\phi(k)}$, donc e_i appartient à l'adhérence de $Vect(e_1, ..., e_{i-1}, ..., e_{i+1}, ..., e_n)$ qui est complet par hypopthèse de récurrence donc fermé, ce qui est absurde car $e_1, ..., e_n$ forme une base de V.
De plus, la norme infinie rend bien V complet car être de Cauchy pour $|.|_\infty$ implique l'être sur chacune de ses coordonnées, or K est complet. La récurrence est prouvée.

□

Grâce à l'équivalence des normes en dimension finie, nous allons en déduire qu'il existe une unique manière de prolonger une norme sur une extension finie.

Définition 1.4.1. *Soit L/K une extension finie d'un corps K, et $x \in L$. On définit la norme de x de L sur K, $N_{L/K}(x)$, comme le déterminant de l'endomorphisme $y \mapsto xy$. De même, on définit la trace de x de L sur K, $Tr_{L/K}(x)$, comme la trace de ce même endomorphisme. Si $P = X^d + ... + a_0$ est le polynôme minimal unitaire de x sur K, alors $N_{L/K}(x) = ((-1)^d a_0)^{\frac{[L:K]}{d}}$*

Proposition 1.4.2. *Soit K un corps valué complet. Soit $P(X) = a_0 + a_1 X + ... + a_n X^n \in K[X]$ un polynôme irréductible tel que $a_0 a_n \neq 0$. Alors*

$$|P|_G = \max\{|a_0|_p, |a_n|_p\}$$

En particulier, si $a_n = 1$ et $a_0 \in \mathscr{O}$, alors $f \in \mathscr{O}$.

Nous donnerons une preuve de cette proposition seulement dans le cas où K est à valuation discrète par raison de simplicité. Dans le cas où K n'est plus à valuation discrète, la preuve utilise la forme forte du lemme de Hensel

Démonstration. Quitte à diviser le polynôme $P(X) = a_0 + a_1X + ... + a_nX^n$ par un élément $\alpha \in K$ tel que $\|\alpha|_p = |P|_G$, on peut supposer $|P|_G = 1$ et $P \in \mathscr{O}[X]$. Soit $i_0 = \inf\{i||a_i|_p = 1\}$. On a alors,

$$P(X) \equiv X^{i_0}(a_{i_0} + a_{i_0+1}X + ... + a_nX^{n-i_0}) mod \pi$$

où π est une uniformisante. Si $\max(|a_0|_p, |a_n|_p) < 1$ alors $0 < i_0 < n$, et on obtient une contradiction en remontant la factorisation grâce au lemme de Hensel puisque P est supposé irréductible. □

Théorème 1.4.1. *Soit K un corps complet pour une valuation v et soit L une extension finie de K. Alors il existe une unique manière de prolonger v en une valuation sur L. En outre, si $x \in L$, alors*

$$v(x) = \frac{1}{[L:K]} v(N_{L/K}(x))$$

Démonstration. Existence : La seule chose non triviale à montrer est l'inégalité : $v(\alpha+\beta) \geq \inf(v(\alpha), v(\beta))$. On peut tout d'abord supposer $\alpha, \beta \neq 0$, qui est évident. Quitte à intervertir α et β on peut supposer $v(\alpha) \leq v(\beta)$. De plus, quitte à soustraire $v(\alpha)$ des deux côtés, on peut se ramener à montrer $v(1 + x) \geq 0$ si $v(x) \geq 0$.
Soit $x \in L$, supposons $v(N_{L/K}(x)) \geq 0$ et montrons que $v(N_{L/K}(1+x)) \geq 0$. Soit $P(X) = X^d+...+a_0$ le polynôme minimal de x. On a $N_{L/K}(x) = ((-1)^d a_0)^{\frac{[L:K]}{d}}$. Par multiplicativité des degrés (comme $K(x) \subset L$), on a $d|[L : K]$, donc $v(a_0) \geq 0$ (i.e $a_0 \in \mathscr{O}$) et comme P est irréductible et unitaire,on obtient d'après la proposition précédente que $P \in \mathscr{O}$. Or le polynôme irréductible de $1 + x$ est $P(X - 1)$ donc $N_{L/K}(1 + x) = ((-1)^d P(-1))^{\frac{[L:K]}{d}} \in \mathscr{O}$, ce qui conclut.
Unicité : Soit deux valuations v_1 et v_2 (i.e deux normes ultramétriques) qui coïncident sur K, elles sont donc compatibles sur K, et comme $[L : K] < +\infty$, L est un K espace vectoriel de dimension finie, de plus K étant complet, on conclut d'après la proposition 1.4.1 que les deux valuations sont équivalentes. Donc, d'après le lemme 1.1.3, il existe $s \in \mathbb{R}_+^*$ tel que pour tous $x \in L$, $v_1(x) = sv_2(x)$, et comme elles coïncident sur K, on a nécessairement $s = 1$. □

La valuation donnée sur L/K prolonge bien celle définit sur K car pour tout $x \in K$, $N_{L/K}(x) = x^{[L:K]}$.

En appliquant ce théorème à $\mathbb{Q}_p$, on a que pour toute extension finie $K/\mathbb{Q}_p$, il existe un unique prolongement de la valuation p-adique à K.

Corollaire 1.4.1. *Si K^{alg} est un clôture algébrique de K, alors il existe une unique manière de prolonger la valuation v à K^{alg}. De plus, $Gal(K^{alg}/K)$ agit par des isométries.*

Démonstration. L'unicité et l'existence sont évidentes en considérant pour tous $x \in K^{alg}$, l'extension finie $K(x)/K$. De plus, si $x \in K^{alg}$ et $\sigma \in Gal(K^{alg}/K)$, alors $N_{K(x)/K}(x) = N_{K(\sigma(x))/x}(\sigma(x))$ et comme $[K(x) : K] = [K(\sigma(x)) : K]$, on a le résultat. □

Corollaire 1.4.2. *Si $P \in K[X]$ irréductible, alors toutes les racines de P (prises dans K^{alg}) sont de même valuation*

Démonstration. Comme les racines d'un polynôme irréductible sont permutées transitivement sous l'action de $Gal(K^{alg}/K)$, car $\forall \sigma \in Gal(K^{alg}/K), \forall x \in K^{alg}, \sigma(P(x)) = P(\sigma(x))$. Il suffit donc d'appliquer le corollaire précédent. □

Proposition 1.4.3. *Soit $K/\mathbb{Q}_p$ une extension finie de degré n. Soit $\mathscr{O}$ son anneau des entiers, $\mathfrak{m}$ son idéal maximal et k son corps résiduel.*
Alors $\mathscr{O}$ est un anneau de valuation discrète qui est la clôture intégrale de $\mathbb{Z}_p$ dans K. De plus, k est une extension de $\mathbb{F}_p$ de degré au plus n.

Démonstration. La première affirmation découle directement de la proposition 1.4.1 et du théorème 1.4.1.
On a $\mathscr{O} \cap \mathbb{Z}_p = p\mathbb{Z}_p$, il existe donc une injection de $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ dans k et donc k est une extension de $\mathbb{F}_p$. Remarquons que k peut être vu comme un $\mathbb{F}_p$ espace vectoriel. Montrons maintenant que $[k : \mathbb{F}_p] \leq n$. Soient $\bar{a_1}, ..., \bar{a_{n+1}} \in k$ et $a_1, ..., a_{n+1}$ leurs représentants respectifs dans $\mathscr{O}$. Comme $[K : \mathbb{Q}_p] = n$, il existe $\lambda_1, ..., \lambda_{n+1} \in \mathbb{Q}_p$ tels que

$$\lambda_1 a_1 + ... + \lambda_{n+1} a_{n+1} = 0$$

Soit $k = \min\{v_p(\lambda_i) |\ 1 \leq i \leq n+1\}$, quitte à multiplier les λ_i par p^{-k} si $k < 0$, on peut supposer $\lambda_i \in \mathbb{Z}_p, \forall i$.
Donc après réduction modulo $\wp$ on obtient

$$\bar{\lambda}_1 \bar{a}_1 + ... + \bar{\lambda}_{n+1} \bar{a}_{n+1} = 0$$

et donc

$$\widetilde{\lambda}_1 . \bar{a}_1 + ... + \widetilde{\lambda}_{n+1} . \bar{a}_{n+1} = 0$$

où . désigne l'action de $\mathbb{F}_p$ dans k définit de manière évidente par $\widetilde{\lambda} . \bar{a} = \bar{\lambda}\bar{a}$. □

Remarque 1.4.1. *On peut montrer de la même manière que si K est un ccorps valué complet et L est une extension finie de K. Alors k_L est une extension algérique de k_K de degré au plus $[L : K]$.*

1.4.2 Ramification

Dans cette partie, nous noterons pour K un corps de nombre p-adique, $\mathscr{O}$ son anneau des entiers, $\mathfrak{m}$ son idéal maximal et k son corps résiduel.

Définition 1.4.2. *Soit L/K une extension finie.*
(i) $n = [L : K]$ le degré de l'extension qui est la dimension de L en tant que K espace vectoriel.
(ii) $f = [k_L : k_K]$ est appelé degré résiduel et correspond à la dimension de k_L en tant que k_K espace vectoriel.
(iii) $e = [|L^*| : |K^*|$ est appelé indice de ramification de K.

Théorème 1.4.2. *Si $[K : \mathbb{Q}_p] = n$, alors $ef = n$.*

Une preuve de ce théorème sans soucis de généralisation se fait en prenant la bonne famille de représentants. Pour plus de détails sur cette preuve, voir Alain M.Robert [4].

Corollaire 1.4.3. *Soit L/K une extension finie de corps de nombres p-adiques. Par la formule des indices on a également $ef = [L : K]$*

Soit $K/\mathbb{Q}_p$ une extension finie, soit π une uniformisante de K, on a pour tous $x \in K$, $x = \pi^k u$ où $k \in \mathbb{Z}$ et u inversible. En particulier, $p = \pi^e u$ où u inversible et e est l'indice de ramification de K.

Définition 1.4.3. *Une extension finie L/K est dite non ramifiée si $e = 1$. Elle est dite totalement ramifiée si $f = 1$, i.e $e = [L : K]$.*

Proposition 1.4.4. *Soit L/K une extension finie, π une uniformisante de L. L est totalement ramifiée si et seulement si $L = K(\alpha)$ où est racine d'un polynôme d'Eisenstein.*

Démonstration. Soit P le polynôme minimal de π.
($\Rightarrow$) on a $v_p(\pi) = \frac{1}{e}$ et $[L : K]$, alors $degP = e$ car $v_p(\prod_{\sigma \in Gal(L/K)} \sigma(\pi)) = \frac{degP}{e} \in \mathbb{N}^*$ donc est nécessairement égal à 1. En multipliant P par π^{e-1} on remarque $P(X) = X^e + a_{e-1}X^{e-1} + ... + a_0$ est polynôme d'Eisenstein puisque $v_p(a_0) = 1$ et $v_p(a_i) \geq \frac{1}{e}, \forall 1 \leq i \leq e-1$.
($\Leftarrow$) on a $[L : K] = e = deg(P)$ donc $ev_p(\pi) = 1$ d'où $v_p(\frac{1}{e})$. □

Théorème 1.4.3. *Soit $K/\mathbb{Q}_p$ une extension finie.*
Soit π une uniformisante de K ($v_p(\pi) = \frac{1}{e}$), il existe une unique décomposition

$$\mathbb{Q}_p \hookrightarrow \ K_f^{unram} = \mathbb{Q}_p(\zeta_{p^f-1}) \hookrightarrow K = K_f^{unram}(\pi)$$

où ζ_{p^f-1} est une racine (p^f-1)-ième de l'unité, telle que $K_f^{unram}/\mathbb{Q}_p$ soit non ramifiée et K/K_f^{unram} soit totalement ramifiée.

Démonstration. Existence : Commençons par connstruire une extension non ramifiée de degré f.Soit $k = \mathbb{F}_{p^f}$, $\mathbb{F}_{p^f}^*$ est cylique, posons $\mathbb{F}_{p^f}^* = \langle \bar{\alpha} \rangle$. Soit $\bar{P} = \sum_{i=0}^{f} \bar{\alpha}_i X^i$ le polynôme minimal de $\bar{\alpha}$(qui est de degré f) à coefficients dans $\mathbb{F}_p$, qui peut être vu comme à coefficient dans k car $\mathbb{F}_p[X] \hookrightarrow k[X]$ où $\bar{P}$. Comme $\bar{\alpha}$ est un générateur de k^*, on a $\bar{\alpha}^{p_1^f} = \bar{1}$, or $\bar{\alpha}$ est racine simple de $\bar{P}$, donc $\bar{P}'(\bar{\alpha}) \neq \bar{0}$ et $\bar{P}(\bar{\alpha}) = \bar{0}$ et donc d'après le lemme de Hensel, il existe $\alpha \in \mathscr{O}, P(\alpha) = 0$ où $P(X) = \sum_{i=0}^{f} \alpha_i X^i \in \mathbb{Z}_p[X]$ avec α_i est un représentant de $\bar{\alpha}_i$ dans $\mathbb{Z}_p$. Donc P est irréductible dans $\mathbb{Q}_p[X]$ (car sinon $\bar{P}$ serait réductible dans $\mathbb{F}_p[X]$). Posons $K_f^{unram} := \mathbb{Q}_p(\alpha)$. On a $[K_f^{unram} : \mathbb{Q}_p] = f$. Soit k_f^{unram} le corps résiduel de K_f^{unram}. On a $\widetilde{\pi}(\alpha)$ racine de $\bar{P} \in \mathbb{F}_p[X] \hookrightarrow k_f^{unram}[X]$ où $\widetilde{\pi} : \mathscr{O}_{K_f^{unram}} \to k_f^{unram}$ surjection canonique. Donc $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = f$, or $\widetilde{\pi}(\alpha) \in k_f^{unram}$ donc

$$f = [\mathbb{F}_p(\widetilde{\pi}(\alpha)) : \mathbb{F}_p] \leq [k_f^{unram} : \mathbb{F}_p] \leq [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = f$$

donc $[k_f^{unram} : \mathbb{F}_p] = f$, donc $k_f^{unram} = \mathbb{F}_{p^f}$ et donc k_f^{unram} est non ramifiée.
Posons $\zeta_{p^f-1} := [\bar{\alpha}]$,le représentant de Teichmüller de $\bar{\alpha}$ dans $\mathscr{O}_{K_f^{unram}}$ (obtenu en appliquant le lemme de Hensel au polynôme $X^{p^f-1}-1$). ζ_{p^f-1} est bien une racine (p^f-1)-ième de l'unité car les $\bar{\alpha}^k$ pour $0 \leq k \leq p^f-1$ sont tous deux à deux distincts.
De plus, $\widetilde{\pi}(\zeta_{p^f-1}) = \widetilde{\pi}(\alpha)$ dans $k_f^{unram} = \mathbb{F}_{p^f}$. Soit $\widetilde{K} = \mathbb{Q}_p(\zeta_{p^f-1}) \subset K_f^{unram}$ et soit $\widetilde{k}$ son corps résiduel. On a $\mathbb{F}_p(\widetilde{\pi}(\zeta_{p^f-1})) = \mathbb{F}_p(\widetilde{\pi}(\alpha)) = \mathbb{F}_{p^f}$. Soit $p : \mathscr{O}_{\widetilde{K}} \to \widetilde{k}$ surjection canonique, d'après la remarque de la proposition 1.4.1, on obtient un morphisme de corps injectif $i : \widetilde{k} \to k_f^{unram} = \mathbb{F}_{p^f}$, et donc $\widetilde{\pi}(\zeta_{p^f-1}) = i \circ p(\zeta_{p^f-1})$ et par conséquent, $\mathbb{F}_p(\widetilde{\pi}(\zeta_{p^f-1})) = \mathbb{F}_p(p(\zeta_{p^f-1})) = \mathbb{F}_{p^f}$. Or $p(\zeta_{p^f-1}) \in \widetilde{k}$, donc

$$f \leq [\widetilde{k} : \mathbb{F}_p] \leq [\widetilde{K} : \mathbb{Q}_p] \leq [K_f^{unram} : \mathbb{Q}_p] = f$$

Or $\widetilde{K} \subset K_f^{unram}$ donc $\widetilde{K} = K_f^{unram}$.
D'après le lemme précédent, $K_f^{unram}(\pi)/K_f^{unram}$ (où π est une uniformisante de K) est totalement ramifiée. Comme $degP_{\min,\pi} = e$ et $K_f^{unram}(\pi) \subset K$, on a nécessairement

$$K_f^{unram}(\pi) \subset K$$

.
Unicité : Soit $L \hookrightarrow K$ une sous-extension de K telle que $L/\mathbb{Q}_p$ soit non ramifiée et K/L totalement ramifiée.
En appliquant le lemme de Hensel dans L au polynôme $X^{p^f-1}-1$, on obtient l'égalité $L = \mathbb{Q}_p(\mu_{p^f-1})$. Or $K_f^{unram} = \mathbb{Q}_p(\zeta_{p^f-1})$, et comme $\langle \mu_{p^f-1} \rangle = \langle \zeta_{p^f-1} \rangle$, on conclut que

$$L = K_f^{unram}$$

. □

1.5 Construction de $\mathbb{C}_p$

Contrairement à $\mathbb{R}$ où $\mathbb{C}$ est une extension algébriquement close et complète de $\mathbb{R}$ de degré fini car $\mathbb{C} = \mathbb{R}(i)$, tout corps de nombre p-adique (*i.e extension finie de* $\mathbb{Q}_p$) n'est pas algébriquement close car il existe des polynômes irréductibles de n'importe quel degré dans $\mathbb{F}_p$ et donc dans $\mathbb{Q}_p$. Notons $\mathbb{Q}_p^{alg}$ la clôture algébrique de $\mathbb{Q}_p$, on a par conséquent $[\mathbb{Q}_p^{alg} : \mathbb{Q}_p] = +\infty$. Cependant le résultat suivant montre que $\mathbb{Q}_p^{alg}$ n'est pas complet.

Proposition 1.5.1. *$\mathbb{Q}_p^{alg}$ n'est pas complet.*

Démonstration. Posons

$$\alpha = \sum_{n=1}^{+\infty} \zeta_{\phi(n)} p^n,$$

où $\phi(n) = n$ si $pgcd(n,p) = 1$, et $\phi(n) = 1$ sinon, avec ζ_n racine n-ième de l'unité. Si $\mathbb{Q}_p^{alg}$ était complet, cette série convergerait vers $\alpha \in \mathbb{Q}_p^{alg}$. Par conséquent, α appartiendrait à

une extension finie K de $\mathbb{Q}_p$. Supposons $\zeta_n \in K, \forall n < m$, nous pouvons supposer $p \nmid m$. Alors,

$$\beta = p^{-m}(\alpha - \sum_{n=1}^{m-1} \zeta_{\phi(n)} p^n) \in K$$

et $\beta \equiv \zeta_m \, mod \, p$. Par conséquent, $X^m - 1 \equiv 0 \, mod \, p$ a une solution dans K. Or p ne divisant pas m, $X^m - 1 = 0$ possède une solution dans K d'après le lemme de Hensel qui est congrue à β modulo p et par conséquent à ζ_m modulo p. Comme les racines m-ièmes de l'unité sont distinctes modulo p, puisque $m = \prod_{\substack{\zeta^m=1 \\ \zeta \neq 1}} (1 - \zeta)$ (qui est obtenu en remarquant que $X^{n-1} + ... + X + 1 = \prod_{k=1}^{n-1}(1 - \zeta_n^k)$). Par conséquent $\zeta_m \in K$. Par récurrence, on a $\zeta_m \in K, \forall m, p \nmid m$. De plus, les racines de l'unité d'ordre premier à p étant distinctes modulo p, on a une infinité de classes modulo p dans l'anneau des entiers de K.Or, $K/\mathbb{Q}_p$ étant une extension finie, on obtient une contradiction. Donc $\alpha \notin \mathbb{Q}_p^{alg}$ et $\mathbb{Q}_p^{alg}$ n'est pas complet □

Pour faire de l'analyse, il est généralement plus intéressant de travailler dans une structure complète, d'où la définition suivante :

Définition 1.5.1. *On appelle $\mathbb{C}_p$ le complété de $\mathbb{Q}_p^{alg}$ pour la norme p-adique.*

Nous allons montrer que $\mathbb{C}_p$ est algébriquement clos, mais nous commencerons par introduire un lemme remarquable dû à Krasner.

Lemme 1.5.1. *(Lemme de Krasner)*
Soit K un corps valué complet. Soit $\alpha, \beta \in K^{alg}$, avec α séparable sur $K(\beta)$ (i.e le polynôme minimal de α dans K^{alg} est à racines simples).
Supposons que pour tout conjugué $\alpha_i \neq \alpha$ de α, on a

$$|\beta - \alpha| < |\alpha_i - \alpha|.$$

Alors $K(\alpha) \subset K(\beta)$ (où $|.|$ désigne l'unique extension à K^{alg} de la norme ultramétrique associée à la valuation définie sur K)

En d'autre termes, si α est suffisamment proche de β, alors $\alpha \in K(\beta)$.

Démonstration. Considérons l'extension $K(\alpha, \beta)/K(\beta)$ et $L/K(\beta)$ la clôture Galoisienne. Soit $\sigma \in Gal(L/K(\beta))$. Alors $\sigma(\beta - \alpha) = \beta - \sigma(\alpha)$. Or, comme $\beta \in K^{alg}$, $K(\beta)/K$ est une extension finie donc $K(\beta)$ est complet pour $|.|$, donc $Gal(L/K(\beta))$ agit par des isométries. On a donc,

$$|\beta - \sigma(\alpha)| = |\beta - \alpha| < |\alpha_i - \alpha|$$

pour tout $\alpha_i \neq \alpha$. Par conséquent,

$$|\alpha - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha_i)|\} < |\alpha_i - \alpha|$$

Donc $\sigma(\alpha) = \alpha, \forall \sigma \in Gal(L/K(\beta))$, donc $\alpha \in K(\beta)$. □

Proposition 1.5.2. $\mathbb{C}_p$ *est algébriquement clos.*

Démonstration. Nous allons utiliser le lemme de Krasner avec $K = \mathbb{C}_p$.
Soit α algébrique sur $\mathbb{C}_p$ et $P(X) \in \mathbb{C}_p[X]$ son polynôme minimal ($degP = n$). Comme $\mathbb{Q}_p^{alg}$ est dense dans $\mathbb{C}_p$,

$$\forall \varepsilon > 0, \exists Q_\varepsilon \in \mathbb{Q}_p^{alg}[X], |P(X) - Q_\varepsilon(X)|_G < \varepsilon$$

. Or, $\forall x \in \mathbb{C}_p, |P(x) - Q_\varepsilon(x)| \leq |P(X) - Q_\varepsilon(X)|_G \max\{|x|^n, 1\}$ car on peut supposer $degQ_\varepsilon \leq degP$.
Par conséquent,

$$|Q_\varepsilon(\alpha)| = |Q_\varepsilon(\alpha) - P(\alpha)| \leq |P(X) - Q_\varepsilon(X)|_G \max\{|\alpha|^n, 1\} < \varepsilon \max\{|\alpha|^n, 1\}$$

Ecrivons $Q_\varepsilon(X) = \prod_{i=1}^n (X - \beta_{i,\varepsilon})$.
Soit $i_0(\varepsilon)$ tel que $|\alpha - \beta_{i_0(\varepsilon),\varepsilon}| = \inf\{|\alpha - \beta_{i,\varepsilon}| \mid 1 \leq i \leq n\}$. Alors,

$$|\alpha - \beta_{i_0(\varepsilon),\varepsilon}| \leq |Q_\varepsilon(\alpha)|^{\frac{1}{n}} < \varepsilon^{\frac{1}{n}} \max\{|\alpha|, 1\}$$

Soit $\varepsilon > 0$ vérifiant $\varepsilon < \frac{\sup\{|\alpha_i - \alpha|\}^n}{\max\{|\alpha|^n, 1\}}$. Pour tout $\alpha_i \neq \alpha$ conjugué de α, on a

$$|\alpha - \beta_{i_0(\varepsilon),\varepsilon}| < |\alpha - \alpha_i|$$

. Donc $\alpha \in \mathbb{C}_p(\beta_{i_0(\varepsilon),\varepsilon}) = \mathbb{C}_p$ d'après le lemme de Krasner, donc $\mathbb{C}_p$ est algébriquement clos. □

On a finalement construit une extension de $\mathbb{Q}_p$ à la fois complète et algébriquement close qui peut être vu comme l'analogue p-adique de $\mathbb{C}$.
Un résultat amusant que nous ne démontrerons pas est que $\mathbb{C}_p$ et $\mathbb{C}$ sont algébriquement isomorphes mais pas topologiquement, puisqu'ils ont le même degré de transcendance.

Le lemme suivant va donner une description de la structure de $\mathbb{C}_p^*$.

Lemme 1.5.2.

$$\mathbb{C}_p^* = p^{\mathbb{Q}} \times W \times U_1$$

où W est le groupe des racines de l'unité et $U_1 = \{x \in \mathbb{C}_p \mid |x - 1| < 1\}$.

Démonstration. Soit $\alpha \in \mathbb{C}_p^*$. Si $\alpha_1 \in \mathbb{Q}_p^{alg}$ est suffisamment proche de α, alors $|\alpha| = |\alpha_1|$ d'après le lemme de Krasner. Comme $|\alpha_1| \in p^{\mathbb{Q}}$ puisque $\mathbb{Q}_p(\alpha_1)/\mathbb{Q}_p$ est une extension finie. Donc $|\alpha| \in p^{\mathbb{Q}}$. On peut maintenant supposer $|\alpha| = 1$.
Soit $\beta \in \mathbb{C}_p^*, |\beta| = 1$. Choisissons $\beta_1 \in \mathbb{Q}_p^{alg}$ proche de β. Toute unité de l'extension finie $\mathbb{Q}_p(\beta_1)/\mathbb{Q}_p$ est congrue à une racine de l'unité ω modulo $\mathfrak{m}_{\mathbb{Q}_p(\beta_1)}$ (représentant de Teichmüller), qui est unique. Donc $|\beta_1 - \omega| < 1$, et donc $|\beta - \omega| < 1$ par inégalité ultramétrique, d'où $|\beta\omega^{-1} - 1| < 1$. Donc, on a

$$\mathbb{C}_p^* = p^{\mathbb{Q}} \times W \times U_1$$

. □

Regardons de plus prêt le corps résiduel de $\mathbb{Q}_p^{alg}$ et celui de $\mathbb{C}_p$.

Lemme 1.5.3. *Si K est un corps ultramétrique algébriquement clos, alors k_K est algébriquement clos.*

Démonstration. Soit $\bar{P}(X) \in k_K[X]$ unitaire de degré $n \geq 1$ et soit $P(X) \in \mathscr{O}_K[X]$ unitaire de degré n relevant $\bar{P}$. Soit $\alpha \in K$ une racine de P. On a $\alpha \in \mathscr{O}$ d'après la proposition 1.4.1 et l'image de α dans k_K est une racine de $\bar{P}$. □

Corollaire 1.5.1. $k_{\mathbb{Q}_p^{alg}} = \mathbb{F}_p^{alg}$

Lemme 1.5.4. *Si K est un corps valué algébriquement clos et $\widehat{K}$ dénote son complété, alors $k_K = k_{\widehat{K}}$.*

Démonstration. $\mathscr{O}_K \cap \mathfrak{m}_{\widehat{K}} = \mathfrak{m}_K$ donc l'application naturelle de k_K dans $k_{\widehat{K}}$ est injective. De plus, comme $\mathscr{O}_K$ est dense dans $\mathscr{O}_{\widehat{K}}$ cette application est sujective. En effet, soit $\bar{x} \in k_{\widehat{K}}$, avec $x \in \mathscr{O}_{\widehat{K}}$ un représentant de $\bar{x}$, par densité il existe $y \in \mathscr{O}_K$ tel que $v(x-y) > 0$. Donc $x \equiv y \, mod \, \mathfrak{m}_{\widehat{K}}$ d'où la surjectivité. □

Corollaire 1.5.2. $k_{\mathbb{C}_p} = k_{\mathbb{Q}_p^{alg}} = \mathbb{F}_p^{alg}$

2 Première construction des L fonctions p-adique

Dans cette partie, nous présenterons une méthode de construction assez brutale des L fonctions p-adiques.

2.1 Caractères de Dirichlet et sommes de Gauss

Soit $n \in \mathbb{N}$, on appelle un caractère de Dirichlet modulo n un morphisme de groupes de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $\mathbb{Q}^{alg}$. Si $m \mid n$, et χ est un caractère de Dirichlet modulo m, on peut voir χ comme un caractère de Dirichlet modulo n en composant par la projection $\pi : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$.

Définition 2.1.1. *(Conducteur)*
Soit χ un caractère de Dirichlet, χ est de conducteur f_χ (noté parfois f) si quelque soit n diviseur de f_χ distinct de f_χ, la restriction de χ au noyau de la projection $\pi : (\mathbb{Z}/f_\chi\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ n'est pas triviale.

Si χ est un caractère de Dirichlet modulo f_χ, on note χ^{-1} le caractère de Dirichlet modulo f_χ définit par $\chi^{-1}(n) = \chi(n)^{-1}$, si $n \in (\mathbb{Z}/f_\chi\mathbb{Z})^*$ On considère aussi souvent χ comme une fonction périodique sur $\mathbb{Z}$ de période f_χ en composant avec la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/f_\chi\mathbb{Z}$ et en étendant par $\chi(n) = 0$, si $pgcd(n, f_\chi) \neq 1$. On a donc $\chi^{-1}(n) = \chi(n)^{-1}$, si $pgcd(n, f_\chi) = 1$ et $\chi^{-1}(n) = 0$ sinon.

Définition 2.1.2. *(Somme de Gauss tordue)*
Soit χ un caractère de Dirichlet modulo f_χ. Si $n \in \mathbb{Z}$, on définit la somme de Gauss tordue $G(\chi, n)$ par la formule

$$G(\chi, n) = \sum_{a \bmod f_\chi} \chi(a)\zeta_{f_\chi}^{na}$$

où $\zeta_{f_\chi} = e^{\frac{2i\pi}{f_\chi}}$. On pose $G(\chi) = G(1, \chi)$

Lemme 2.1.1. *(i) Si $n \in \mathbb{N}$, alors $G(\chi, n) = \chi^{-1}(n)G(\chi)$.*
(ii) $G(\chi)G(\chi^{-1}) = \chi(-1)f_\chi$

Démonstration. (i) Si $pgcd(n, f_\chi)$, alors n est inversible dans $(\mathbb{Z}/f_\chi\mathbb{Z})^*$, ce qui permet d'écrire

$$G(\chi, n) = \sum_{a \bmod f_\chi} \chi(a)\zeta_{f_\chi}^{na} = \chi^{-1}(n) \sum_{na \bmod f_\chi} \chi(na)\zeta_{f_\chi}^{na} = \chi^{-1}(n)G(\chi)$$

Si $pgcd(n, f_\chi) = d$, on pose $f_\chi = df'$ et $n = dn'$. Soit U le noyau de la projecion $(\mathbb{Z}/f_\chi\mathbb{Z})^* \to (\mathbb{Z}/f'\mathbb{Z})^*$. Si on choisit S un système de représentants de $(\mathbb{Z}/f_\chi\mathbb{Z})^*$ dans $(\mathbb{Z}/f'\mathbb{Z})^*$, on a

$$G(\chi, n) = \sum_{a \in S} \sum_{u \in U} \chi(au)\zeta_{f_\chi}^{au}$$

Or, si $u \in U$ et $a \in \mathbb{Z}$, alors $nau - na = na(u-1) \equiv 0 \, mod \, f_\chi$ et donc $\zeta_{f_\chi}^{anu} = \zeta_{f_\chi}^{au}$. Par conséquent,

$$G(\chi, n) = \sum_{a \in S} \chi(a) \zeta_{f_\chi}^{na} (\sum_{u \in U} \chi(u)) = 0$$

car $\sum_{u \in U} \chi(u) = 0$ puisque χ est un caractère non trivial de U (sinon χ serait de conducteur f').
(ii) Utilisant le (i), on obtient

$$\begin{aligned} G(\chi)G(\chi^{-1}) = \sum_{b \, mod \, f_\chi} \zeta_{f_\chi}^{b} \chi^{-1}(b) G(\chi) &= \sum_{b \, mod \, f_\chi} \zeta_{f_\chi}^{b} \sum_{a \, mod \, f_\chi} \chi(a) \zeta_{f_\chi}^{ab} \\ &= \sum_{a \, mod \, f_\chi} \chi(a) \sum_{b \, mod \, f_\chi} \zeta_{f_\chi}^{(a+1)b} \end{aligned}$$

et comme $\sum_{b \, mod \, f_\chi} \zeta_{f_\chi}^{(a+1)b} = \begin{cases} f_\chi \, , \; si \; a = -1 \\ 0 \qquad\quad sinon \end{cases}$ on en déduit que $G(\chi)G(\chi^{-1}) = \chi(-1) f_\chi$.
□

2.2 Rappels sur les L séries et coefficients de Bernouilli généralisés

Soit χ un caractère de Dirichlet de conducteur f. La L série attachée à χ est définit par

$$L(\chi, s) = \sum_{n=0}^{+\infty} \frac{\chi(n)}{n^s}, \;\; \Re(s) > 1$$

où $s \in \mathbb{C}$. Pour $\chi = 1$ on retrouve la fameuse fonction Zêta de Riemann. Egalement, de la même manière que l'on a

$$\zeta(s) = \prod_{p \in \mathscr{P}} (1 - p^{-s})^{-1}, \;\; \Re(s) > 1$$

on trouve aisément la jolie formule suivante :

$$L(\chi, s) = \prod_{p \in \mathscr{P}} (1 - \chi(p) p^{-s})^{-1}, \;\; \Re(s) > 1$$

De manière encore plus générale, on peut définir la foncion zeta de Hurwitz

$$\zeta(s, b) := \sum_{n=0}^{+\infty} \frac{1}{(b+n)^s}, \;\; \Re(s) > 1, \; 0 < b \leq 1$$

et obtenir ainsi

$$L(\chi, s) = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta(s, \frac{a}{f})$$

Ces L fonctions ont la particularité d'être prolongeable analytiquement au plan $\mathbb{C}$ tout entier privé d'un pôle simple en $s = 1$. Ce résultat sera démontré dans la section 4.

L'idée majeure de cette partie est de montrer $L(\chi, 1-n) \in \mathbb{Q}, \forall n \in \mathbb{N}^*$. Plus précisément, nous allons expliciter cette valeur grâce aux outils suivants.
Les coefficients de Bernouilli "classiques" B_n sont définit en développement en série de Taylor $f_0(t) = \frac{t}{e^t-1}$, c'est-à-dire :

$$\frac{t}{e^t-1} = \sum_{n=0}^{+\infty} B_n \frac{t^n}{n!}$$

On peut donc également définir les coefficients de Bernouilli généralisés par :

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft}-1} = \sum_{n=0}^{+\infty} B_{n,\chi} \frac{t^n}{n!}$$

De plus, on définit les polynômes de Bernouilli $B_n(X)$ par :

$$\frac{te^{tX}}{e^t-1} = \sum_{n=1}^{+\infty} B_n(X) \frac{t^n}{n!}$$

On en déduit sans difficultée que

$$B_n(1-X) = (-1)^n B_n(X)$$

et en effectuant le produit de Cauchy des séries $\frac{t}{e^t-1}$ et e^{tX}, que

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$$

Proposition 2.2.1. *Soit F tel que $f \mid F$. Alors,*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right)$$

Démonstration.

$$\sum_{n=0}^{+\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} = \sum_{a=1}^{F} \chi(a) \frac{te^{(a/F)Ft}}{e^{Ft}-1}$$

L'intervertion des sommes est possible en étudiant la convergence simple de la suite des sommes partielles.
Soit $g = \frac{F}{f}$ et $a = b + cf$. Alors, on a

$$\sum_{b=1}^{f} \sum_{c=0}^{g-1} \chi(b) \frac{te^{(b+cf)t}}{e^{fgt}-1} = \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{ft}-1} = \sum_{n=0}^{+\infty} B_{n,\chi} \frac{t^n}{n!}.$$

□

Théorème 2.2.1. $L(\chi, 1-n) = -\frac{B_{n,\chi}}{n}, n \geq 1$. *Plus généralement,* $\zeta(1-n, b) = -\frac{B_n(b)}{n}, n \geq 1, 0 < b \leq 1$.

Démonstration. La preuve est un résultat d'analyse complexe. Le lecteur intéressé pourra se référer au livre de Washington [5] □

A première vue, le théorème suivant semble n'avoir que peu d'intérêt en soi. Cependant, comme nous le verrons au théorème 2.4.1, ces deux théorèmes révolutionnent notre vision à priori des L fonctions p-adiques.

Théorème 2.2.2. *Si* $\zeta_f = e^{\frac{2i\pi}{f}}$ *et* $G(\chi) = \sum_{a \bmod f} \chi(a)\zeta_f^a$ *la somme de Gauss associée. Alors*

$$L(\chi, 1) = -\frac{1}{G(\chi^{-1})} \sum_{a=1}^{f} \chi^{-1}(a) \log_p(1 - \zeta_f^a)$$

Démonstration. Ce résultat sera démontrer dans la dernière section. □

2.3 Quelques généralitées sur les fonctions p-adiques

2.3.1 Exponentielle et logarithme p-adique

On allons commencer par introduire la fonction exponentielle. On la définit sous la forme d'une série formelle :

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$$

Enonçant un petit résultat classique qui nous sera bien utile par la suite.

Lemme 2.3.1. $v_p(n!) = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$
Plus précisément, si $n = \sum_{i=k}^{N} a_i p^{i-k}$ *alors* $v_p(n!) = \frac{n - S_p(n)}{p-1}$ *où* $S_p(n) = \sum_{i=1}^{n} a_i$.

Démonstration. $v_p(n!) = \sum_{k \geq 1} k(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{n}{p^{k-1}} \rfloor = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$
Si $n = \sum_{i=0}^{N}$ où $a_N \neq 0$, donc $\lfloor \frac{n}{p^k} \rfloor = \sum_{i=k}^{N} a_i p^{i-k}$, si $N \geq k$
donc

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{N} \sum_{i=k}^{N} a_i p^{i-k} = \sum_{i=1}^{N} \sum_{k=1}^{i} a_i p^{i-k} \\ &= \sum_{i=1}^{N} a_i p^i \sum_{k=1}^{i} p^{-k} = \sum_{i=1}^{N} a_i p^i \frac{(1 - p^{-i})}{p-1} \\ &= \frac{n - \sum_{i=1}^{n} a_i}{p-1} \end{aligned}$$

□

Corollaire 2.3.1. $\frac{n-p}{p-1} - \frac{\log n}{\log p} < v_p(n!) < \frac{n}{p-1}$

Proposition 2.3.1. *Dans* $\mathbb{C}_p$, $\exp(X)$ *a pour rayon de convergence* $p^{-1/(p-1)}$

Démonstration. D'après le corollaire précédent, $|\frac{x^n}{n!}|_p$ tends vers 0 si $|x|_p < p^{-1/(p-1)}$ et tend vers $+\infty$ si $|x|_p > p^{-/(p-1)}$. Or, rappelons que pour une norme ultramétrique une série converge si et seulement si son terme général tend vers 0. D'où le résultat. □

On peut constater que $e = \exp(1)$ n'est pas défini, et que e^p l'est. On pourrait définir e par $(\exp(p))^{\frac{1}{p}}$ mais il ne serait pas unique.

On définit le logarithme également sous la forme d'une série formelle, ce qui donne :

$$\log_p(1+X) = \sum_{n=0}^{+\infty} \frac{(-1)^{n+1}X^n}{n}$$

Proposition 2.3.2. *Si* $v_p(x) > 0$, *la série entière* $\log_p(1+x) = \sum_{n=0}^{+\infty} \frac{(-1)^{n+1}x^n}{n}$ *converge dans* $\mathbb{C}_p$. *De plus, si* $v_p(x) > 0$ *et* $v_p(y) > 0$, *alors* $\log_p((1+X)(1+Y)) = \log_p(1+X) + \log_p(1+Y)$.

Démonstration. On a $v_p(\frac{(-1)^{n+1}x^n}{n}) \geq nv_p(x) - v_p(n) \geq nv_p(x) - \frac{\log n}{\log p}$ et donc $v_p(\frac{(-1)^{n+1}x^n}{n})$ tend vers $+\infty$ quand n tend vers $+\infty$ si $v_p(x) > 0$.
De plus, on a $\log_p((1+X)(1+Y)) = \log_p(1+X) + \log_p(1+Y)$ en dérivant les séries entières. Un développement en série entie entière de $\log_p(1+X+X+XY)$ nous permet de montrer que les deux séries sont égales à

$$\sum_{i_1+i_2+i_3 \geq 1} \frac{(-1)^{i_1+i_2+i_3}(i_1+i_2+i_3)!}{(i_1+i_2+i_3)i_1!i_2!i_3!} X^{i_1+i_3}Y^{i_2+i_3}$$

. Maintenant, la série $\sum_{i_1+i_2+i_3 \geq 1} \frac{(-1)^{i_1+i_2+i_3}(i_1+i_2+i_3)!}{(i_1+i_2+i_3)i_1!i_2!i_3!} x^{i_1+i_3}y^{i_2+i_3}$ coverge car le terme général tend vers 0 quand $i_1 + i_2 + i_3$ tend vers $+\infty$ et on peut réordonner les termes comme on veut, on en déduit le résultat. □

Proposition 2.3.3. *Il existe une unique extension de* $\log_p$ *à tout* $\mathbb{C}_p^*$ *telle que* $\log_p(p) = 0$ *et* $\log_p(xy) = \log_p(x) + \log_p(y)$ *pour tous* $x, y \in \mathbb{C}_p^*$.

Démonstration. En utilisant le lemme 1.5 , soit $\alpha = p^r \omega x \in \mathbb{C}_p^*$, où $r \in \mathbb{Q}, w \in W$ et $x \in U_1$. Définissons $\log_p(\alpha) = \log_p(x)$. Comme $x \in U_1$, $\log_p$ est bien défini sur $\mathbb{C}_p^*$ et satisfait de manière évidente les conditions demandées.
Supposons $f(\alpha)$ donne une autre extension de $\log_p$. Si $\omega^N = 1$, alors

$$f(\alpha) = \frac{1}{N}f(\alpha^N) = \frac{1}{N}f(p^{rN}) + \frac{1}{N}f(1) + \frac{1}{N}f(x^N) = 0 + 0 + \frac{1}{N}\log_p(x^N) = \log_p(x)$$

d'où l'unicité. □

Lemme 2.3.2. *Si* $|x| < p^{-1/(p-1)}$ *alors* $|\log_p(1+x)| = |x|$ *et si* $|x| \leq p^{-1/(p-1)}$ *alors* $|\log_p(1+x)| \leq |x|$.

La preuve s'effectue en étudiant la norme des termes de $\log_p(1+x)$ et en remarquant que $|n| \geq \frac{1}{n}, \forall n \in \mathbb{N}^*$.
A présent, donnons une caractérisation des zéros de $\log_p$ à travers la proposition suivante.

Proposition 2.3.4. $\log_p(x) = 0 \Longleftrightarrow \exists N \in \mathbb{N}, x^{p^N} = 1$

Démonstration. Comme $\mathbb{C}_p^* = p^{\mathbb{Q}} \times W \times U_1$ on peu supposer $x = 1 + y$ où $|y| < 1$. Soit $N \in \mathbb{N}$ tel que $|y^{p^N}| < p^{-1/(p-1)}$. Alors

$$x^{p^N} = (1+y)^{p^N} = 1 + p^N y + ... + \binom{N}{j} y^j + ... + y^{p^N}.$$

Tous les termes du milieu ont une norme inférieure à $|py| < |p| < p^{-1/(p-1)}$, et le choix de N implique $|y^{p^N}| < p^{-1/(p-1)}$. Par conséquent, $|x^{p^N} - 1| < p^{-1/(p-1)}$ et d'après le lemme précédent

$$0 = |\log_p(x^{p^N})| = |x^{p^N} - 1|$$

Donc x est une p^N-ième racine de l'unité. □

Proposition 2.3.5. *Si* $|x| < p^{-1/(p-1)}$ *alors*

$$\log_p \exp(x) = x$$

et

$$\exp \log_p(1+x) = 1 + x$$

Remarquons que l'application naturelle de $Aut_{cont}(\mathbb{C}_p)$ dans $G_{\mathbb{Q}_p} = Gal(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$ est un isomorphisme de groupes. En effet, l'injectivité résulte de la densité de $\mathbb{Q}_p^{alg}$ dans $\mathbb{C}_p$ et la surjectivité, de ce qu'un élément de $Gal(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$ agit par une isométrie sur $\mathbb{Q}_p^{alg}$. Donc, si $\sigma \in Gal(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$, on peut grâce à l'isomorphisme précédent, considérer $\sigma \in Aut_{cont}(\mathbb{C}_p)$. Donc, par continuité, $\log_p(1+\sigma x) = \sigma \log_p(1+x)$ et donc par unicité de $\log_p$, on a $\sigma^{-1} \log_p(\sigma\alpha) = \log_p(\alpha)$ pour $\alpha \in \mathbb{C}_p^*$ i.e $\log_p(\sigma\alpha) = \sigma(\log_p(\alpha))$. Par conséquent, pour $\alpha \in \mathbb{Q}_p^{alg}$, $\log_p(\alpha) \in \mathbb{Q}_p(\alpha)$.

2.3.2 Les fonctions continues

Commençons par introduire des polynômes qui auront un rôle central dans la caractérisation des fonctions continues. Ce sont les polynômes binomiaux définis par

$$\binom{X}{n} = \frac{X(X-1)...(X-n)}{n!}.$$

Par conséquent $\binom{X}{n}$ est un polyôme de degré n et si X est un entier, on obtient un coefficient binomial. De plus, par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$, et par continuité des polynômes,

on a $\binom{X}{n} \in \mathbb{Z}_p$ si $X \in \mathbb{Z}_p$. Cependant, ce résultat n'est pas vrai pour les extensions de $\mathbb{Q}_p$ (voir le livre de Washington [5]).

De plus, un théorème classique de Mahler que l'on démontre dans la partie sur l'analyse fonctionnelle p-adique (voir théorème 3.1.2) énonce que toute fonction continue $f : \mathbb{Z}_p \to \mathbb{Q}_p$ peut s'écrire de manière unique sous la forme

$$f(X) = \sum_{n=0}^{+\infty} a_n \binom{X}{n}$$

où $a_n \to 0$ quand $n \to +\infty$.

Lemme 2.3.3. *Soit $P_i(X) = \sum_{n=0}^{+\infty} a_{n,i} X^n$, pour $i \in \mathbb{N}$, une suite de série formelle qui convergent sur un sous-ensemble fixé D de $\mathbb{C}_p$ et supposons*
(1) $a_{n,i} \to a_{n,0}$ quand $i \to +\infty$ pour tout $n \in \mathbb{N}$.
(2) Pour chaque $X \in D$ et tout $\varepsilon > 0$, il existe $n_0 = n_0(X, \varepsilon)$ tel que $|\sum_{n \geq n_0} a_{n,i} X^n| < \varepsilon$ uniformément en i.
Alors

$$\lim_{i \to +\infty} P_i(x) = P_0(X)$$

Démonstration. Soient ε et X, on choisit n_0 comme ci-dessus. Alors

$$|P_i(X) - P_0(X)| \leq \max_{n \leq n_0} \{\varepsilon, |a_{n,0} - a_{n,i}|.|X^n|\} = \varepsilon$$

pour i suffisamment grand. □

Proposition 2.3.6. *Supposons $r < p^{-1/(p-1)} < 1$ et*

$$f(X) = \sum_{n=0}^{+\infty} a_n X^n$$

avec $|a_n| \leq M r^n$ où $M \in \mathbb{Q}_+^*$. Alors $f(X)$ peut être exprimée comme une série formelle de rayon de convergence au moins $R = (r p^{1/(p-1)})^{-1} > 1$.

Démonstration. Soit

$$P_i(X) = \sum_{n \leq i} a_n \binom{X}{n} = \sum_{n \leq i} a_{n,i} X^n, i \in \mathbb{N}^*$$

Alors

$$a_{n,i} = a_n \frac{entier}{n!} + a_{n+1} \frac{entier}{(n+1)!} + ... + a_i \frac{entier}{i!}$$

Donc

$$|a_{n,i}| \leq \max_{j \geq n} \left| \frac{a_j}{j!} \right| \leq M R^{-n} \leq M(\max_{j \geq n} \frac{r^j}{|j!|}) \leq M(\max_{j \geq n} R^{-j}) \leq M R^{-n}$$

De plus,

$$|a_{n,i} - a_{n,i+k}| = |a_{i+1}\frac{entier}{(i+1)!} + ... + a_{i+k}\frac{entier}{(i+k)!}| \leq MR^{-(i+1)} \underset{i\to+\infty}{\longrightarrow} 0$$

Donc la suite $(a_{n,i})_{i\in\mathbb{N}^*}$ est de Cauchy. Posons $a_{n,0} = \lim\limits_{i\to+\infty} a_{n,i}$. Alors $|a_0| < MR^{-n}$. Soit $P_0(X) = \sum_{n=0}^{+\infty} a_{n,0}X^n$, donc P_0 et également les polynômes $P_1, P_2, ...$ convergent dans $D = \{x \in \mathbb{C}_p | \, |x| < R\}$.
Finalement, si $X \in D$, alors

$$\left| \sum_{n\geq n_0} a_{n,i}X^n \right| \leq \max_{n\geq n_0}\{MR^{-n}|X|^n\} \underset{n_0\to+\infty}{\longrightarrow} 0$$

uniformément en i. Donc $\lim\limits_{i\to+\infty} P_i(x) = P_0(X)$ d'après le lemme précédent, donc $f(X)$ est analytique sur D. □

2.3.3 Applications sur $\mathbb{Z}_p$

Pour plus de facilité, nous utiliserons la notation $q = p$ si $p \neq 2$ et $q = 4$ si $p = 2$.
Soit $a \in \mathbb{Z}_p^*$ et soit $\omega(a)$ son représentant de Teichmüller. Définissons

$$\langle a \rangle := a\omega(a)^{-1}$$

, donc $\langle a \rangle \equiv 1 \, mod \, q$. Par conséquent $\log_p(a) = \log_p\langle a \rangle$.
Remarquons aussi que $\log_p(a) = \frac{\log_p(a^{\varphi(q)})}{\varphi(q)}$ puisque $a^{\varphi(q)} \equiv 1 \, mod \, q$
On peut définir également $\langle a \rangle^x = \exp(x \log_p\langle a \rangle) = \exp(x \log_p(a))$. Comme $|\log_p\langle a \rangle| \leq |q| = \frac{1}{q}$, $\langle a \rangle^x$ converge si $|x| < qp^{-1/(p-1)} > 1$. D'après la proposition 2.3.1, on a que $\langle a \rangle^1 = \langle a \rangle$ et par conséquent, si $n \in \mathbb{Z}$, alors $\langle a \rangle^n$ coïncide avec la définition usuelle.
De plus, la dernière proposition nous donne que

$$\langle a \rangle^x = (1 + \langle a \rangle - 1)^x = \sum_{n=0}^{+\infty} \binom{x}{n} (\langle a \rangle - 1)^n$$

Or comme $|\langle a \rangle - 1| \leq q^{-1}$, on peut poser $r = q^{-1}$ et donc la série représente une fonction analytique de rayon de convergence au moins $qp^{-1/(p-1)}$. Finalement,

$$\exp(x \log_p\langle a \rangle) = \sum_{n=0}^{+\infty} \binom{x}{n} (\langle a \rangle - 1)^n$$

puisque se sont tous les deux des fonctions analytiques qui sont égales sur $\mathbb{N}$, puis par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$ l'égalité en découle.

2.4 Première construction des L fonctions p-adiques

Ayant démontré que $L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} \in \mathbb{Q}, \forall n \in \mathbb{N}^*$, nous allons tenter de trouver des fonctions p-adiques qui interpolent ces valeurs des fonctions L, nous les appelleront L fonctions p-adiques.
Posons tout d'abord

$$H(s,a,F) = \sum_{\substack{m \equiv a(F) \\ m>0}} m^{-s} = \sum_{n=0}^{+\infty} \frac{1}{(a+nF)^s} = F^{-s}\zeta(s, \frac{a}{F})$$

où s est une varable complexe, a et F sont des entiers vérifiants $0 < a < F$, et $\zeta(s,b) = \sum_{n=0}^{+\infty} \frac{1}{(b+n)^s}$ est la foncion zeta de Hurwitz. Alors,

$$H(1-n,a,F) = -\frac{F^{n-1}B_n(a/F)}{n} \in \mathbb{Q}, n \geq 1$$

et H a un pôle simple en $s=1$ de résidu $\frac{1}{F}$.

Théorème 2.4.1. *(Von Staudt-Clausen)*
Soit n un entier positif pair. Alors

$$B_n + \sum_{\substack{(p-1)|n \\ p \in \mathscr{P}}} \frac{1}{p} \in \mathbb{Z}$$

Par conséquent, $\forall n, \forall p \in \mathscr{P}, pB_n \in \mathbb{Z}_p$

Une preuve de ce théorème est donnée dans le livre de Lawrence C. Washington [5].

Théorème 2.4.2. *Supposons $q|F$ et $p \nmid a$. Alors il existe une fonction p-adique méromorphe $H_p(s,a,F)$ définie sur*

$$\{x \in \mathbb{C}_p || x| < qp^{-1/(p-1)} > 1\}$$

telle que

$$H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F), n \geq 1.$$

En particulier, si $n \equiv 0 \, mod \, \varphi(q)$ alors

$$H_p(1-n,a,F) = H(1-n,a,F)$$

La fonction H_p est analytique sauf pour un pôle simple en $s=1$ de résidu $\frac{1}{F}$.

Démonstration. Posons

$$H_p(s,a,F) = \frac{1}{s-1}\frac{1}{F}\langle a \rangle^{1-s} \sum_{j=0}^{+\infty} \binom{1-s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

Commençons par montrer la convergence. D'après le théorème de Von Staudt-Clausen, on a $|(B_j)(F/a)^j| \leq p|q|^j$. Par conséquent, la proposition 2.3.2 avec $r = |q| = \frac{1}{q}$ nous donne que

$$\sum_{j=0}^{+\infty} \binom{s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

est analytique sur $D = \{s \in \mathbb{C}_p | \, |1-s| < qp^{-1/(p-1)}\}$. Comme $qp^{-1/(p-1)} > 1$, on a $D = \{s \in \mathbb{C}_p | \, |s| < qp^{-1/(p-1)}\}$, donc

$$\sum_{j=0}^{+\infty} \binom{1-s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

est analytique sur D. D'une manière similaire $\langle a \rangle^s$, et donc $\langle a \rangle^{1-s}$, est analytique sur D. Finalement, $(1-s)H_p(s,a,F)$ est analytique sur D.
On a

$$\begin{aligned} H_p(1-n,a,F) &= \frac{-1}{nF}\langle a \rangle^n \sum_{j=0}^{n} \binom{n}{j} (B_j) \left(\frac{F}{a}\right)^j \\ &= -\frac{F^{n-1}\omega^{-n}(a)}{n} B_n(\frac{a}{F}) \\ &= \omega^{-n}(a) H(1-n,a,F), n \geq 1 \end{aligned}$$

Pour $s = 1$, on a un résidu

$$\frac{1}{F}\langle a \rangle^0 \sum_{j=0}^{+\infty} \binom{0}{j} (B_j) \left(\frac{F}{a}\right)^j = \frac{1}{F}$$

□

Nous sommes maintenant prêt à construire les L fonctions p-adiques. Soit χ un caractère de Dirichlet. Si l'on fixe une fois pour toute un plongement de $\mathbb{Q}^{alg}$ dans $\mathbb{C}_p$ (ce qui est légitime car $(.)^{alg}$ est un foncteur covariant de la catégorie des corps dans la catégorie des corps algébriquements clos), on peut regarder χ comme étant à valeur dans $\mathbb{C}_p$. De plus, on peut remarquer que $\omega : \mathbb{Z} \subset \mathbb{Z}_p \to \mathbb{C}_p$ (représentant de Teichmüller) définit un caractère de Dirichlet p-adique de conducteur q et d'ordre $\varphi(q)$. Ainsi, ω génère le groupe des caractères de Dirichlet modulo q.

Théorème 2.4.3. *Soit χ un caractère de Dirichlet de conducteur f et soit F un multiple de q et f. Alors il existe une fonction p-adique méromorphe (analytique si $\chi \neq 1$) $L_p(\chi, s)$ sur $\{s \in \mathbb{C}_p | \, |s| < qp^{-1/(p-1)}\}$ telle que*

$$L_p(\chi, 1-n) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, n \geq 1$$

Si $\chi = 1$ alors $L_p(1, s)$ est analytique sauf en un pôle simple pour $s = 1$ de résidu $(1 - \frac{1}{p})$. En effet, on a la formule

$$L_p(\chi, s) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{+\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j$$

Démonstration. Vérifions que la formule donnée possède les bonnes propriétés. On a

$$L_p(\chi, s) = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(s, a, F)$$

et l'analycité de L_p découle de l'analycité de H_p. Quand $s = 1$, $L_p(\chi, s)$ a pour résidu $\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)(1/F)$. Si $\chi = 1$, alors cette somme est égale à $1 - \frac{1}{p}$. Si $\chi \neq 1$, alors la somme est

$$\frac{1}{F}\sum_{a=1}^{F}\chi(a) - \sum_{b=1}^{F/p}\chi(pb).$$

La première somme vaut 0. Si $p|f$ alors $\chi(pb) = 0$, pour tout b. Si $p \nmid f$, alors $f|(F/p)$, donc la somme vaut également 0. Par conséquent $L_p(\chi, s)$ n'a pas de pôle en $s = 1$ si $\chi \neq 1$. Si $n \geq 1$ alors

$$\begin{aligned}
L_p(\chi, 1-n) &= \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)H_p(1-n, a, F)\\
&= -\frac{1}{n}F^{n-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right)\\
&= -\frac{1}{n}F^{n-1}\sum_{a=1}^{F}\chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right)\\
&\quad + \frac{1}{n}p^{n-1}\left(\frac{F}{p}\right)^{n-1}\sum_{b=1}^{F/p}\chi\omega^{-n}(pb)B_n\left(\frac{b}{F/p}\right)
\end{aligned}$$

Si $p|f_{\chi\omega^{-n}}$ alors $\chi\omega^{-n}(pb) = 0$. Sinon, $f_{\chi\omega^{-n}}|(F/p)$. D'après la proposition 2.2 on obtient,

$$\begin{aligned}
L_p(\chi, 1-n) &= -\frac{1}{n}(B_{n,\chi\omega^{-n}} - \chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}})\\
&= -\frac{1}{n}(1 - \chi\omega^{-n}(p)p^{n-1})B_{n,\chi\omega^{-n}}
\end{aligned}$$

Ce qui complète la preuve. □

Remarque 2.4.1. *Le terme* $(1-\chi\omega^{-n}(p)p^{n-1})$ *s'appelle le facteur d'Euler en p de* $L_p(\chi, s)$. *De manière générale, les L fonctions p-adiques sont la réunion des* $p-1$ *branches qui correspondent aux* $L_p(\chi\omega^j, s)$ *pour* $j = 0, 1, ..., p-2$. *Si* χ *est un caractère impaire alors n et* $\chi\omega^{-n}$ *ont différentes parités et donc* $B_{n,\chi\omega^{-n}} = 0$. *Par conséquent, par analycité* $L_p(\chi, s)$ *est identiquement nulle pour tout caractère impaire. Si* χ *est pair alors* $B_{n,\chi\omega^{-n}} \neq 0$ *et donc* $L_p(\chi, s)$ *n'est pas identiquement nulle.*

2.4.1 Cas $s = 1$

Théorème 2.4.4. *Soit* χ *un caractère de Dirichlet non trivial pair de conducteur* f. *Soit* ζ *une racine primitive* f*-ième de l'unité, soit* $\bar{\chi} = \chi^{-1}$, *et* $G(\chi) = \sum_{a=1}^{f} \chi(a)\zeta^a$ *la somme de associée. Alors*

$$L_p(\chi, 1) = -\left(1 - \frac{\chi(p)}{p}\right) \frac{1}{G(\chi^{-1})} \sum_{a=1}^{f} \chi^{-1}(a) \log_p(1 - \zeta^a)$$

Une démonstration de ce théorème sera donnée dans la dernière section.

Remarque 2.4.2. $L_p(1, \chi)$ *et* $L(1, \chi)$ *ne différencie que d'un facteur d'Euler ! Or l'interpolation des L fonctions s'est effectuée seulement sur les entier négatifs (ou nuls). Il n'y a donc pas de lien à priori entre* $L_p(1, \chi)$ *et* $L(1, \chi)$..

Effectuons un petit aparté philosophique en remarquant que cela révolutionne notre vision à priori des L fonctions p-adiques. En effet, les L fonctions p-adiques ne se contenteraient pas de compléter les L fonctions complexes comme le laisserait sous-entendre la dichotomie du théorème d'Ostrowsky, mais supplémentent les L fonctions complexes ; au sens où les L fonctions p-adiques et complexes ressemblent plus (philosophiquement) à des projections sur respectivement, le "monde" p-adique et le "monde" complexe, qu'à une simple restriction ensembliste.
J'aimerait traduire mathématiquement cette hypothèse, mais mes explications sont pour le moment seulement fantaisistes.

3 Distributions p-adiques

Dans toute cette partie, nous allons construire des espaces de Banach et anneaux de fonctions p-adiques ainsi que leurs duaux dans le but d'obtenir une théorie de distributions sur $\mathbb{C}_p$. Elle ne constitue qu'un bref résumé de la construction founie par Colmez dans ces cours de M2.
On fixe L un sous-corps fermé de $\mathbb{C}_p$. On l'a choisit fermé pour que L soit complet.

3.1 Un peu d'analyse fonctionnelle p-adique

Dans cette partie nous introduirons de nombreux espaces p-adiques et exhiberons une base pour chacun d'entre eux afin de mieux les décrire. Cette courte présentation sur les espaces p-adiques est tirée des cours de colmez de M2 (voir [1]). Ainsi, les longues ou triviales démonstrations seront épargnées et on s'en réfèrera si besoin est.

3.1.1 Généralitées sur les espaces de Banach p-adiques

Définition 3.1.1. *(L-Banach)*
Si B est un L-espace vectoriel, une valuation v_B sur B est une fonction à valeurs dans $\mathbb{R} \cup \{+\infty\}$ qui vérifie les propriétés suivantes :
(i) $v_B(x) = +\infty \Leftrightarrow x = 0$
(ii) $v_B(x+y) \geq \inf\{v_B(x), v_B(y)\}$ *quels que soient* $x, y \in B$
(iii) $v_B(\lambda x) = v_p(\lambda) + v(x)$ *quels que soient* $\lambda \in L, x \in B$ *Un L-Banach est un L-espace vectoriel topologique, la topologie étant définie par une valuation v_B pour laquelle il est complet. Une application $f : B_1 \to B_2$ est un morphisme de L-Banach si elle est L-linéaire et continue ; c'est une isométrie de L-Banach de B_1 dans B_2 si en plus $v_{B_2}(f(x)) = v_{B_1}(x)$ pour tout $x \in B_1$.*

Exemple 3.1.1. *(i)Si I 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. 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.*
(ii) Si B est un L-Banach, on note B' son dual topologique (i.e l'ensemble des formes linéaires continues $f : B \to L$). B' muni de la topologie forte définie par la valuation $v_{B'}$ donnée par la formule

$$v_{B'}(f) = \inf_{x\in B\setminus\{0\}} v_p(f(x)) - v_p(x)$$

est un L-Banach.

Proposition 3.1.1. *(i) Si $f : B_1 \to B_2$ est un morphisme de L-Banach, alors f^{-1} est continue et donc f est un isomorphisme de L-Banach. (Théorème d'isomorphisme de Banach).*
(ii) Une limite simple d'applications linéaires continues sur un L-Banach est continue (Théorème de Banach-Steinaus).

Définition 3.1.2. *(Bases orthonormales et bases de Banach)*
Soit B un L-Banach. Une famille $(e_i)_{i\in I}$ d'éléments de B est une base orthonormale de B si l'application $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i e_i$ de $\ell^0_\infty(I, B)$ dans B est une isométrie de L-Banach. On dit que c'est une base de Banach si cette appliication est seulement un isomorphisme de L-Banach.
Autrement dit, une famille $(e_i)_{i\in I}$ est une base orthonormale de B si elle vérifie :
(i) tout élément $x \in B$ 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 tendent 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). Cela implique, d'après le théorème d'isomorphisme de Banach que les deux valuations sont équivalentes.
Une famille $(e_i)_{i\in I}$ d'éléments de B est une base orthogonale s'il existe une famille $(\lambda_i)_{i\in I}$ d'éléments de L telle que, quelque soit la famille $(x_i)_{i\in I}$ d'éléments de L, on ait $v_B(\sum_{i\in I} x_i\lambda_i e_i) = \inf_{i\in I} v_p(x_i)$. Une base orthonormale est donc orthogonale.

Proposition 3.1.2. *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 $B^0 = \{x \in B | v_B(B) \geq 0\}$, alors $(e_i)_{i\in I}$ est une base orthonormale de B si ett seulement si $(\bar{e}_i)_{i\in I}$ est une base algébrique du k_L-espace vectoriel $\bar{B} = B^0/\pi_L B^0$.

Cette proposition, dont une preuve est fournie dans [1], légitimise la quête d'une base Banach des espaces qui vont être construits.

La partie suivante va traiter des fonctions continues p-adiques et sera principalement la prolongation de la partie les concernant de la section 2.

3.1.2 Fonctions continues (suite)

Soit $\mathscr{C}^0(\mathbb{Z}_p, L)$ l'ensemble des fonctions continues de $\mathbb{Z}_p$ dans L. Comme $\mathbb{Z}_p$ est compact, toute fonction continue est bornée. Cela permet de définir une valuation $v_{\mathscr{C}^0}$ sur $\mathscr{C}^0(\mathbb{Z}_p, L)$ par

$$v_{\mathscr{C}^0}(f) = \inf_{x\in\mathbb{Z}_p} v_p(f(x))$$

ce qui en fait un L-Banach.

En utilisant les polynômes binomiaux définie dans la section 2, on a la proposition suivante.

Proposition 3.1.3. *Si $n \in \mathbb{N}$, alors $v_{\mathscr{C}^0}\left(\binom{x}{n}\right) = 0$*

Démonstration. On a $\binom{n}{n} = 1$ et donc $v_{\mathscr{C}^0}\left(\binom{x}{n}\right) \leq 0$. De plus, $\binom{n+k}{n} \in \mathbb{N}, \forall k \in \mathbb{N}$, donc $v_p\left(\binom{n+k}{n}\right) \geq 0, \forall k \in \mathbb{N}$. Comme $n + \mathbb{N}$ étant dense dans $\mathbb{Z}_p$, on en déduit que

$v_p\left(\binom{x}{n}\right) \geq 0, \forall x \in \mathbb{Z}_p$. □

Si $z \in L$ vérifie $v_p(z-1) > 0$, alors la série $\sum_{n=0}^{+\infty} \binom{x}{n}(z-1)^n$ converge normalement d'après la proposition précédente et définit donc une fonction continue $\phi_z(x)$ en $x \in \mathbb{Z}_p$. D'autre part, si $k \in \mathbb{N}$, on a $\phi_z(k) = z^k$ ce qui nous permet de noter $x \mapsto z^x$ la fonction $x \mapsto \phi_z(x)$. On remarque que $z^{x+y} = z^x z^y, \forall a, y \in \mathbb{Z}_p$, car cette formule est vraie si $x, y \in \mathbb{N}$, or $\mathbb{N}^2$ est dense dans $\mathbb{Z}_p^2$.

Nous allons à présent donner une écriture simpathique des fonctions continues en termes de leurs coefficients de Mahler. Commençons par définir la dérivée k-ième $\phi^{[k]}$ d'une fonction quelconque ϕ par récurrence à partir des formules

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

et si $n \in \mathbb{N}$, on définit le n-ième coefficient de Mahler $a_n(\phi)$ par la formule $a_n(\phi) := \phi^{[n]}(0)$. On a également les formules

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

Lemme 3.1.1. *Si P_n désigne le polynôme binomial $\binom{x}{n}$, alors*

(i) $P_n^{[k]} = P_{n-k}$ si $k \leq n$, 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. Par une simple récurrence □

Théorème 3.1.1. *(Mahler)*
(i) Si $\phi \in \mathscr{C}^0(\mathbb{Z}_p, L)$, alors

1. $\lim_{n \to +\infty} a_n(\phi) = 0$
2. $\sum_{n=0}^{+\infty} a_n(\phi) \binom{x}{n} = \phi(x)$

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

Démonstration. La formule définissant les coefficients de Mahler montre que l'on a $v_p(a_n(\phi)) \geq v_{\mathscr{C}^0}(\phi)$, pour tout $n \in \mathbb{N}$. L'application $\phi \mapsto a(\phi)$ est donc continue de $\mathscr{C}^0(\mathbb{Z}_p, L)$ dans $\ell_\infty(\mathbb{N}, L)$, et on a $v_{\ell_\infty}(a(\phi)) \geq v_{\mathscr{C}^0}(\phi)$.

Soit B le sous-espace de $\mathscr{C}^0(\mathbb{Z}_p, L)$ des ϕ tels que $a(\phi) \in \ell_\infty^0(\mathbb{N}, L)$. B est fermé dans $\mathscr{C}^0(\mathbb{Z}_p, L)$ puisque $\ell_\infty^0(\mathbb{N}, L)$ est dense dans $\ell_\infty(\mathbb{N}, L)$.

Si $a = (a_n)_{n \in \mathbb{N}} \in \ell_\infty^0(\mathbb{N}, L)$, la série $\phi_a = \sum_{n=0}^{+\infty} a_n \binom{x}{n}$ converge normalement dans $\mathscr{C}^0(\mathbb{Z}_p, L)$ d'après la proposition 3.1.2 et on a $v_{\mathscr{C}^0}(\phi_a) \geq v_{\ell_\infty}(a)$. D'autre part, le lemme précédent donne $\phi_a^{[k]}(x) = \sum_{n=0}^{+\infty} a_{n+k} \binom{x}{n}$ et donc $a(\phi_a) = a$.

L'application $\phi \mapsto a(\phi)$ est injective car si $a(\phi) = 0$, alors $\phi(k) = 0$ quel que soit $k \in \mathbb{N}$. On conclut par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$. De plus, si $\phi \in B$ alors $\phi - \phi_{a(\phi)} = 0$ puisque $a(\phi - \phi_{a(\phi)} = 0$ et a est injective. Donc, si $\phi \in B$, alors ϕ satisfait la condition (i) $b)$. Egalement, on a

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

ce qui montre le (ii).

Maintenant, introduisons un lemme afin de montrer que $B = \mathscr{C}^0(\mathbb{Z}_p, L)$.

Lemme 3.1.2. *Si $\phi \in \mathscr{C}^0(\mathbb{Z}_p, L)$, il existe $k \in \mathbb{N}$ tel que $v_{\mathscr{C}^0}(\phi^{[p^k]} \geq v_{\mathscr{C}^0}(\phi) + 1$.*

Démonstration. Comme $\mathbb{Z}_p$ est compact, ϕ est uniformément continue sur $\mathbb{Z}_p$, et par conséquent il existe $k \in \mathbb{N}$ tel que l'on ait $v_p(\phi(x+p^k)-\phi(x)) \geq v_{\mathscr{C}^0}(\phi)+1$ quel que soit $x \in \mathbb{Z}_p$. De plus, on a la formule

$$\phi^{[p^k]}(x) = \phi(x + p^k) - \phi(x) + \left(\sum_{i=1}^{p^k-1} (-1)^i \binom{p^k}{i} \phi(x + p^k - i) \right) + (1 + (-1)^{p^k})\phi(x)$$

Or $\forall 1 \leq i \leq p^k - 1$, $v_p(\binom{p^k}{i}) \geq 1)$, donc le terme du milieu a une valuation supérieure à $v_{\mathscr{C}^0}(\phi)+1$. De même, $(1+(-1)^{p^k})\phi(x) = 0$ si $p = 2$ et de valuation supérieure à $v_{\mathscr{C}^0}(\phi)+1$ sinon. On a donc bien le résultat. □

Revenons à la preuve de $B = \mathscr{C}^0(\mathbb{Z}_p, L)$. En répétant ce lemme, ainsi qu'en utilisant l'égalité $(\phi^{[k_1]})^{[k_2]} = \phi^{[k_1+k_2]}$, on obtient que $v_p(a_n(\phi))$ tend vers $+\infty$ quand n tend vers $+\infty$, puisque $v_p(a_n) \geq v_{\mathscr{C}^0}(\phi^{[N]})$ si $n \geq N$. □

Corollaire 3.1.1. *Les $\binom{x}{n}$, pour $n \in \mathbb{N}$, forment une base orthonormale de $\mathscr{C}^0(\mathbb{Z}_p, L)$.*

Le théorème de Mahler nous donne donc que toute fonction continue p-adique f peut s'écrire sour la forme :

$$f(x) = \sum_{n=0}^{+\infty} \binom{x}{n} a_n(f)$$

Une autre décomposition nous sera utile par la suite : c'est *la décomposition en ondelettes*. Pour cela, nous allons introduire une nouvelle classe de fonctions que sont les fonctions localement constantes.
Si $h \in \mathbb{N}$, on note $LC_h(\mathbb{Z}_p, L)$ l'ensemble des fonctions de $\mathbb{Z}_p$ dans L dont la restriction à $a + p^h\mathbb{Z}_p$ est constante, quel que soit $a \in \mathbb{Z}_p$. On note $LC(\mathbb{Z}_p, L)$ l'espace des fonctions localement constantes sur $\mathbb{Z}_p$, à valeurs dans L. Comme $\mathbb{Z}_p$ est compact, c'est la réunion croissante des $LC_h(\mathbb{Z}_p, L)$, pour $h \in \mathbb{N}$.

Exemple 3.1.2. *Si z est une racine de l'unité d'ordre une puissance de p, disons p^n, alors $x \mapsto z^x \in LC_n(\mathbb{Z}_p, L)$.*

Lemme 3.1.3. *$LC(\mathbb{Z}_p, L)$ est dense dans $\mathscr{C}^0(\mathbb{Z}_p, L)$.*

Démonstration. Comme $\mathbb{Z}_p$ est compact, toute fonction continue sur $\mathbb{Z}_p$ est uniformément continue. Soit $\phi \in \mathscr{C}^0(\mathbb{Z}_p, L)$, soit $\phi_n = \sum_{i=0}^{p^n-1} \phi(i)\mathbf{1}_{i+p^n\mathbb{Z}_p} \in LC(\mathbb{Z}_p, L)$, et soit $C > 0$, par uniforme continuité de ϕ il existe $n \in \mathbb{N}$ tel que si $v_p(x-y) \geq n$ alors $v_p(\phi(x)-\phi(y)) \geq C$. Si $x \in \mathbb{Z}_p$, il existe $i \in \{0, ..., p^n-1\}$ tel que $x \in i + p^n\mathbb{Z}_p$, donc $v_p(\phi(x) - \phi_n(i)) = v_p(\phi(x) - \phi(i)) \geq C$. On en déduit que $v_{\mathscr{C}^0}(\phi - \phi_n) \geq C$, ce qui permet de conclure. □

Si $i \in \mathbb{N}$, on note $\ell(i)$ le plus petit entier n vérifiant $p^n > i$. On a donc

$$\ell(0) = 0 \quad et \quad \ell(i) = \left\lfloor \frac{\log i}{\log p} \right\rfloor + 1, \quad si\ i \geq 1$$

Proposition 3.1.4. *(i) Les $\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p}$, pour $0 \leq i \leq p^h-1$, forment une base de $LC_h(\mathbb{Z}_p, L)$.*
(ii) Les $\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p}$, pour $i \in \mathbb{N}$, forment une base de $LC(\mathbb{Z}_p, L)$.
(iii) Les $\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p}$, pour $i \in \mathbb{N}$, forment une base orthonormale de $\mathscr{C}^0(\mathbb{Z}_p, L)$.

Démonstration. *(i)* Par définition, les $\mathbf{1}_{i+p^h\mathbb{Z}_p}$, pour $0 \leq i \leq p^h - 1$, forment une base de $LC_h(\mathbb{Z}_p, L)$. Comme

$$\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p} = \sum_{j=0}^{p^h-\ell(i)-1} \mathbf{1}_{i+jp^{\ell(i)}p^h\mathbb{Z}_p}, \quad si\ i \leq p^h - 1,$$

La matrice permettant de passer des $\mathbf{1}_{i+p^h\mathbb{Z}_p}$ aux $\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p}$ étant triangulaire avec que des 1 sur la diagonale, elle est donc inversible.

Le *(ii)* et *(iii)* se déduisent par densité de $LC(\mathbb{Z}_p, L)$ dans $\mathscr{C}^0(\mathbb{Z}_p, L)$, et par densité de l'espace des suites nulles en dehors d'un ensemble fini dans $\ell^0_\infty(\mathbb{N}, L)$. On conclut par continuité. □

Définition 3.1.3. *On appelle base d'ondelettes la base orthonormale de $\mathscr{C}^0(\mathbb{Z}_p, L)$ constituée des $\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p}$, pour $i \in \mathbb{N}$. Si $\phi \in \mathscr{C}^0(\mathbb{Z}_p, L)$, et $\phi = \sum_{i\in\mathbb{N}} b_i(\phi)\mathbf{1}_{i+p^{\ell(i)}\mathbb{Z}_p}$ est la décomposition de ϕ en ondelettes, et les $b_i(\phi)$, $i \in \mathbb{N}$, sont les coefficients d'amplitude.*

3.1.3 Fonctions localement analytiques

Si $a \in L$ et si $r \in \mathbb{R}$, soit $\mathscr{D}(a, r)$ le disque fermé $\{x \in \mathbb{C}_p | v_p(x-a) \geq r\}$. Une fonction $\phi : \mathscr{D}(a, r) \to \mathbb{C}_p$ est L-analytique s'il existe une suite $a_k(\phi, a)$, où $k \in \mathbb{N}$, d'éléments de L, telle que $v_p(a_k(\phi, a))+kr$ tend vers $+\infty$ quand k tend vers $+\infty$, et $\phi(x) = \sum_{n=0}^{+\infty} a_k(\phi, a)(x-a)^k$ quel que soit $x \in \mathscr{D}(a, r)$. On note $A_n(\mathscr{D}(a, r), L)$ l'ensemble des fonctions analytiques sur $\mathscr{D}(a, r)$ et que l'on munit de la valuation $v_{\mathscr{D}(a,r)}$ définie par

$$v_{\mathscr{D}(a,r)}(\phi) = \inf_{k\in\mathbb{N}} v_p(a_k(\phi, a)) + kr$$

qui en fait un L-Banach.

Remarque 3.1.1. *Les $\mathbf{1}_{\mathscr{D}(a,r)}\frac{(x-a)^k}{p^{\lfloor kr \rfloor}}$, pour $k \in \mathbb{N}$, forment une base de Banach de $A_n(\mathscr{D}(a, r), L)$, et même une base orthonormale si $r \in \mathbb{Z}$.*

Proposition 3.1.5. *Si $\phi_1, \phi_2 \in A_n(\mathscr{D}(a,r), L)$, alors $\phi_1\phi_2 \in A_n(\mathscr{D}(a,r), L)$ et*

$$v_{\mathscr{D}(a,r)}(\phi_1\phi_2) = v_{\mathscr{D}(a,r)}(\phi_1) + v_{\mathscr{D}(a,r)}(\phi_2)$$

On démontre l'égalité entre les valuations en raisonnement par double inégalité puis en utilisant le produit de Cauchy de deux séries.

Proposition 3.1.6. *Si $\phi \in A_n(\mathscr{D}(a,r), L)$, alors*

$$v_{\mathscr{D}(a,r)}(\phi) = \inf_{x \in \mathscr{D}(a,r)} v_p(\phi(x))$$

La preuve n'ayant que peu d'intérêt, on renvoit le lecteur intéressé au cours de M2 de Colmez [1].

Etudions maintenant les fonctions localement analytiques sur $\mathbb{Z}_p$.
Si $h \in \mathbb{N}$, soit $LA_h(\mathbb{Z}_p, L)$ l'espace des fonctions $\phi : \mathbb{Z}_p \to L$ dont la restriction à $a + p^h\mathbb{Z}_p$ est la restrictiond'une fonction L-analytique $\phi_{a,h}$ sur $\mathscr{D}(a,h)$, quel que soit $a \in \mathbb{Z}_p$. On munit $LA_h(\mathbb{Z}_p, L)$ de la valuation v_{LA_h} définie par

$$v_{LA_h}(\phi) = \inf_{a \in \mathbb{Z}_p} v_{\mathscr{D}(a,h)}(\phi_{a,h})$$

qui en fait un L-Banach.
Soit $LA(\mathbb{Z}_p, L)$ l'espace des fonctions localement analytiques sur $\mathbb{Z}_p$. C'est la réunion des $LA_h(\mathbb{Z}_p, L)$, où $h \in \mathbb{N}$, et on le munit de la topologie définie par la famille des valuations v_{LA_h} pour $h \in \mathbb{N}$.

Remarque 3.1.2. *On peut aussi donner une autre description de v_{LA_h}.*
En effet, si $a \in \mathbb{Z}_p$, il existe une suite $a_k(\phi, a)$, $k \in \mathbb{N}$, d'éléments de L telle que l'on ait $\phi(x) = \sum_{k=0}^{+\infty} a_k(\phi, a) \left(\frac{x-a}{p^h}\right)^k$ quel que soit $x \in a + p^h\mathbb{Z}_p$. On a alors $v_{\mathscr{D}(a,h)}(\phi_{a,h}) = \inf_{k\in\mathbb{N}} v_p(a_k(\phi, a))$, et donc

$$v_{LA_h}(\phi) = \inf_{a \in S} \inf_{k \in \mathbb{N}} v_p(a_k(\phi, a))$$

si $S \subset \mathbb{Z}_p$ contient un système de représentants de $\mathbb{Z}_p/p^h\mathbb{Z}_p$.

Etant donné $h \in \mathbb{N}$, on peut écrire tout entier n de manière unique sous la forme

$$n = (m(n) + 1)p^h - i(n)$$

avec $1 \leq i(n) \leq p^h$ et $m(n) \in \mathbb{N}$. Soit alors $e_{h,n}(x)$ la fonction

$$e_{h,n}(x) = \mathbf{1}_{n+p^h\mathbb{Z}_p}(x) \left(\frac{x + i(n)}{p^h}\right)^{m(n)}.$$

Lemme 3.1.4. *Les $e_{h,n}$ pour $n \in \mathbb{N}$ forment une base orthonormale de $LA_h(\mathbb{Z}_p, L)$. Plus précisément, si $\phi \in LA_h(\mathbb{Z}_p, L)$ et si $\phi_i(x) = \phi(-i + p^h x)$, alors :*
(i) ϕ_i est analytique sur $\mathbb{Z}_p$ et donc $\phi_i(x) = \sum_{m\in\mathbb{N}} \alpha_{i,m} x^m$, où $\alpha_{i,m} \underset{m\to+\infty}{\longrightarrow} 0$,
(ii) $\phi = \sum_{i=1}^{p^h} \sum_{mm\in\mathbb{N}} \alpha_{i,m} e_{h,(m+1)p^h-i} = \sum_{n\in\mathbb{N}} \alpha_{i(n),m(n)} e_{h,n}$,
(iii) $v_{LA_h}(\phi) = \inf_{n\in\mathbb{N}} v_p(\alpha_{i(n),m(n)})$.

Démonstration. Cela résulte de l'identité $\phi(x) = \sum_{i=1}^{p^h} \mathbf{1}_{-i+p^h\mathbb{Z}_p}(x)\phi_i(\frac{x+i}{p^h})$ et de la remarque 3.1.3 car $\{-i|\, 1 \leq i \leq p^h\}$ est un système de représentants de $\mathbb{Z}_p$ modulo $p^h\mathbb{Z}_p$ □

Venons-en au résultant fondamental de cette partie, dû à Amice, concernant les fonctions localement analytiques.

Théorème 3.1.2. *Les* $\lfloor \frac{n}{p^h} \rfloor ! \binom{x}{n}$ *pour* $n \in \mathbb{N}$ *forment une base orthonormale de* $LA_h(\mathbb{Z}_p, L)$.

La démonstration étant assez technique, on renvoit le lecteur intéressé aux cours de M2 de Pierre Colmez [1].

Corollaire 3.1.2. *Si* $\phi \in \mathscr{C}^0(\mathbb{Z}_p, L)$*, les conditions suivantes sont équivalentes :*
(i) $\phi \in LA(\mathbb{Z}_p, L)$
(ii) $\liminf \frac{1}{n} v_p(a_n(\phi)) > 0$

Démonstration. $(i) \Rightarrow (ii)$ Supposons $\phi \in LA(\mathbb{Z}_p, L)$, il existe alors $h \in \mathbb{N}$ tel que $\phi \in LA_h(\mathbb{Z}_p, L)$. Alors, d'après le théorème précédent ainsi que le corollaire 2.3.1 on en déduit que $\liminf \frac{1}{n} v_p(a_n(\phi)) \geq \frac{1}{(p-1)p^h}$
$(ii) \Rightarrow (i)$ Si $\liminf \frac{1}{n} v_p(a_n(\phi)) > 0$, il existe $h \in \mathbb{N}$ tel que $\liminf \frac{1}{n} v_p(a_n(\phi)) > \frac{1}{(p-1)p^h}$. Alors, $(\lfloor \frac{n}{p^h} \rfloor !)^{-1} a_n(\phi)$ tend vers 0 et donc $\phi \in LA_h(\mathbb{Z}_p, L)$. □

3.1.4 Fonctions de classe $\mathscr{C}^r$

Nous allons définir de manière similaire aux fonctions d'une variable réelle, la dérivation de fonctions p-adiques.
Une fonction $\phi : \mathbb{Z}_p \to L$ est *dérivable en* $x_0 \in \mathbb{Z}_p$, si la quantité $\frac{\phi(x_0+h)-\phi(x_0)}{h}$ admet une limite quand h tend vers 0. La limite est alors notée $\phi'(x_0)$. Une fonction est *dérivable à l'ordre* 1 si elle est dérivable en tout point de $\mathbb{Z}_p$ (une fonction dérivable est donc en particulier continue). Plus généralement, on définit par récurrence la dérivabilité à l'ordre k de la manière suivante : une fonction ϕ est *dérivable à l'ordre* k si elle est dérivable à l'ordre $k-1$ et si sa dérivée $(k-1)$-ième est dérivable à l'ordre 1.
Si $r \geq 0$, on dit que $\phi : \mathbb{Z}_p \to L$ *est de classe* $\mathscr{C}^r$, s'il existe des fonctions $\phi^{(j)} : \mathbb{Z}_p \to L$, pour $0 \leq j \leq \lfloor r \rfloor$, telles que , si l'on définit $\varepsilon_{\phi,r} : \mathbb{Z}_p \times \mathbb{Z}_p \to L$ et $C_{\phi,r} : \mathbb{N} \to \mathbb{R} \cup \{+\infty\}$, par

$$\varepsilon_{\phi,r}(x,y) = \phi(x+y) - \sum_{j=0}^{\lfloor r \rfloor} \phi^{(j)}(x)\frac{y^j}{j!} \quad et \quad C_{\phi,r} = \inf_{x \in \mathbb{Z}_p, y \in p^h\mathbb{Z}_p} v_p(\varepsilon_{\phi,r}(x,y)) - rh$$

alors $C_{\phi,r}(h)$ tend vers $+\infty$ quand h tend vers $+\infty$.

Remarque 3.1.3. *Si* $r = 0$*, on obtient que la définition de fonction de classe* $\mathscr{C}^0$ *coïncide avec la définition d'uniforme continuité. Or,* $\mathbb{Z}_p$ *étant compact, on en déduit que fonction est de classe* $\mathscr{C}^0$ *ssi elle est continue.*

On note $\mathscr{C}^r(\mathbb{Z}_p, L)$ l'espace des fonctions $\phi : \mathbb{Z}_p \to L$ de classe $\mathscr{C}^r$. On munit $\mathscr{C}^r(\mathbb{Z}_p, L)$ de la valuation $v'_{\mathscr{C}^r}$ définie par

$$v'_{\mathscr{C}^r}(\phi) = \inf\left(\inf_{0\leq j\leq \lfloor r\rfloor, x\in\mathbb{Z}_p} v_p(\frac{\phi^{(j)}(x)}{j!}), \inf_{x,y\in\mathbb{Z}_p} v_p(\varepsilon_{\phi,r}(x,y)) - rv_p(y)\right),$$

ce qui en fait un L-Banach.

Montrons quelques résultats intéressants sur les fonctions de classe $\mathscr{C}^r$.

Lemme 3.1.5. *Soit $C(N) = \sum_{n=1}^{N} v_p(n!)$, et soit a_k, pour $0 \leq k \leq N$, une famille d'éléments de L. Alors, quel que soit $h \in \mathbb{Z}$,*

$$\inf_{0\leq k\leq N}(v_p(a_k) + kh) \geq \inf_{x\in p^h\mathbb{Z}_p} v_p(\sum_{k=0}^{N} a_k\frac{x^k}{k!}) - C(N).$$

Démonstration. Nous allons raisonner par récurrence sur N.
OK si $N = 0$,
On suppose l'inégalité vraie pour $N - 1 \geq 0$. Soit $P, Q \in L[x]$ définis par

$$P(x) = \sum_{k=0}^{N} a_k\frac{x^k}{k!} \quad et \quad Q(x) = \sum_{k=0}^{N-1} a_k\frac{x^k}{k!}$$

$$\begin{aligned}
p^{-Nh}\sum_{j=0}^{N}(-1)^{N-j}\binom{N}{j}P(x+jp^h) &= p^{-Nh}\sum_{j=0}^{N}(-1)^{N-j}\binom{N}{j}\sum_{k=0}^{N} a_k\frac{(x+jp^h)^k}{k!}\\
&= p^{-Nh}\sum_{j=0}^{N}\sum_{k=0}^{N}(-1)^{N-j}\binom{N}{j}a_k\frac{(x+jp^h)^k}{k!}\\
&= p^{-Nh}\sum_{j=0}^{N}\sum_{k=0}^{N}(-1)^{N-j}\binom{N}{j}\frac{a_k}{k!}\sum_{n=0}^{k}\binom{k}{n}x^{n-k}j^n p^{nh}\\
&= p^{-Nh}\sum_{k=0}^{N}\sum_{n=0}^{k}\left(\sum_{j=0}^{N}(-1)^{N-j}\binom{N}{j}j^n\right)\frac{a_k}{k!}\binom{k}{n}x^{n-k}p^{nh}
\end{aligned}$$

Or on a le lemme suivant

Lemme 3.1.6. *Si $N > n$, $\sum_{j=0}^{N}(-1)^{N-j}\binom{N}{j}j^n = 0$*
et $\sum_{j=0}^{N}(-1)^{N-j}\binom{N}{j}j^N = N!$

Démonstration. En effet,

$$\begin{aligned}(e^t-1)^N &= \sum_{j=0}^{N}\binom{N}{j}(-1)^{N-j}e^{tj}\\ &= \sum_{j=0}^{N}\binom{N}{j}(-1)^{N-j}\sum_{n=0}^{+\infty}\frac{(tj)^n}{n!}\\ &= \sum_{n=0}^{+\infty}\left(\sum_{j=0}^{N}\binom{N}{j}(-1)^{N-j}j^n\right)\frac{t^n}{n!}\\ &= 1.t^N + t^{N+1}(...)\end{aligned}$$

□

Retour à la démonstration :
Alors, d'après le lemme, quels que soient $x \in \mathbb{Q}_p$ et $h \in \mathbb{Z}$, on a

$$a_N = p^{-Nh}\sum_{j=0}^{N}(-1)^{N-j}\binom{N}{j}P(x+jp^h)$$

donc $v_p(a_N) + Nh \geq \inf_{x\in p^h\mathbb{Z}_p} v_p(P(x))$ d'où pour $x \in p^h\mathbb{Z}_p$

$$v_p(Q(x)) = v_p(P(x) - a_N\frac{x^N}{N!}) \geq \inf_{x\in p^h\mathbb{Z}_p}(v_p(P(x)), v_p(a_N\frac{x^N}{N!})) \geq \inf_{x\in p^h\mathbb{Z}_p} v_p(P(x)) - v_p(N!)$$

Or, par hypothèse de récurrence, on a

$$\inf_{0\leq k\leq N-1}(v_p(a_k)+kh) \geq \inf_{x\in p^h\mathbb{Z}_p} v_p(Q(x)) - C(N-1) \geq \inf_{x\in p^h\mathbb{Z}_p} v_p(P(x)) - C(N)$$

ce qui permet de conclure. □

Proposition 3.1.7. *Si $r \geq 1$, et si $\phi \in \mathscr{C}^r(\mathbb{Z}_p, L)$, alors ϕ est dérivable en tout point. De plus,*
(i) $\phi' \in \mathscr{C}^{r-1}(\mathbb{Z}_p, L)$, et il existe $C_0(r) \in \mathbb{R}$ tel que $v'_{\mathscr{C}^{r-1}}(\phi') \geq v'_{\mathscr{C}^r}(\phi) - C_0(r)$ quel que soit $\phi \in \mathscr{C}^r(\mathbb{Z}_p, L)$.
(ii) $(\phi')^{(j)} = \phi^{(j+1)}$ si $j \leq r-1$.

Démonstration. Il est clair, par définition, que si ϕ est de classe $\mathscr{C}^r$ alors ϕ est dérivable en tout point de dérivée $\phi'(x) = \phi^{(1)}(x) = \lim_{y\to 0}\frac{\phi(x+y)-\phi(x)}{y}$. Par ailleurs en développant $\varepsilon_{\phi,r}(x, y+z) - \varepsilon_{\phi,r}(x+y, z)$ qui est égal à

$$\left(\phi(x+y+z) - \sum_{j=0}^{\lfloor r\rfloor}\phi^{(j)}(x)\frac{(y+z)^j}{j!}\right) - \left(\phi(x+y+z) - \sum_{j=0}^{\lfloor r\rfloor}\phi^{(j)}(x+y)\frac{z^j}{j!}\right),$$

on obtient, si $v_p(z) \geq h$ et $v_p(y) \geq h$, la minoration

$$v_p\left(\sum_{j=0}^{\lfloor r \rfloor} \frac{z^j}{j!}\left(\phi^{(j)}(x+y) - \sum_{k=0}^{\lfloor r \rfloor - j} \phi^{(j+k)}(x)\frac{y^k}{k!}\right)\right) \geq rh + C_{\phi,r}(h).$$

D'après le lemme précédent, si $v_p(y) \geq h$, cela implique la formule

$$v_p\left(\phi^{(j)}(x+y) - \sum_{k=0}^{\lfloor r \rfloor - j} \phi^{(j+k)}(x)\frac{y^k}{k!}\right) \geq (r-j)h + C_{\phi,r}(h) - C([r]).$$

Par conséquent, si $0 \leq j \leq \lfloor r \rfloor$, alors $\phi^{(j)} \in \mathscr{C}^{r-j}(\mathbb{Z}_p, L)$. Egalement, on obtient les formules $v'_{\mathscr{C}^{r-j}}(\phi^{(j)}) \geq v'_{\mathscr{C}^r}(\phi) - C([r])$, et $(\phi^{(j)})^{(k)} = \phi^{(j+k)}$, si $j + k \leq \lfloor r \rfloor$. Ceci permet de conslure. □

Remarque 3.1.4. *La proposition ci-dessus montre que les propriétés habituelles de dérivation restent toujours vérifiées en p-adique.*

Proposition 3.1.8. *Si $\phi_1 : \mathbb{Z}_p \to \mathbb{Z}_p$ est de classe $\mathscr{C}^r$ et si $\phi_2 : \mathbb{Z}_p \to L$ est de classe $\mathscr{C}^r$, alors $\phi_2 \circ \phi_1 : \mathbb{Z}_p \to L$ est de classe $\mathscr{C}^r$.*

Démonstration. Le développement limité marche de la même manière que dans le cas réel □

On se doute intuitivement qu'une fonction localement analytique est de classe $\mathscr{C}^r$ pour tout $r > 0$.

Proposition 3.1.9. *Si $h \in \mathbb{N}$, et si $r \geq 0$, alors $LA_h(\mathbb{Z}_p, L) \subset \mathscr{C}^r(\mathbb{Z}_p, L)$. De plus, si $\phi \in LA_h(\mathbb{Z}_p, L)$, alors*

$$v'_{\mathscr{C}^r}(\phi) \geq v_{LA_h}(\phi) - rh$$

Démonstration. La démonstration s'effectue en développant en série de Taylor une fonction ϕ localement analytique puis en montrant qu'elle vérifie la définition d'une fonction de classe $\mathscr{C}^r$. □

De la même manière que pour les autres espaces, nous allons expliciter une base de Banach de $\mathscr{C}^r(\mathbb{Z}_p, L)$.

Si $i \in \mathbb{N}$ et $k \in \mathbb{N}$, on note $e_{i,k,r}$ l'élément de $\mathscr{C}^r(\mathbb{Z}_p, L)$ défini par

$$e_{i,k,r}(x) = p^{\lfloor \ell(i) r \rfloor} \mathbf{1}_{i+p^{\ell(i)r}\mathbb{Z}_p}(x)\left(\frac{x-i}{p^{\ell(i)}}\right)^k$$

Théorème 3.1.3. *La famille des $e_{i,k,r}$, pour $i \in \mathbb{N}$, $0 \leq k \leq r$, est une base de Banach de $\mathscr{C}^r(\mathbb{Z}_p, L)$.*

La preuve se fait en introduisant une sous-famille dense de fonctions de $\mathscr{C}^r(\mathbb{Z}_p, L)$ que sont les fonctions localement polynômiales (pour une preuve complète : voir [1]).

Définition 3.1.4. *On appelle base de vaguelettes la base de Banach de $\mathscr{C}^r(\mathbb{Z}_p, L)$ constituée des $e_{i,k,r}$, pour $i \in \mathbb{N}$, $0 \leq k \leq r$. Si $\sum_{i\in\mathbb{N}} \sum_{0\leq k\leq r} b_{i,k} e_{i,k,r}$ est la décomposition de $\phi \in \mathscr{C}^r(\mathbb{Z}_p, L)$, en vaguelettes, les $b_{i,k}$ sont les coefficients d'amplitude de ϕ.*

Proposition 3.1.10. *Si $r \geq 1$, la dérivation $\frac{d}{dx}$ induit une surjection de $\mathscr{C}^r(\mathbb{Z}_p, L)$ sur $\mathscr{C}^{r-1}(\mathbb{Z}_p, L)$; son noyau est l'adhérence de $LC(Z_p, L)$ dans $\mathscr{C}^r(\mathbb{Z}_p, L)$.*

Voir le cours de Colmez [1]

Le théorème suivant, dont une démonstration est également donnée dans le cours de Colmez [1], donne une caractérisation des fonctions de classe $\mathscr{C}^r$ en termes de leur développement de Mahler.

Théorème 3.1.4. *Si $r \geq 0$, si $\phi \in \mathscr{C}^r(\mathbb{Z}_p, L)$, et si $\phi = \sum_{n=0}^{+\infty} \binom{x}{n} a_n(\phi)$ est la décomposition de Mahler de ϕ, alors $v_p(a_n) - r\ell(n)$ tend vers $+\infty$ quand n tend vers $+\infty$. De plus, la valuation $v_{\mathscr{C}^r}$ définie sur $\mathscr{C}^r(\mathbb{Z}_p, L)$ par*

$$\mathscr{C}^r(\mathbb{Z}_p, L)(\phi) = \inf_{n\in\mathbb{N}} (v_p(a_n(\phi)) - r\ell(n))$$

est équivalente à $v'_{\mathscr{C}^r}$

Corollaire 3.1.3. *Les $p^{\lfloor \ell(n)r \rfloor} \binom{x}{n}$, pour $n \in \mathbb{N}$, forment une base de Banach de $\mathscr{C}^r(\mathbb{Z}_p, L)$*

Le corollaire est une conséquence immédiate du théorème.

3.2 Anneaux de fonctions analytiques p-adiques

Un autre point à aborder avant d'attaquer la construction de distributions p-adiques est l'étude des séries formelles à coefficients dans L sous-corps fermé de $\mathbb{C}_p$.

3.2.1 Théorème de préparation de Weierstass

Soit $L\{T\}$ l'anneau des séries convergeant sur la boule $\{x \in \mathbb{C}_p |\ v_p(x) \geq 0\}$; c'est aussi l'ensemble des séries $f = \sum_{k=0}^{+\infty} a_k T^k$ telles que $\lim\limits_{k\to+\infty} v_p(a_k) = +\infty$. On peut obtenir également $L\{T\}$ en complétant $L[T]$ pour la valuation de Gauss que l'on notera $v^{[0]}$ au lieu de v_G.

Le but de cette partie est de créer une sorte d'homologue p-adique au théorème de prologement analytique complexe. On peut remarquer sera que ce dernier théorème ne peut exister tel quel à cause de la non connexité du monde p-adique. Cependant, nous allons adapter un résultat algébrique remarquable à $L\{T\}$, le théorème de préparation de Weierstass. Ce théorème ne nous sera pas directement utile pour la construction des distributions p-adiques, néanmoins, il fait partie des théorèmes de base de l'analyse p-adique et intervient notamment dans l'étude de la structure algébrique de $\mathscr{R}_L^+$ (anneau des fonctions analytiques que l'on verra plus tard), c'est donc la raison pour laquelle j'ai décidé de l'insérer dans ce rapport.

La proposition suivante est un résultat simple mais très puissant qui nous sera bien utile pour la démonstration du théorème de préparation de Weierstass.

Proposition 3.2.1. *(Continuité de la division euclidienne)*
Si $P \in \mathscr{O}_L[T]$ est unitaire, alors tout $f \in L\{T\}$ peut s'écrire de manière unique sous la forme $f = Pq(f)+r(f)$, où $q(f) \in L\{T\}$, $r(f) \in L[T]$ et $deg(r(f)) \leq deg(P)-1$. De plus, $v^{[0]}(q(f)) \geq v^{[0]}(f)$ et $v^{[0]}(r(f)) \geq v^{[0]}(f)$

Démonstration. Unicité : Il suffit de montrer que l'application $(g, R) \to Pg + R$ est injective. Si $Pg = -R$ alors P, étant unitaire et à coefficients entiers, a $degP$ zéros appartenant à la boule $\{x \in \mathbb{C}_p |\ v_p(x) \geq 0\}$, alors que R en a au plus $degP - 1$ s'il n'est pas nul, donc $g = R = 0$.
Existence : par un petit procédé algorithmique en utlisant le fait que P est unitaire et à coefficients dans $\mathscr{O}_L$, on trouve que le quotient $q(Q)$ et le reste $r(Q)$ de la division euclidienne d'un polynôme $Q \in \mathscr{O}_L[T]$ par P appartiennent aussi à $\mathscr{O}_L[T]$. De plus, les applications r et q de $L[T]$ dans $L[T]$ vérifient $v^{[0]}(r(Q)) \geq v^{[0]}(Q)$ et $v^{[0]}(q(Q)) \geq v^{[0]}(Q)$, donc elles s'étendent par continuité à $L\{T\}$ en des applications vérifiant les mêmes inégalités. □

Théorème 3.2.1. *(de préparation de Weierstass)*
(i) $g = \sum_{k\in\mathbb{N}} b_k T^k \in L\{T\}$ est inversible dans $L\{T\}$ si et seulement si $b_0 \neq 0$ et $v_p(b_k) > v_p(b_0)$ si $k \geq 1$.
(ii) Si $f = \sum_{k\in\mathbb{N}} a_k T^k \in L\{T\}$ 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 $g = \sum_{k=0}^{+\infty} b_k T^k$

Démonstration. *(i)* ($\Rightarrow$) $g \in L\{T\}$ inversible. On peut supposer $v^{[0]}(g) = 0$ quitte à diviser par un élément de L^*. 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 $\bar{g}\bar{g}^{-1} = \bar{1}$ dans $k_K[T]$. On en déduit que $\bar{g}$ est une constante non nulle,
($\Leftarrow$) Si $b_0 \neq 0$ et $v_p(b_k) > v_p(b_0)$ si $k \geq 1$, 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.
(ii) La suite $v_p(a_k)$ tendant vers $+\infty$, il existe $d \in \mathbb{N}$ tel que l'on ait $v_p(a_d) \leq v_p(a_k)$ (resp. $v_p(a_d) < v_p(a_k)$) si $k \in \mathbb{N}$ (resp. si $k > d$). Soient $\alpha_0 = a_d$ et $P_0 = \sum_{k=0}^{d} \frac{a_k}{a_d} T^k$.
Existence : Nous allons montrer que l'on peut trouver $R \in \mathfrak{m}_L[T]$, de degré $\leq d-1$, 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 $P_0 u + R = \alpha_0^{-1} f - P_0 - Ru$. Pour cela, nous allons considérer l'application $\theta : (u, R) \mapsto \theta(u, R)$ où $\theta(u, R)$ est le couple 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. Considérons l'isomorphisme suivant $\varphi :$

$$\begin{array}{ccc} \mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1} & \longrightarrow & P_0\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1} \\ (u, R) & \longmapsto & P_0 u + R \end{array},$$

les inégalités de continuités obtenues dans cette même proposition précédente nous donne

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

On a de même l'inégalité

$$v^{[0]}(\theta(u,R) - \theta(\tilde{u},\tilde{R})) \geq \inf(v^{[0]}(u-\tilde{u}), v^{[0]}(R-\tilde{R}) + \inf(v^{[0]}(\tilde{u}), v^{[0]}(R))$$

Or $\inf(v^{[0]}(\tilde{u}), v^{[0]}(R)) > 0$ et $\inf(v^{[0]}(u), v^{[0]}(\tilde{R})) > 0$ donc il existe $\varepsilon > 0$ tel que $\forall u, \tilde{u}, R, \tilde{R}$ on ait

$$v^{[0]}(\theta(u,R) - \theta(\tilde{u},\tilde{R})) \geq \inf(v^{[0]}(u-\tilde{u}), v^{[0]}(R-\tilde{R}) + \varepsilon$$

De plus, $\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1}$ est complet. En effet, $\mathfrak{m}_L\{T\}$ est complet en tant que complété de $\mathfrak{m}_L[T]$ pour $v^{[0]}$ puisque $\mathfrak{m}_L$ est complet pour v_p car fermé ($\mathfrak{m}_L = \mathscr{B}_{|.|<1}(0)$ et la norme étant ultramétrique la boule est ouverte et fermée dans un complet). En outre, $\mathfrak{m}_L[T]_{d-1}$ est un $\mathscr{O}_L$-module de type fini car $\mathscr{O}_L[T]_{d-1}$ est un $\mathscr{O}_L$-module de type fini et $\mathfrak{m}_L[T]_{d-1} \subset \mathscr{O}_L[T]_{d-1}$. Egalement, $\mathfrak{m}_L[T]_{d-1}$ est un sous-module de $\mathscr{O}_L[T]_{d-1}$ définit par l'action :

$$\begin{aligned} \mathscr{O}_L \times \mathfrak{m}_L[T]_{d-1} &\longrightarrow \mathfrak{m}_L[T]_{d-1} \\ (\alpha, \textstyle\sum_{i=0}^{d-1} a_i T^i) &\longmapsto \textstyle\sum_{i=0}^{d-1} (\alpha.a_i) T^i \end{aligned}$$

et $v^{[0]}$ correspond à la valuation associée à la norme infinie, et comme $\mathscr{O}_L$ est complet pour v_p, on obtient que $\mathfrak{m}_L[T]_{d-1}$ est complet pour $v^{[0]}$ et donc $\mathfrak{m}_L\{T\} \oplus \mathfrak{m}_L[T]_{d-1}$ est complet pour les mêmes raisons.
Il suffit donc de prendre $P = P_0 + R_0$ et $g = \alpha(1+u_0)$ pour avoir le résultat.
Unicité : Si $Pg = \tilde{P}\tilde{g}$, avec $g, \tilde{g}$ inversibles dans $L\{T\}$, alors $\frac{\tilde{P}}{P}$ n'a aucun zéro ni pôle sur la boule $\{x \in \mathbb{C}_p |\ v_p(x) \geq 0\}$ et comme P et $\tilde{P}$ sont des polynômes unitaires dont tous les zéros appartiennent à cette boule (puisqu'à coefficients entiers), on en conclut que $P = \tilde{P}$ et que $g = \tilde{g}$. □

3.2.2 Fonctions analytiques sur le disque unité

L'objectif de cette partie est de construire un anneau de fonctions analytique sur le disque unité ouvert de $\mathbb{C}_p$ et d'en étudier la structure algébrique. Si $r \in \mathbb{R}$ on définit $\mathscr{E}_L^{[r,+\infty]}$ l'ensemble des fonctions sur $\mathscr{D}(0,r)$ définies sur L. On note $\mathscr{R}_L^+$ ou $\mathscr{E}_L^{]0,+\infty]}$ l'ensemble des fonctions analytiques sur $\mathscr{D}(0,0^+) := \{x \in \mathbb{C}_p |\ v_p(x) > 0\}$ définies sur L. On a donc $\mathscr{R}_L^+ = \cap_{r>0} \mathscr{E}_L^{[r,+\infty]}$. De plus, on note $\mathscr{E}_L^+$ l'ensemble des fonctions analytiques bornées sur $\mathscr{D}(0,0^+)$. Autrement dit, on a

$$\mathscr{E}_L^{[r,+\infty]} = \{\sum_{n=0}^{+\infty} a_n T^n,\ a_n \in L \textit{ et } v_p(a_n) + rn \to +\infty \textit{ quand } n \to +\infty\},$$

$$\mathscr{E}_L = \{\sum_{n=0}^{+\infty} a_n T^n,\ a_n \in L \textit{ et } \exists C \in \mathbb{R} \textit{ tel que } v_p(a_n) \geq C : \textit{quel que soit } n \in \mathbb{N}\},$$

$$\mathscr{R}_L^+ = \{\sum_{n=0}^{+\infty} a_n T^n,\ a_n \in L \textit{ et } \forall r > 0, v_p(a_n) + rn \to +\infty \textit{ quand } n \to +\infty\},$$

En particulier, $L\{T\}$ n'est autre que $\mathscr{E}_L^{[0,+\infty]}$ considéré dans la partie précédente.

De plus, l'anneau $\mathscr{E}_L^{[r,+\infty]}$ est aussi un L-Banach pour la valuation $v^{[r]}$ définie par $v^{[r]}(\sum_{n=0}^{+\infty} a_n T^n) = \inf_{n\in\mathbb{N}} v_p(a_n) + rn$. On munit $\mathscr{R}_L^+$ de la famille de valuation $v^{[r]}, r > 0$,

et $C \in \mathbb{R}$. Une suite f_n tend 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 $r > 0$. Comme $v^{[r]}(f) < v^{[s]}(f)$ si $r < s$, on peut donc se contenter de ne considérer seulement les $v^{[r_h]}$ où r_h est une suite de réels > 0 tendant vers 0, pour définir la topologie de $\mathscr{R}_L^+$.
Or, $\mathscr{R}_L^+$ est l'intersection d'une famille d'espaces de Banach, c'est donc un espace de Fréchet. En particulier, les théorèmes de Baires et de Banach-Steinaus sont encore valables sur $\mathscr{R}_L^+$.

Proposition 3.2.2. *Soit $r \in \mathbb{Q}$,*
(i) Si $f \in \mathscr{E}_L^{[r,+\infty]}$, alors f n'a q'un nombre fini de zéros dans $\mathscr{D}(0,r)$. De plus, si $P = \prod_{x \in \mathscr{D}(0,r)}^{(T-x)^{v_x(f)}}$ 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.

Si $h \in \mathbb{N}$, soit $\zeta_{p^{h+1}}$ une racine $p^{h+1\text{e}}$ de l'unité, et soit $v_h = v_p(\zeta_{p^{h+1}} - 1)$, on a $v_h = \frac{1}{(p-1)p^h}$. En effet, on peut remarquer que le polynôme irréductible de $\zeta_{p^{h+1}}$ est $X^{(p-1)p^h} + X^{(p-2)p^h} + ... + X^{p^h} + 1$, en effectuant le changement de variable $X \to X + 1$, puis en utilisant le critère d'Eisenstein. Finalement, comme les racines d'un polynôme irréductible ont même valuation, on obtient le résultat.

Comme v_h tend vers 0 quand h tend vers $+\infty$, alors la topologie de $\mathscr{R}_L^+$ est aussi définit par la famille de valuations $(v_h)_{h \in \mathbb{N}}$.

Définition 3.2.1. *(Eléments d'ordre r)*
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 minoré à partir d'un certain rang.
On note $\mathscr{R}_{L,r}^+$ le sous-ensemble de $\mathscr{R}_L^+$ des éléments d'ordre r.

On peut munir $\mathscr{R}_{L,r}^+$ de la valuation v_r définie par $v_r(f) = \inf_{n \in \mathbb{N}} v_p(b_n) + r\ell(n)$ ce qui en fait un L-Banach.
L'espace $\mathscr{R}_{L,0}^+$ n'est autre que $\mathscr{E}_L$.

3.2.3 Actions de $\mathbb{Z}_p^*, \varphi$ et ψ

• Actions de $\mathbb{Z}_p^*$ et φ

Si $x \in L^*$, alors $(1+T)^x - 1 = \sum_{n=0}^{+\infty} \binom{x}{n} T^n$ est une uniformisante de $L((T))$. Cela permet de définir un automorphisme continu (pour v_T) $f \mapsto f \star x \in L[[T]]$, en envoyant $\sum_{n=0}^{+\infty} a_n T^n$ sur $\sum_{n=0}^{+\infty} a_n((1+T)^x - 1)^n$. De plus, on a

$$((1+T) \star x) \star y = ((1+T)^x) \star y = ((1+T)^y)^x = (1+T)^{xy} \tag{1}$$

ce qui implique que $(f \star x) \star y = f \star xy$ quel que soit $f \in L[[T]]$. Finalement, cela définit une action de groupe de L^* sur $L[[T]]$.

Lemme 3.2.1. *(i) Si $a \in \mathbb{Z}_p^*$, et si $r \geq 0$, alors $v^{[r]}((1+T)^a - 1) = v^{[r]}(T)$.*
(ii) Si $r \geq 0$, et si $s = \inf(r+1, pr)$, alors $v^{[r]}((1+T)^p - 1) = v^{[s]}(T)$.

Démonstration. Le (i) suit de ce que $\binom{a}{n} \in \mathbb{Z}_p$ si $a \in \mathbb{Z}_p^*$ (par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$), et le (ii) vient sans difficulté en déroulant le calcul. □

On définit l'application φ sur $L[[T]]$ par $\varphi : f \mapsto f \star p$. D'après l'équation (1), on en déduit que les actions φ et $\mathbb{Z}_p^*$ commutent entre elles sur $L[[T]]$.

Proposition 3.2.3. (i) *Si $r \geq 0$ et si $a \in \mathbb{Z}_p^*$, alors $f \mapsto f \star a$ est une isométrie de $\mathscr{E}_L^{[r,+\infty]}$ dans lui-même.*
(ii) *Si $r \geq 0$, 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. (i) Soit $f = \sum_{n=0}^{+\infty} a_n T^n \in \mathscr{E}_L^{[s,+\infty]}$. Si $s' \in \mathbb{R}$, et $x \in L$, on a

$$v^{[s]}(f) = \inf_{n\in\mathbb{N}} v^{[s]}(a_n T^n) = \inf_{n\in\mathbb{N}} v_p(a_n) + n v^{[s]}(T)$$

$$v^{[s']}(f \star x) \geq \inf_{n\in\mathbb{N}} v^{[s']}(a_n((1+T)^x - 1)^n) \geq \inf_{n\in\mathbb{N}} v_p(a_n) + n v^{[s']}((1+T)^x - 1)$$

En appliquant ceci à $s = s' = r$, et $x = a \in \mathbb{Z}_p^*$ et en utilisant le (i) du lemme précédent, on en déduit que $v^{[r]}(f \star a) \geq v^{[r]}(f)$. On obtient l'autre sens de l'inégalité en remplaçant f par $f \star a^{-1}$.
(ii) En réutilisant les équations obtenu précédemment avec $s' = r$ et $s = r'$ ainsi que le (ii) du lemme précédent, on déduit que si $f \in \mathscr{E}_L^{[r,+\infty]}$ alors $\varphi(f) \in \mathscr{E}_L^{[r',+\infty]}$. Or $z \mapsto (1+z)^p - 1$ induit une surjection de $\mathscr{D}(0,r')$ sur $\mathscr{D}(0,r)$, d'après le (i). Par conséquent, cela implique que

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

□

Corollaire 3.2.1. *Les actions de $\mathbb{Z}_p^*$ et φ laissent stables $\mathscr{R}_L^+$ et sont continues sur $\mathscr{R}_L^+$.*

- L'opérateur ψ

Lemme 3.2.2. (i) *Si $0 \leq r \leq \frac{1}{p-1}$, et si $\zeta^p = 1$, alors $v^{[r]}((1+T)\zeta - 1) = v^{[r]}(T)$.*
(ii) *L'application $f \mapsto f \star \zeta$, où $(f \star \zeta)(T) = f((1+T)\zeta - 1)$, est une isométrie de $\mathscr{E}_L^{[r,+\infty]}$ si $0 \leq r \leq \frac{1}{p-1}$, et définit une action de groupe de μ_p sur $\mathscr{E}_L^{[r,+\infty]}$ et $\mathscr{R}_L^+$ si $\mu_p \subset L$.*

Démonstration. Le (i) vient de l'inégalité $v_p(\zeta - 1) \geq \frac{1}{p-1}$. Le (ii) se démontre à partir du (i), de manière similaire à la démonstration de la proposition précédente. □

Lemme 3.2.3. *Soit $n \in \mathbb{N}$.*
(i) *Il existe un unique $Q_n \in \mathbb{Q}_p[T]$ tel que $\mathbb{Q}_n((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p}((1+T)\zeta - 1)^n$.*
(ii) *Si $0 \leq r \leq \frac{r}{p-1}$, alors $v^{[rp]}(Q_n) \geq n v^{[r]}(T) - 1$.*

Démonstration. (i) Soit $R_n(T) = \frac{1}{p}\sum_{\zeta^p}((1+T)\zeta - 1)^n$. En développant $R_n(T)$, comme $\sum_{\zeta^p=1}\zeta^i = 0$ si i n'est pas un multiple de p. Donc

$$R_n(T) = \sum_{\substack{p \mid n-k \\ k\leq n}} \binom{n}{k}(-1)^k(1+T)^{n-k}$$

donc $R_n(T) = Q((1+T)^p)$ où Q est unique par construction. Maintenant, effectuons le changement de base $X^n \to X^n - 1$, pour $n \in \mathbb{N}^*$. Il existe donc un unique polynôme $Q_n \in \mathbb{Q}_p[T]$ tel que

$$\mathbb{Q}_n((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p}((1+T)\zeta - 1)^n.$$

($Q_n \in \mathbb{Q}_p[T]$ car on a besoin d'un corps pour effectuer le changement de base).

(ii) D'après le lemme précédent, on a $v^{[r]}(R_n) \geq nv^{[r]}(T) - 1$. On conclut grâce à l'identité $v^{[rp]}(Q_n) = v^{[r]}(R_n)$. □

Proposition 3.2.4. (i) *Si* $0 \leq r \leq \frac{p}{p-1}$ *et si* $f \in \mathscr{E}_L^{[r/p,+\infty]}$, *il existe* $\psi(f) \in \mathscr{E}_L^{[r,+\infty]}$ *unique tel que* $\psi(f)((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p=1} f((1+T)\zeta - 1)$. *De plus,* $\psi : \mathscr{E}_L^{[r/p,+\infty]} \to \mathscr{E}_L^{[r,+\infty]}$ *est continue et* ψ *laisse stable* $\mathscr{R}_L^+$ *et est continue sur* $\mathscr{R}_L^+$.
(ii) ψ *commute à* $\mathbb{Z}_p^*$ *sur* $\mathscr{R}_L^+$ *et sur* $\mathscr{E}_L^{[r,+\infty]}$, *si* $0 \leq r \leq \frac{1}{p-1}$.
(iii) $\psi \circ \varphi = id$, *et plus généralement,* $\psi(\varphi(f)g) = f\psi(g)$, *si* $f, g \in \mathscr{E}_L^{[r,+\infty]}$, *et* $0 \leq r \leq \frac{1}{p-1}$.

Démonstration. (i) Si $f = \sum_{n=0}^{+\infty} a_n Q_n$. Le précédent lemme montre que $\psi : \mathscr{E}_L^{[r/p,+\infty[} \to \mathscr{E}_L^{[r,+\infty[}$ est continue si $0 \leq r \leq \frac{p}{p-1}$. De plus, si f est un polynôme, on a $\psi(f)((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p} f((1+T)\zeta - 1)$. Or l'application $f \mapsto \frac{1}{p}\sum_{\zeta^p} f((1+T)\zeta - 1)$ est continue d'après le lemme 3.2.3, d'où le résultat. En conclusion, si $0 \leq r \leq \frac{p}{p-1}$, alors $\sup(\frac{p}{p-1} - 1, \frac{p}{p(p-1)}) = \frac{1}{p-1}$ et donc $\psi : \mathscr{E}_L^{[r/p,+\infty[} \to \mathscr{E}_L^{[r,+\infty[}$ et $\varphi : \mathscr{E}_L^{[r,+\infty[} \to \mathscr{E}_L^{[r/p,+\infty[}$.

(ii) Soit $x \in \mathbb{Z}_p^*$, on a

$$\psi((1+T)^n) \star x = Q_n(1+T) \star x = Q_n((1+T)^x)$$

Or

$$\psi((1+T)^n \star x) = \psi((1+T)^{nx}) = \psi(((1+T)^x)^n) = Q_n((1+T)^x)$$

donc par linéarité, puis continuité, on en déduit que ψ commute avec l'action de $\mathbb{Z}_p^*$ sur $\mathscr{R}_L^+$.

(*iii*) On peut remarquer que

$$\begin{aligned}\varphi \circ \psi \circ \varphi(T) &= \frac{1}{p} \sum_{\zeta^p=1} (\varphi(f) \star \zeta)(T) \\ &= \frac{1}{p} \sum_{\zeta^p=1} \varphi(f)((1+T)\zeta - 1) \\ &= \frac{1}{p} \sum_{\zeta^p=1} f((1+T)^p - 1) \\ &= \varphi(f)\end{aligned}$$

Or $\varphi : L[[T]] \to L[[T]]$ est surjective et est une isométrie de $\mathscr{E}_L^{[r,+\infty]}$ dans $\mathscr{E}_L^{[r',+\infty]}$. Par restriction, $\varphi : \mathscr{R}_L^+ \to \mathscr{R}_L^+$ est bien définie et est surjective. Par conséquent,

$$\psi \circ \varphi = id$$

. La généralisation avec $f, g \in \mathscr{E}_L^{[r,+\infty]}$ s'obtient en utilisant la même méthode. □

Remarque 3.2.1. (*i*) *$\mathbb{Z}_p^*$ agit par des isométries sur $\mathscr{R}_{L,r}^+$ muni de v_r'*
(*ii*) *φ et ψ laissent stables $\mathscr{R}_{L,r}^+$ et sont continus sur $\mathscr{R}_{L,r}^+$.*

3.3 Distributions p-adiques

Sachant que $\mathbb{Z}_p$ est compact et qu'une fonction localement analytique est de classe $\mathscr{C}^r$ pour tout $r > 0$, on remarque que les fonctions localement analytique vont avoir le même rôle que les fonctions $\mathscr{C}^\infty$ à support compact dans la théorie classique des Distributions.

Nous allons simplement analyser les espaces duaux des L-Banach p-adiques, qui seront par conséquent toujours des L-Banach p-adiques.

3.3.1 Distribution continues

Définition 3.3.1. *(Distribution continue sur $\mathbb{Z}_p$)*
On appelle distribution continue sur $\mathbb{Z}_p$ une forme linéaire continue sur $LA(\mathbb{Z}_p, L)$.
On note $\mathscr{D}(\mathbb{Z}_p, L)$ l'ensemble des distributions continues sur $\mathbb{Z}_p$. $\mathscr{D}(\mathbb{Z}_p, L)$ correspond donc au dual topologique de $LA(\mathbb{Z}_p, L)$.

Si $\mu \in \mathscr{D}(\mathbb{Z}_p, L)$, μ peut être vu comme une forme linéaire sur $LA(\mathbb{Z}_p, L)$ dont la restriction à chaque $LA_h(\mathbb{Z}_p, L)$ est continue, en remarquant que

$$\mathscr{D}(\mathbb{Z}_p, L) = (LA(\mathbb{Z}_p, L))' = (\bigcup_{h\in\mathbb{N}} LA_h(\mathbb{Z}_p, L))' = \bigcap_{h\in\mathbb{N}} (LA_h(\mathbb{Z}_p, L))'$$

On peut donc définir la valuation v_{LA_h} sur $\mathscr{D}(\mathbb{Z}_p, L)$ par

$$v_{LA_h}(\mu) = \inf_{\phi \in LA_h(\mathbb{Z}_p, L)\setminus\{0\}} v_p(\mu(\phi)) - v_{LA_h}(\phi)$$

et on munit donc $\mathscr{D}(\mathbb{Z}_p, L)$ de la famille de valuations $(v_{LA_h})_{h\in\mathbb{N}}$.

De plus, le dual topologique d'un L-Banach étant un L-Banach (pour la valuation "subordonnée"), on obtient que $\mathscr{D}(\mathbb{Z}_p, L)$ est un espace de Fréchet (comme intersection de L-Banach).

On écrira en général $\mu(\phi)$ sous la forme plus parlante $\int_{\mathbb{Z}_p} \phi(x)\mu(x)$ ou plus simplement $\int_{\mathbb{Z}_p} \phi\mu$.

Nous allons à présent définir une transformée qui agira comme un pont entre les distributions et les anneaux de fonctions analytiques.

Définition 3.3.2. *(Transformée d'Amice)*
Si $\mu \in \mathscr{D}(\mathbb{Z}_p, L)$, on lui associe la série formelle

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

appelée transformée d'Amice de μ.

Lemme 3.3.1. *Si $\mu \in \mathscr{D}(\mathbb{Z}_p, L)$, et si $z \in \mathscr{D}(0, 0^+)$, alors $\mathscr{A}_\mu(z) = \int_{\mathbb{Z}_p} (1+z)^x \mu(x)$*

Démonstration. Il existe $h \in \mathbb{N}$ 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 $LA_h(\mathbb{Z}_p, \mathbb{C}_p)$ car $\frac{z^n}{\lfloor \frac{n}{p^h} \rfloor !}$ tend vers 0. D'où le résultat. □

Théorème 3.3.1. *L'application $\mu \mapsto \mathscr{A}_\mu(T)$ est un isomorphisme d'espace de Fréchet de $\mathscr{D}(\mathbb{Z}_p, L)$ sur $\mathscr{R}_L^+$.*
De plus, si $\mu \in \mathscr{D}(\mathbb{Z}_p, L)$, et si $h \in \mathbb{N}$, on a

$$v^{[v_h]}(\mathscr{A}_\mu) \leq v_{LA_h}(\mu) \leq v^{[v_{h+1}]}(\mathscr{A}_\mu)$$

Démonstration. Soit μ une distribution et soit $\mathscr{A}_\mu(T) = \sum_{n=0}^{+\infty} b_n T^n$ sa transformée d'Amice. En utilisant le théorème d'Amice (donnant la base orthonormale des fonction localement analytique), on montre que quels que soient $h, n \in \mathbb{N}$, on a

$$v_p(b_n) \geq v_{LA_h}(\mu) + v_{LA_h}(\binom{x}{n}) = v_{LA_h}(\mu) - v_p(\lfloor \frac{n}{p^h} \rfloor !) \geq v_{LA_h}(\mu) - n v_h$$

Ceci permet de montrer que $\mathscr{A}_\mu$ converge sur $\mathscr{D}(0, v_h^+)$ (disque ouvert), pour tout $h \in N$, et donc appartient à $\mathscr{R}_L^+$, et l'on a l'inégalité $v^{[v_h]}(\mathscr{A}_\mu) \geq v_{LA_h(\mu)}$.

Réciproquement, si $\mathscr{A}_\mu(T) = \sum_{n=0}^{+\infty} b_n T^n \in \mathscr{R}_L^+$, alors pour tout $h, n \in N$,

$$v_p(\lfloor \frac{n}{p^h} \rfloor ! b_n) \geq v_p(b_n) + \lfloor \frac{n}{p^{h+1}} \rfloor \geq v_p(b_n) + n v_{h+1} - 1 \geq v^{[v_{h+1}]}(\mathscr{A}_\mu) - 1,$$

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

$$v_{LA_h(\mu)} = \inf_{n\in\mathbb{N}} v_p(\lfloor \frac{n}{p^h} \rfloor ! b_n) \geq v^{[v_{h+1}]}(\mathscr{A}_\mu) - 1.$$

□

3.3.2 Distribution tempérées et mesure

Construisons une classe de distribution encore plus générale que les distributions continues.

Définition 3.3.3. *(Distribution d'ordre r)*
Soit $r \geq 0$, une distribution continue sur $\mathbb{Z}_p$ est dite d'ordre r si elle s'étend par continuité à $\mathscr{C}^r$.
On note $\mathscr{D}_r(\mathbb{Z}_p, L)$ l'ensemble des distributions d'ordre r.

On munit l'ensemble des distributions d'ordre r de la valuation

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

Définition 3.3.4. *(Distribution tempérée)*
Une distribution est dite tempérée, s'il existe $r \in \mathbb{R}_+$, telle qu'elle soit d'ordre r.
On note $\mathscr{D}_{temp}$ l'ensemble des distributions tempérées.

Proposition 3.3.1. *L'application $\mu \mapsto \mathscr{A}_\mu$ induit une isométrie de $\mathscr{D}_r(\mathbb{Z}_p, L)$ sur $\mathscr{R}^+_{L,r}$.*

Démonstration. La démonstration est assez évidente en utilsant la définition de $v_{\mathscr{C}^r}$. □

Définition 3.3.5. *(Mesure)*
Une distribution d'ordre 0 est appelée une mesure. L'espace $\mathscr{D}_0(\mathbb{Z}_p, L)$ des mesures est donc le dual topologique des fonctions continues.

En utilisant la décomposition en ondelettes d'une fontion continue, on peut contruire une mesure en ne connaissant que les intégrales $\int_{\mathbb{Z}_p} \mathbf{1}_{a+p^n\mathbb{Z}_p}\mu(x)$ pour $a \in \mathbb{Z}_p$ et $n \in \mathbb{N}$.

Soit $\mu \in \mathscr{D}_0(\mathbb{Z}_p, L)$. Si $a \in \mathbb{Z}_p$ et $n \in \mathbb{N}$, soit $\mu(a+p^n\mathbb{Z}_p) = \int_{\mathbb{Z}_p} \mathbf{1}_{a+p^n\mathbb{Z}_p}\mu(x)$ la mesure de $a+p^n\mathbb{Z}_p$. Comme $a+p^n\mathbb{Z}_p$ est la réunion disjointe des $a+jp^n+p^{n+1}\mathbb{Z}_p$ pour $j \in \{0, ..., p-1\}$, on a $\mu(a + p^n\mathbb{Z}_p) = \sum_{j=0}^{p-1} \mu(a + jp^n + p^{n+1}\mathbb{Z}_p)$.
De plus, comme $v_p(\mathbf{1}_{a+p^n\mathbb{Z}_p}) = 0$, et comme $v_p(\int_{\mathbb{Z}_p} \mathbf{1}_{a+p^n\mathbb{Z}_p}\mu(x)) - v_{\mathscr{C}^0}(\mathbf{1}_{a+p^n\mathbb{Z}_p}) \geq v'_{\mathscr{D}_0}(\mu)$ par définition de $v'_{\mathscr{D}_0}$, on obtient que $v_p(\mu(a + p^n\mathbb{Z}_p)) \geq v'_{\mathscr{D}_0}(\mu), \forall a \in \mathbb{Z}_p, \forall n \in \mathbb{N}$. Donc les $\mu(a + p^n\mathbb{Z}_p)$ sont bornés.
Si $\phi \in \mathscr{C}^0(\mathbb{Z}_p, L)$, alors

$$\sum_{a=0}^{p^n-1} \phi(a)\mathbf{1}_{a+p^n\mathbb{Z}_p} \underset{n\to+\infty}{\longrightarrow} \phi$$

dans $\mathscr{C}^0(\mathbb{Z}_p, L)$. Donc

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

ce qui ressemble étroitement à une somme de Riemann.

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

(i) $\mu(a+p^n\mathbb{Z}_p)=\mu(b+p^n\mathbb{Z}_p)$ si $v_p(b-a)\geq n$
(ii) $\mu(a+p^n\mathbb{Z}_p)=\sum_{j=0}^{p-1}\mu(a+jp^n+p^{n+1}\mathbb{Z}_p)$,
(iii) Il existe $c\in\mathbb{R}$ tel que $v_p(\mu(a+p^n\mathbb{Z}_p))\geq C$ quels que soient $a\in\mathbb{Z}_p$ et $n\in\mathbb{N}$,
alors (i) et (ii) permettent d'étendre μ en une forme linéaire sur $LC(\mathbb{Z}_p,L)$, et (iii) permet de montrer que $v_p(\mu(\phi))\geq v_{\mathscr{C}^0}(\phi)+C$, ce qui permet d'étendre μ par continuité à $\mathscr{C}^0(\mathbb{Z}_p,L)$.

Proposition 3.3.2. *Si on définit $v_{\mathscr{D}_r}(\mu)$, pour $\mu\in\mathscr{D}_r(\mathbb{Z}_p,L)$, par la formule*

$$v_{\mathscr{D}_r}(\mu)=\inf_{n\in\mathbb{N}}v_{LA_n}(\mu)+rn=\inf_{a\in\mathbb{Z}_p,k\in\mathbb{N},n\in\mathbb{N}}\left(\left(\int_{a+p^n\mathbb{Z}_p}\left(\frac{x-a}{p^n}\right)^k\mu\right)+rn\right),$$

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

Une démonstration se fait en introduisant le dual topologique des fonctions localement polynômiales ainsi que la base des $e_{i,k,r}$.
Pour une preuve détaillée, voir le cours de M2 de Pierre Colmez [1].

3.3.3 Opérations sur les distributions

(i) Masse de Dirac :

Si $a\in\mathbb{Z}_p$, soit $\delta_a$la masse de Dirac en a, c'est-à-dire la mesure qui à ϕ associe $\phi(a)$. Sa transformée d'Amice est $(1+T)^a$.

Comme les polynômes sont denses dans $\mathscr{R}_L^+$, et $\mathscr{R}_{L,r}^+$, quel que soit $r\geq 0$, l'espace vectoriel engendré par les masses de Dirac est dense dans $\mathscr{D}(\mathbb{Z}_p,L)$ et $\mathscr{D}_r(\mathbb{Z}_p,L)$, sii $r\geq 0$.

(ii) Multiplication par une fonction :

Si μ est une distribution continue sur $\mathbb{Z}_p$ et f une fonction localement analytique sur $\mathbb{Z}_p$, on définit la distribution $f\mu$ par la formule $\int_{\mathbb{Z}_p}\phi(f\mu)=\int_{\mathbb{Z}_p}(f\phi)\mu$.
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

$$x\binom{x}{n}=((x-n)+n)\binom{x}{n}=(n+1)\binom{x}{n+1}+n\binom{x}{n}$$

Donc

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

Donc

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

On peut aussi obtenir une formule simpathique en introduisant la *transformée de Laplace* $\mathscr{L}_\mu$ de μ, qui est la série entière définie par

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

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

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

• Multiplication par z^x si $v_p(z-1) > 0$:

Si $v_p(y-1) > 0$, et si $\lambda \in \mathscr{D}(\mathbb{Z}_p, L)$, alors $\int_{\mathbb{Z}_p} y^x \lambda(x) = \mathscr{A}_\lambda(y-1)$ d'après le lemme 3.3.1. En appliquant ceci à $\lambda = z^x\mu$, on obtient $\mathscr{A}_\lambda(y-1) = \mathscr{A}_\mu(yz-1)$, quel que soit $y \in \mathscr{D}(0, 0^+)$. Par conséquent, comme $\mathscr{D}(0,0^+)$ est infini, 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'une masse de Dirac en 0 près. La transformée d'Amice de $x^{-1}\mu$ est donc une primitive de $(1+T)^{-1}\mathscr{A}_\mu(T)$, où la constannte d'intégration correspond à l'indétermination mentionnée ci-dessus.

(*iii*) Restriction à un ouvert compact :

On va multiplier notre distribution pas la fonction caractéristique d'un ouvert compact. Si $n \in \mathbb{N}$ et $b \in \mathbb{Z}_p$, alors la fonction caractéristique de $b + p^n\mathbb{Z}_p$ est $x \mapsto p^{-n}\sum_{\zeta^{p^n}=1} \zeta^{-b}\zeta^x$. Cela se traduit, pour les transformées d'Amice, par la formule

$$\mathscr{A}_{Res_{a+p^n\mathbb{Z}_p}(\mu)}(T) = p^{-n}\sum_{\zeta^{p^n}=1} \zeta^{-b}\mathscr{A}_\mu((1+T)\zeta - 1)$$

Si $k \geq 1$, d'après les remarques faites sur la transformée de Laplace, on a la formule

$$\mathscr{L}_{x^{-k}\mu}(t) = \partial^{-k}\mathscr{L}_\mu(t) + P(t)$$

où $P \in L[t]$ tel que $degP \leq k-1$. Par conséquent, on obtient

$$\mathscr{A}_{x^{-k}\mu}(T) = \partial^{-k}\mathscr{A}_\mu(T) + P(\log(1+T))$$

par changement de variable.

Proposition 3.3.3. *Soient $n \in \mathbb{N}$, $b \in \mathbb{Z}_p$ et $k \in \mathbb{Z}$. On a alors*

$$\int_{b+p^n\mathbb{Z}_p} x^k\mu = p^{-n}\sum_{\zeta^{p^n}=1} \zeta^{-b}\partial^{-k}\mathscr{A}_\mu(\zeta - 1)$$

si $k \geq 0$ ou si $k \leq -1$ et $b \notin p^n\mathbb{Z}_p$.

Démonstration. C'est une conséquence directe de ce que l'on a énoncé précédemment. Si $k \leq -1$, l'indépendance du terme de droite par rapport aux constantes d'intégration suit de ce que $\log(\zeta) = 0$ si $\zeta^{p^n} = 1$ et de ce que $\sum_{\zeta^{p^n}=1} \zeta^{-b} = 0$ si $b \notin p^n\mathbb{Z}_p$. □

(*iv*) Dérivée d'une distribution :

Si $\mu \in \mathscr{D}(\mathbb{Z}_p, L)$, on définit sa dérivée $d\mu$ par la formule

$$\int_{\mathbb{Z}_p} \phi(x) d\mu(x) = \int_{\mathbb{Z}_p} \phi'(x)\mu(x)$$

et donc $\mathscr{A}_{d\mu}(T) = \log(1+T)\mathscr{A}_\mu(T)$. On peut remarquer, qu'il n'est en général pas possible en p-adique de déterminer la primitive d'une distribution car $\log(1+T)$ possède une infinité de zéros dans le disque unité $\mathscr{D}(0, 0^+)$.

(*v*) Actions de $\mathbb{Z}_p^*, \varphi$ et ψ :

• On fait agir $a \in \mathbb{Z}_p^*$ sur une distribution μ :

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

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

• On fait agir φ sur une distribution μ par :

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

• On fait agir ψ sur une distribution μ par :

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

et donc

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

On obtient donc les relations suivantes :

(*a*) $\psi \circ \varphi = id$

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

De plus, $\psi(\mu) = 0$ si et seulement si μ est à support dans $\mathbb{Z}_p^*$, et

$$Res_{\mathbb{Z}_p^*}(\mu) = (1 - \varphi \circ \psi)\mu$$

(*vi*) Convolutions des distributions :

Si λ et μ sont deux distributions, on définit leur convolée $\lambda * \mu$ par

$$\int_{\mathbb{Z}_p} \phi\lambda * \mu = \int_{\mathbb{Z}_p} \left(\int_{\mathbb{Z}_p} \phi(x+y)\mu(x) \right) \lambda(y).$$

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 $z \in \mathscr{D}(0, 0^+)$, et donc que

$$\mathscr{A}_{\lambda*\mu} = \mathscr{A}_\lambda \mathscr{A}_\mu$$

Pour donner un sens à l'intégrale double, il faut montrer que $y \mapsto \int_{\mathbb{Z}_p} \phi(x+y)\lambda(x)$ est localement analytique, ce qui ce fait grâce à un développement de Taylor. Pour plus de détails, voir le cours de Colmez [1].

Proposition 3.3.4. (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 $r+s$.*

On renvoit également à Colmez [1] pour une démonstration, centrée sur les transformées d'Amice.

Remarque 3.3.1. *La formule $\mathscr{A}_{\lambda*\mu} = \mathscr{A}_\lambda \mathscr{A}_\mu$ montre que si $\delta_a * \mu = \mu$ quel que soit $a \in \mathbb{Z}_p$, alors $\mu = 0$. Il n'a donc pas de distribution continue sur $\mathbb{Z}_p$ invariante par translation. Autrement dit, il n'existe pas de mesure de Haar p-adique.*

4 Seconde construction des L fonctions p-adiques

4.1 Rappels sur les L fonctions complexes

Pour cette partie, nous aurons besoin de quelques prérequis sur la fonction zeta que l'on trouve notamment dans le chapitre 2 du livre de Koblitz[3].

Si $\Re(s) > 1$, on a notamment la formule

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{1}{e^t - 1} t^s \frac{dt}{t}$$

où Γ est la fonction Gamma d'Euler méromorphe sur $\mathbb{C}$.

Proposition 4.1.1. *Si $f \in \mathscr{C}^\infty(\mathbb{R}_+)$, à décroissance rapide à l'infini, alors la fonction*

$$L(f, s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} f(t) t^s \frac{dt}{t}$$

définie pour $\Re(s) > 0$ admet un prolonngement holomorphe à $\mathbb{C}$ tout entier, e si $n \in \mathbb{N}$, alors $L(f, -n) = (-1)^n f^{(n)}(0)$.

Démonstration. soit $\varphi \in_C lasse^\infty(\mathbb{R}_+)$, valant 1 sur $[0, 1]$ et 0 sur $[2, +\infty[$. On a $f = \varphi f + (1 - \varphi)f$, donc

$$L(f, s) = L(\varphi f, s) + L((1 - \varphi)f, s)$$

par linéarité de l'intégrale. Donc, par théorème de convergence dominé (version holomorphe), on en déduit que $s \mapsto \Gamma(s)L((1 - \varphi)f, s)$ est holomorphe sur $\mathbb{C}$.
Quitte à remplacer f par φf, on peut supposer f à support compact, car $L((1-\varphi)f, -n) = 0$ quel que soit $n \in \mathbb{N}$, puisque $\frac{1}{\Gamma(-n)} = 0$ quel que soit $n \in \mathbb{N}$.
Par ailleurs, par intégration par parties, on obtient

$$L(f, -n) = (-1)^{n+1} L(f^{(n+1)}, 1) \quad et \quad L(f, s) = -L(f', s + 1) \quad si\, \Re(s) > 1$$

donc cela permet de prolonger $L(f, s)$ en une fonction holomorphe sur $\mathbb{C}$.
D'autre part,

$$L(f, -n) = (-1)^{n+1} \int_0^{+\infty} f^{(n+1)}(t)dt = (-1)^n f^{(n)}(0)$$

□

Théorème 4.1.1. *(i) La fonction ζ a un prolongement méromorphe à $\mathbb{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$ de résidu 1.*
(ii) Si $n \in \mathbb{Q}$, alors $\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$

Démonstration. On a $\zeta(s) = \frac{1}{s-1} L(f_0, s - 1)$, avec $f_0(t) = \frac{t}{e^t - 1}$ (qui est bien $\mathscr{C}^\infty$ à décroissance rapide en l'infini), comme on le remarque en utilisant la formule classique $\Gamma(s) = (s - 1)\Gamma(s - 1)$. □

Remarque 4.1.1. *On peut constater que ce résultat concorde bien avec le résultat trouvé au théorème 2.2. En effet, en posant $\chi = 1$ puis en utilisant le fait que $B_n = B_n(0) = (-1)^n B_n(1) = (-1)^n B_{n,1}$, on obtient bien le même résultat.*

4.2 Fonction Zêta de Kubota-Leopoldt

4.2.1 Congruences de Kummer

Si $a \in \mathbb{R}_+^*$, on peut appliquer la proposition 4.1 à la fonction $f_a(t) = \frac{1}{e^t-1} - \frac{a}{e^{at}-1}$ qui est $\mathscr{C}^\infty$ sur $\mathbb{R}_+$ et à décroissance rapide à l'infini.

Corollaire 4.2.1. *Si $a \in \mathbb{R}_+^*$, la fonction $(1-a^{1-s})\zeta(s) = L(f_a, s)$ prolonge analytiquement à $\mathbb{C}$ tout entier et, si $n \in \mathbb{N}$, alors $(1-a^{1+n})\zeta(-n) = (-1)^n f_a^{(n)}(0)$. En particulier, si $a \in \mathbb{Q}$, alors $(1-a^{1+n})\zeta(-n) \in \mathbb{Q}$.*

Proposition 4.2.1. *Si $a \in \mathbb{Z}_p^*$, il existe une mesure μ_a dont la transformée de Laplace est $f_a(t)$. De plus, $v_{\mathscr{D}_0}(\mu_a) \geq 0$ et si $n \in \mathbb{N}$, alors $\int_{\mathbb{Z}_p} x^n \mu_a = (-1)^n(1-a^{1+n})\zeta(-n)$.*

Démonstration. Pour démontrer l'existence d'une telle mesure μ_a, il suffit de montrer que la série obtenue en remplaçant e^t par $1+T$ est à coefficients bornés, i.e est dans $\mathscr{E}_L = \mathscr{R}_{L,0}^+$; ce sera la trannsformée d'amice de μ_a. Or, on peut écrire $(1+T)^a - 1$ sous la forme $aT(1+Tg(T))$ avec $g(T) = \sum_{n=2}^{+\infty} \frac{1}{a}\binom{a}{n} T^{n-2} \in \mathbb{Z}_p[[T]]$ et donc

$$\frac{1}{T} - \frac{a}{(1+T)^a - 1} = \sum_{n=1}^{+\infty} (-T)^{n-1} g^n \in \mathbb{Z}_p[[T]].$$

Comme on a obtenu une série à coefficients entiers, on a par conséquent $v_{\mathscr{D}_0}(\mu_a) \geq 0$. Finalement, on a $\int_{\mathbb{Z}_p} x^n \mu_a = \mathscr{L}_{\mu_a}^{(n)}(0) = f_a^{(n)}(0)$. □

Proposition 4.2.2. *(Congruences de Kummer)*
Soit $a \in \mathbb{N} \setminus \{1\}$, soit $k \geq 1$. Si n_1 et n_2 sont deux entiers $\geq k$ vérifiant $n_1 \equiv n_2 \, mod \, (p-1)p^{k-1}$, alors

$$v_p((1-a^{1+n_1})\zeta(-n_1) - (1-a^{1+n_2})\zeta(-n_2)) \geq k$$

Démonstration. Comme on a supposé $n_1 \geq k$ et $n_2 \geq k$, on a $v_p(x^{n_1}) \geq k$ et $v_p(x^{n_2}) \geq k$ si $x \in p\mathbb{Z}_p$. D'autre part, comme $Card((\mathbb{Z}/p^k\mathbb{Z})^*) = (p-1)p^{k-1}$, et que l'on a supposé $n_1 \equiv n_2 \, mod \, (p-1)p^{k-1}$, on a $x^{n_1} - x^{n_2} \in p^k\mathbb{Z}_p$ si $x \in \mathbb{Z}_p^*$. En résumé, $v_p(x^{n_1} - x^{n_2}) \geq k$ quel que soit $x \in \mathbb{Z}_p$, et donc $v_{\mathscr{C}^0}(x^{n_1} - x^{n_2}) \geq k$. Comme $v_{\mathscr{D}_0}(\mu_a) \geq 0$, cela implique

$$v_p((1-a^{1+n_1})\zeta(-n_1) - (1-a^{1+n_2})\zeta(-n_2)) = v_p(\int_{\mathbb{Z}_p} (x^{n_1} - x^{n_2})\mu_a(x)) \geq k$$

□

4.2.2 Restriction à $\mathbb{Z}_p^*$

L'énoncé ci-dessus peut être rendu plus esthétique en se restreignant à $\mathbb{Z}_p^*$. Cependant, il n'y a à priori aucun lien entre $\int_{\mathbb{Z}_p^*} x^n \mu$ et $\int_{\mathbb{Z}_p} x^n \mu$. Par contre, la proposition suivante qu'il existe un tel lien dans le cas de la mesure μ_a.

Proposition 4.2.3. *Si $a \in \mathbb{Z}_p^*$, alors*
(i) $\psi(\mu_a) = \mu_a$
(ii) $Res_{\mathbb{Z}_p^*}(\mu_a) = (1-\varphi)\mu_a$
(iii) $\int_{\mathbb{Z}_p^*} x^n \mu_a = (1-p^n)\int_{\mathbb{Z}_p} x^n \mu_a$

Démonstration. Soit $F(T) = \psi(\frac{1}{T})$. Par définition, on a

$$F((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p=1} \frac{1}{(1+T)\zeta - 1} = \frac{-1}{p}\sum_{\zeta^p=1}\sum_{n=0}^{+\infty}((1+T)\zeta)^n$$
$$= -\sum_{n=0}^{+\infty}(1+T)^{pn} = \frac{1}{(1+T)^p - 1}$$

Donc $\psi(\frac{1}{T}) = \frac{1}{T}$. D'autre part, la transformée d'Amice de μ_a est $\frac{1}{T} - a\frac{1}{T} \star a$, et comme ψ commute avec l'action de $a \in \mathbb{Z}_p^*$, et $\psi(\mathscr{A}_\mu) = \mathscr{A}_{\psi(\mu)}$, on en déduit le (i).

Le (ii) suit du (i) et de la formule $Res_{\mathbb{Z}_p^*}(\mu) = (1-\varphi\psi)\mu$.

Le (iii) suit du (ii) et de ce que $\int_{\mathbb{Z}_p} x^n \varphi(\mu) = \int_{\mathbb{Z}_p}(px)^n \mu$. □

Corollaire 4.2.2. *Soit $a \in \mathbb{N} \setminus \{1\}$ premier à p. Soit $k \geq 1$. Si n_1 et n_2 sont deux entiers vérifiant $n_1 \equiv n_2 \, mod\, (p-1)p^{k-1}$, alors*

$$v_p((1-a^{1+n_1})(1-p^{n_1})\zeta(-n_1) - (1-a^{1+n_2})(1-p^{n_2})\zeta(-n_2)) = v_p(\int_{\mathbb{Z}_p^*}(x^{n_1} - x^{n_2})\mu_a(x)) \geq k$$

Ce corollaire traduit une propriété de continuité p-adique de la fonction $n \mapsto (1-p^n)\zeta(-n)$, ce que l'on va préciser par la suite.

4.2.3 Transformée de Mellin p-adique et transformée Γ de Leopoldt

On note Δ le groupe des racines de l'unité contenues dans $\mathbb{Q}_p^*$. Donc Δ est le groupe (cyclique) des racines $\phi(q)$-ième de l'unité, et $\mathbb{Z}_p^*$ est la réunion disjointe des $\varepsilon + q\mathbb{Z}_p$, pour $\varepsilon \in \Delta$. De plus, on peut prolonger à $\mathbb{Z}_p$ la fonction de Teichmüller $\omega : \mathbb{Z}_p \to \Delta \cup \{0\}$ en posant $\omega(x) = 0$ si $x \in p\mathbb{Z}_p$.

Proposition 4.2.4. *Si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, la fonction $x \mapsto \omega(x)^i\langle x\rangle^s$ est une fonction localement analytique sur $\mathbb{Z}_p$. De plus,*

$$\omega(x)^i\langle x\rangle^s = x^n \ \ si\ n \equiv i \ \ mod\, \phi(q) \ \ et \ \ si\ x \in \mathbb{Z}_p^*, \quad \omega(x)^i\langle x\rangle^s = \lim_{\substack{n\to+\infty \\ n\equiv i \ mod\, \phi(q)}} x^n, \ \ \forall x, s \in \mathbb{Z}_p.$$

Démonstration. L'analycité locale vient de ce que l'on a $\omega(x)^i\langle x\rangle^s = 0$ sur $p\mathbb{Z}_p$ et

$$\omega(x)^i\langle x\rangle^s = \varepsilon^i(\frac{x}{\varepsilon})^s = \sum_{n=0}^{+\infty}\binom{s}{n}\varepsilon^{i-n}(x-\varepsilon)^n$$

si $x \in \varepsilon + q\mathbb{Z}_p$ et $\varepsilon \in \Delta$. Le reste vient de ce que Δ est d'ordre $\phi(q)$. □

Définition 4.2.1. *(Transformée de Mellin)*
Si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, on définit la i-ème branche $Mel_{i,\mu}$, transformée de Mellin d'une distribution continue μ par la formule

$$Mel_{i,\mu} = \int_{\mathbb{Z}_p} \omega(x)^i \langle x \rangle^s \mu(x) = \int_{\mathbb{Z}_p^*} \omega(x)^i \langle x \rangle^s \mu(x)$$

la seconde égalité résultant du fait que $\omega(x) = 0$ si $x \in p\mathbb{Z}_p$. D'autre part, on a $Mel_{i,\mu}(n) = \int_{\mathbb{Z}_p^*} x^n \mu$ si $n \equiv i \mod \phi(q)$.

Remarque 4.2.1. *On peut définir de manière plus générale la transformée de Mellin d'une distribution sur $\mathbb{Z}_p^*$ comme la fonction qui à un caractère localement analytique $\beta : \mathbb{Z}_p^* \to \mathbb{C}_p^*$ associe l'intégrale*

$$Mel_\mu(\beta) = \int_{\mathbb{Z}_p^*} \beta(x)\mu(x)$$

On a donc la formule $Mel_\mu(\omega(x)^i \langle x \rangle^s) = Mel_{i,\mu}$.

L'existence des $\phi(q)$ branches de la transformée de Mellin correspond au fait que l'espace des caractères continus de $\mathbb{Z}_p^*$ dans $\mathbb{C}_p^*$ est la réunion des $\phi(q)$ boules ouvertes, une pour chaque caractère de Δ.

soit u un générateur topologique du groupe multiplicatif $1+q\mathbb{Z}_p$, et soit $\theta : 1+q\mathbb{Z}_p \to \mathbb{Z}_p$ le morphisme de groupes qui à x associe $\frac{\log x}{\log u}$. Ce morphisme est analytique, inversible et son inverse aussi , ce qui fait que si f est une fonction localement analytique sur $\mathbb{Z}_p$ (resp. continue), alors $\theta^* f$ définie par $\theta^* f(x) = f(\theta(x))$ est localement analytique sur $1 + q\mathbb{Z}_p$ (resp. continue).
Si μ est une distribution à support dans $1 + q\mathbb{Z}_p$, on définit la distribution $\theta_*\mu$ sur $\mathbb{Z}_p$ par la formule

$$\int_{\mathbb{Z}_p} \phi\theta_*\mu = \int_{1+q\mathbb{Z}_p} \theta_*\phi\mu$$

et par les remarques précédentes faites sur θ_*, on en déduit que l'image d'une mesure par θ_* est encore une mesure.

Lemme 4.2.1. *Si X est un ouvert compact de $\mathbb{Z}_p$, si $\alpha \in \mathbb{Z}_p^*$, et si μ est une distribution continue sur $\mathbb{Z}_p$, alors*

$$Res_X(\mu \star \alpha) = Res_{\alpha^{-1}X}(\mu) \star \alpha.$$

Démonstration. Il suffit de remarquer que $\mathbf{1}_X(\alpha x) = \mathbf{1}_{\alpha^{-1}X}(x)$ et de dérouler les calculs. □

Définition 4.2.2. *(Transformée Γ de Leopoldt)*
Si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$ et si μ est une distribution sur $\mathbb{Z}_p^*$, on définit la i-ème branche Γ_μ^i de la transformée Γ de μ par la formule

$$\Gamma_\mu^i = \theta_* Res_{1+q\mathbb{Z}_p}\left(\sum_{\varepsilon\in\Delta} \varepsilon^{-i}\mu \star \varepsilon\right) = \theta_*\left(\sum_{\varepsilon\in\Delta} \varepsilon^{-i} Res_{\varepsilon^{-1}+q\mathbb{Z}_p}(\mu) \star \varepsilon\right)$$

La deuxième égalité résulte du lemme précédent. De plus, si μ est une mesure, alors $\mu\star\varepsilon$ est une mesure et $v_{\mathscr{D}_0}(\mu\star\varepsilon) = v_{\mathscr{D}_0}(\mu)$. Par conséquent, comme l'image d'une mesure par θ_* est encore une mesure, on obtient que Γ^i_μ est encore une mesure et que $v_{\mathscr{D}_0}(\Gamma^i_\mu) \geq v_{\mathscr{D}_0}(\mu)$.

Proposition 4.2.5. *Si μ est une distribution continue et $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, alors*

$$Mel_{i,\mu}(s) = \int_{\mathbb{Z}_p^*} \omega(x)^i \langle x\rangle^s \mu(x) = \int_{\mathbb{Z}_p} u^{sy} \Gamma^i_\mu(y) = \mathscr{A}_{\Gamma^i_\mu}(u^s - 1)$$

Démonstration. La seule égalité qui n'est pas la conséquence immédiate d'une définition est la seconde. Si $y = \theta(x) = \frac{\log x}{\log u}$, et on a $u^{sy} = \exp(s\log x) = \langle x\rangle^s$ et donc

$$\begin{aligned}
\int_{\mathbb{Z}_p} u^{sy}\Gamma^i_\mu(y) &= \int_{1+q\mathbb{Z}_p} \langle x\rangle^s \sum_{\varepsilon\in\Delta} \varepsilon^{-i}\mu\star\varepsilon \\
&= \sum_{\varepsilon\in\Delta} \int_{1+q\mathbb{Z}_p} \langle x\rangle^s \varepsilon^{-i}\mu\star\varepsilon \\
&= \sum_{\varepsilon\in\Delta} \int_{\varepsilon^{-1}+q\mathbb{Z}_p} \langle \varepsilon x\rangle^s \varepsilon^{-i}\mu \\
&= \sum_{\varepsilon\in\Delta} \int_{\varepsilon^{-1}+q\mathbb{Z}_p} \omega(x)^i\langle x\rangle^s \mu(x)
\end{aligned}$$

car $\langle \varepsilon x\rangle = \langle x\rangle$, $\omega(x) = \varepsilon^{-1}$ si $x \in \varepsilon^{-1} + q\mathbb{Z}_p$ et finalement $\mathbb{Z}_p^* = \bigsqcup_{\varepsilon\in\Delta}(\varepsilon + q\mathbb{Z}_p)$. □

Corollaire 4.2.3. *Si μ est une distribution continue et si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, la fonction $Mel_{i,\mu}(s)$ est une fonction analytique de s et même de $u^s - 1$.*

4.2.4 Construction de la fonction Zêta de kubota-Leopoldt

Si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, et si $a \in \mathbb{Z}_p^*$ vérifie $\langle a\rangle \neq 1$, définissons $g_{a,i}$ par la formule

$$g_{a,i}(s) = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}} Mel_{-i,\mu_a}(-s) = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}} \int_{\mathbb{Z}_p^*} \omega(x)^{-i}\langle x\rangle^{-s}\mu_a(x)$$

Nous allons à présent démontrer le théorème suivant dû à Kubota et Leopoldt

Théorème 4.2.1. *Si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, il existe une unique fonction $\zeta_{p,i}$, continue sur $\mathbb{Z}_p$ (resp. $\mathbb{Z}_p \setminus \{1\}$) si $i \neq 1$ (resp. si $i = 1$) telle que la fonction $(s-1)\zeta_{p,i}(s)$ soit analytique sur $\mathbb{Z}_p$ ($i+p\mathbb{Z}_p$ si $p = 2$), et que l'on ait $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$ si $n \in \mathbb{N}$ vérifie $-n \equiv i \mod \phi(q)$.*

Démonstration. Unicité : Elle est évidente par densité de $i + \phi(q)\mathbb{N}$ dans $\mathbb{Z}_p$.
Existence : Montrons que $g_{a,i}$ vérifie bien les conditions demandées et ne dépend pas de a. D'après le corollaire 4.2.3, $Mel_{i,\mu}(s)$ est une fonction analytique de s. D'autre part, étudions l'analycité de $s \mapsto \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}}$.

• *1^er cas* : Si $\omega(a)^{1-i} \neq 1$, $s \mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ est analytique ne s'annulant pas sur $\mathbb{Z}_p$ car $\langle a\rangle^{1-s} \in 1+q\mathbb{Z}_p$ puisque

$$\langle a\rangle^{1-s} = (1+\langle a\rangle - 1)^{1-s} = \sum_{n=0}^{+\infty} \binom{1-s}{n} (\langle a\rangle - 1)^n \in 1+q\mathbb{Z}_p.$$

• *2^e cas* : Si $\omega(a)^{1-i} = 1$ on a

$$\langle a\rangle^{1-s} = (1+\langle a\rangle - 1)^{1-s} = \sum_{n=0}^{+\infty} \binom{1-s}{n} (\langle a\rangle - 1)^n \equiv 1+(1-s)(\langle a\rangle - 1) \ mod\, p^{k+1}\mathbb{Z}_p$$

où $k = v_p(\langle a\rangle - 1)$ donc

$$\frac{\langle a\rangle^{1-s}-1}{p^k} \equiv (1-s)u \ mod\, p\mathbb{Z}_p$$

où $u = \frac{\langle a\rangle - 1}{p^k}$ et par conséquent $v_p(u) = 0$. Donc $1-s = u^{-1}\frac{\langle a\rangle^{1-s}-1}{p^k}$ dans $\mathbb{F}_p$, et donc, si $\langle a\rangle^{1-s} = 1$ pour $s \in \mathbb{Z}_p$, alors $s \in 1+p\mathbb{Z}_p$. Par récurrence, supposons $s \in 1+p^n\mathbb{Z}_p$, où $n \in \mathbb{N}^*$. Alors, on a

$$\langle a\rangle^{1-s} \equiv 1+(1-s)(\langle a\rangle - 1) \ mod\, p^{n+k+1}\mathbb{Z}_p$$

car

$$\forall m > 1, \quad v_p\left(\binom{1-s}{m}(\langle a\rangle - 1)^m\right) > k+n+1 \qquad (1)$$

donc $s \in 1+p^{n+1}\mathbb{Z}_p$, donc $\forall n \in \mathbb{N}^*, s \in 1+p^n\mathbb{Z}_p$ donc $s = 1$.
preuve de (1) :

$$\begin{aligned} v_p\left(\binom{1-s}{m}(\langle a\rangle - 1)^m\right) &= mk + v_p\left(\binom{1-s}{m}\right) \\ &= mk + v_p(1-s) + v_p(\frac{1}{m}) + v_p(\binom{-s}{m}) \\ &\geq mk + n - v_p(m) + 0 = k+n+[(m-1)k - v_p(m)] = k+n+C_{k,m} \end{aligned}$$

or $v_p(m) < \frac{\log m}{\log p} + 1$, donc $C_{k,m} \geq (m-1)k - 1 - \frac{\log m}{\log p} = f_k(m)$ où $f_k : x \mapsto (x-1)k - 1 - \frac{\log m}{\log p}$. De plus, f_k est de classe $\mathscr{C}^1$ sur $\mathbb{R}_+^*$ (au sens usuel défini sur $\mathbb{R}$), et $f_k'(x) = k - \frac{1}{x\log p} \geq k - \frac{1}{x\log 2} > k-1 > 0$, $\forall x \geq 2, \forall k \geq 1$.
Donc f_k est strictement croissante quel que soit $k > 1$. Comme $C_{k,m} \geq f_k(m) > f_k(1) = 0, \forall m \geq 2$ et comme $C_{k,m}$ est entier, alors $C_{k,m} > 1$, donc

$$\forall m > 1, \quad v_p\left(\binom{1-s}{m}(\langle a\rangle - 1)^m\right) > k+n+1$$

fin de la preuve de (1).

Donc $\langle a\rangle^{1-s}-1$ ne s'annule que pour $s=1$. On en déduit que $g_{a,i}$ est continue sur $\mathbb{Z}_p\backslash\{1\}$ et même sur $\mathbb{Z}_p$ si $\omega(a)^{1-i}\neq 1$. De plus, si $-n\equiv i mod\phi(q)$, on a $\omega(a)^{1-i}=\omega(a)^{1+n}$ et $\omega(x)^{-i}=\omega(x)^n$, si $x\in\mathbb{Z}_p^*$.
Donc

$$\begin{aligned} g_{a,i}(-n) &= \frac{1}{1-\omega(a)^{1+n}\langle a\rangle^{1+n}}\int_{\mathbb{Z}_p^*}\omega(x)^n\langle x\rangle^n\mu_a(x) \\ &= \frac{1}{1-a^{n+1}}\int_{\mathbb{Z}_p^*}x^n\mu_a(x)=(-1)^n(1-p^n)\zeta(-n)\end{aligned}$$

Donc $g_{a,i}(-n)$ ne dépend pas du choix de a. Si $a,a'\in\mathbb{Z}_p^*$, alors $g_{a,i}-g_{a',i}$ est un quotient de fonctions analytiques s'annulant en un nombre infini de points, ce qui implique qu'elle est identiquement nulle et que la fonction $g_{a,i}$ est bien indépendante du choix de a. En conclusion, il suffit donc de poser $\zeta_{p,i}=g_{a,i}$ pour $\langle a\rangle\neq 1$ et $\omega(a)^{1-i}\neq 1$ (si $i\neq 1$). □

4.2.5 résidu en $s=1$ de la fonction zeta p-adique

On a $\frac{\log(1+T)}{T}\in\mathscr{R}_L^+$, donc il existe une distribution μ_{KL} telle que $\mathscr{A}_{\mu_{KL}}(T)=\frac{\log(1+T)}{T}$, on a également $\mathscr{L}_{\mu_{KL}}(t)=\mathscr{A}_{\mu_{KL}}(e^t-1)=\frac{t}{e^t-1}=f_0(t)$ et

$$\int_{\mathbb{Z}_p}x^n\mu_{KL}=f_0^{(n)}(0)=(-1)^{n-1}n\zeta(1-n)$$

Comme le montre le lemme suivant, on peut remarquer que cette mesure n'est pas invariante par translation.

Lemme 4.2.2. $\int_{a+p^n\mathbb{Z}_p}\mu_{KL}(x)=\frac{1}{p^n}$

Démonstration. On a $\int_{a+p^n\mathbb{Z}_p}\mu_{KL}(x)=\frac{1}{p^n}\sum_{\varepsilon^{p^n}=1}\varepsilon^{-a}\mathscr{A}_{\mu_{KL}}(\varepsilon-1)$ et comme $\log(\varepsilon)=0$ si ε est une racine de l'unité d'ordre une puissance de p. Donc il reste seulement le terme correspondant à $\varepsilon=1$, ce qui donne le résultat. □

Proposition 4.2.6. *On a :*
(i) $\psi(\mu_{KL})=p^{-1}\mu_{KL}$
(ii) $Res_{\mathbb{Z}_p^*}(\mu_{KL})=(1-p^{-1}\varphi)\mu_{KL}$
(iii) $\int_{\mathbb{Z}_p^*}x^n\mu_{KL}=(-1)^{n-1}n(1-p^{n-1})\zeta(1-n),\quad si\ n\in\mathbb{N}.$

Démonstration. *(i)* On a la formule $\psi(\frac{1}{T})=\frac{1}{T}$ démontrée dans la démontration de la proposition 4.2.2. De plus, $\varphi(\log(1+T))=\log((1+T)^p)=p\log(1+T)$, or $\psi(\varphi(a)b)=a\psi(b)$. Donc

$$\frac{\log(1+T)}{T}=\log(1+T)\psi(\frac{1}{T})=\psi(p\frac{\log(1+T)}{T})$$

Donc

$$\mathscr{A}_{\psi(\mu_{KL})}(T)=\psi(\mathscr{A}_{\mu_{KL}}(T))=p^{-1}\mathscr{A}_{\mu_{KL}}(T)=\mathscr{A}_{p^{-1}\mu_{KL}}(T)$$

donc

$$\psi(\mu_{KL})=p^{-1}\mu_{KL}$$

Les preuves de *(ii)* et *(iii)* sont similaires à celles effectuées dans la proposition 4.2.2. □

Théorème 4.2.2. *La branche $\zeta_{p,1}$ de la fonction zêta p-adique a un pôle simple en $s = 1$ de résidu $1 - \frac{1}{p}$.*

Démonstration. Avec ce qui précède, on peut écrire $\zeta_{p,i}$, si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$ sous la forme

$$\zeta_{p,i}(s) = \frac{(-1)^{i-1}}{s-1} Mel_{1-i,\mu_{KL}}(1-s) = \frac{(-1)^{i-1}}{s-1} \int_{\mathbb{Z}_p^*} \omega(x)^{1-i} \langle x \rangle^{1-s} \mu_{KL}(x)$$

En effet, les termes de doite et de gauche de la formule ci-dessus sont analytiques sur $\mathbb{Z}_p \backslash \{1\}$, et prennent la même valeur aux entiers négatifs $-n \in \mathbb{N}$, vérifiant $-n \equiv i mod \phi(q)$. Donc, ils sont égaux en tout point. De plus,

$$\begin{aligned} \lim_{s \to 1} (s-1)\zeta_{p,i}(s) &= \int_{\mathbb{Z}_p^*} \omega(x)^{i-1} \mu_{KL}(x) \\ &= \sum_{\varepsilon \in \Delta} \omega(\varepsilon)^{1-i} \int_{\varepsilon + p\mathbb{Z}_p} \mu_{KL}(x) = 1 - \frac{1}{p} \ si \ i = 1, \ et \ 0 \ \ sinon \end{aligned}$$

□

Remarque 4.2.2. *On peut rapprocher la formule $\lim_{s \to 1}(s-1)\zeta_{p,1}(s) = 1 - \frac{1}{p}$ de la formule analogue pour la fonction zêta de Riemann. La différence encore une fois est donnée par un facteur d'Euler.*

4.3 Les L fonctions p-adiques

Pour cette deuxième construction des L fonctions p-adiques, nous nous appuierons sur les remarques faites à propos des sommes de Gauss au début de la section 2.

4.3.1 Rappels sur les L fonctions complexes

Soit χ un caractère de Dirichlet de conducteur f. Nous rappelons que la L série attachée à χ est définit par

$$L(\chi, s) = \sum_{n=0}^{+\infty} \frac{\chi(n)}{n^s}, \ \ \Re(s) > 1$$

où $s \in \mathbb{C}$. Si on utilise $\chi(n) = \frac{1}{G(\chi^{-1})} \sum_{b \ mod \ D} \chi^{-1}(b) \varepsilon_D^{nb}$ où $\varepsilon_D^{nb} = e^{\frac{2i\pi nb}{D}}$, alors

$$L(\chi, s) = \frac{1}{G(\chi^{-1})} \sum_{b \ mod \ D} \chi^{-1}(b) \sum_{n=1}^{+\infty} \frac{\varepsilon_D^{nb}}{n^s}$$

Or en utilisant

$$\int_0^{+\infty} e^{-nt} t^s \frac{dt}{t} = \frac{\Gamma(s)}{n^s}$$

on obtient, toujours pour $\Re(s) > 1$,

$$\begin{aligned} L(\chi, s) &= \frac{1}{G(\chi^{-1})} \frac{1}{\Gamma(s)} \sum_{b \bmod D} \chi^{-1}(b) \sum_{n=1}^{+\infty} \int_0^{+\infty} (\varepsilon_D^b e^{-t})^n t^s \frac{dt}{t} \\ &= \frac{1}{G(\chi^{-1})} \frac{1}{\Gamma(s)} \sum_{b \bmod D} \chi^{-1}(b) \int_0^{+\infty} \frac{1}{\varepsilon_D^b e^{-t} - 1} t^s \frac{dt}{t} \\ &= \frac{1}{G(\chi^{-1})} \frac{1}{\Gamma(s)} \int_0^{+\infty} \sum_{b \bmod D} \frac{\chi^{-1}(b)}{\varepsilon_D^b e^{-t} - 1} t^s \frac{dt}{t} \end{aligned}$$

Les intervertions somme-intégrale peuvent se justifier grâce au théorème de Fubini, nous ne les détaillerons pas.

La dernière égalité nous donne par conséquent, d'après la proposition 4.1 que $L(\chi, s)$ s'étend en une fonction holomorphe sur $\mathbb{C}$ tout entier et que, si $n \in \mathbb{N}$, alors $L(\chi, -n) = (-1)^n f_\chi^{(n)}(0)$ où f_χ définie par $f_\chi(t) = \sum_{b \bmod D} \frac{\chi^{-1}(b)}{\varepsilon_D^b e^{-t} - 1}$ est bien de classe $\mathscr{C}^\infty$. Pour supprimer le $(-1)^n$ de l'équation, on peut considérer $\mathscr{L}_\chi$ telle que $\mathscr{L}_\chi(t) = f_\chi(-t)$, on a par conséquent $L(\chi, -n) = \mathscr{L}_\chi^{(n)}(0)$. De plus, en utilisant l'égalité

$$\frac{1}{\varepsilon_D^{-b} e^{-t} - 1} = -1 - \frac{1}{\varepsilon_D^b e^t - 1}$$

ainsi que $\sum_{b \bmod D} \chi^{-1}(b) = 0$, on obtient $L(\chi, -n) = (\frac{d}{dt})^n \mathscr{L}_\chi(t)_{|t=0}$, avec

$$L(\chi, s) = \frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \frac{\chi^{-1}(b)}{\varepsilon_D^b e^t - 1}$$

4.3.2 Fonctions L p-adiques

Soit χ un caractère de Dirichlet de conducteur $D > 1$ premier à p. Si $\chi^{-1}(b) \neq 0$, alors ε_D^b est une racine de l'unité d'ordre premier à p et distincte de 1, ce qui implique $v_p(\varepsilon_D^b - 1) = 0$. On en déduit le fait que la série entière

$$F_\chi(T) = \frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \frac{\chi^{-1}(b)}{(1+T)\varepsilon_D^b - 1} = \frac{1}{G(\chi^{-1})} \sum_{b \bmod D} \chi^{-1}(b) \sum_{n=0}^{+\infty} \frac{\varepsilon_D^{nb}}{(\varepsilon_D^b - 1)^{n+1}} T^n$$

est à coefficients bornés (et même à coefficients entiers car $G(\chi)$ et $G(\chi^{-1})$ sont entiers algébriques et $v_p(G(\chi)G(\chi^{-1})) = v_p(D) = 0$, ce qui implique $v_p(G(\chi)) = v_p(G(\chi^{-1})) = 0$) et donc la transformée d'Amice d'une mesure μ_χ sur $\mathbb{Z}_p$ dont la transformée de Laplace est $F_\chi(e^t - 1)\mathscr{L}_\chi(t)$. On a donc $\int_{\mathbb{Z}_p} x^n \mu_\chi = \mathscr{L}_\chi^{(n)}(0) = L(\chi, -n)$, d'après les remarques sur les L fonctions complexes, et $v_{\mathscr{D}_0}(\mu_\chi) \geq 0$.

Définition 4.3.1. *On définit la L fonction p-adique associée à χ comme étant la transformée de Mellin de μ_χ et on note $\beta \mapsto L_p(\chi \otimes \beta)$ cette fonction. Si β est un caractère*

localement analytique sur $\mathbb{Z}_p^*$, on a donc

$$L_p(\chi \otimes \beta) = \int_{\mathbb{Z}_p^*} \beta(x)\mu_\chi(x).$$

D'autre part, si $i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, on pose

$$L_{p,i}(\chi, s) = L_p(\chi \otimes (\omega^{-i}(x)\langle x\rangle^{-s})) = \int_{\mathbb{Z}_p^*} \omega^{-i}(x)\langle x\rangle^{-s}\mu_\chi(x)$$

Proposition 4.3.1. *$i \in \mathbb{Z}/\phi(q)\mathbb{Z}$, la fonction $L_{p,i}(\chi, s)$ est analytique sur $\mathbb{Z}_p$ et on a $L_{p,i}(\chi, -n) = (1 - \chi(p)p^n)L(\chi, -n)$ si $n \in \mathbb{N}$ vérifie $-n \equiv i \ mod\, \phi(q)$.*

Démonstration. L'analycité de $L_{p,i}(\chi, s)$ découle des remarques faites sur la transformée de Mellin. De plus, d'après la démonstration de la proposition 4.2.2, on a la formule

$$\sum_{\zeta^p=1} \frac{1}{(1+T)\varepsilon_D^b\zeta - 1} = p\frac{1}{(1+T)^p\varepsilon_D^{pb} - 1}$$

On en déduit que la transformée d'Amice de la restriction à $\mathbb{Z}_p^*$ de μ_χ est

$$\frac{-1}{G(\chi^{-1})} \sum_{b \, mod\, D} \left(\frac{\chi^{-1}(b)}{(1+T)\varepsilon_D^b - 1} - \frac{\chi^{-1}(b)}{(1+T)^p\varepsilon_D^{pb} - 1} \right)$$

en mettant $\chi^{-1}(b)$ sous la forme $\chi(p)\chi^{-1}(pb)$ en utilisant que $b \mapsto pb$ est une bijection modulo D, on peut réécrire la formule ci-dessus sous la forme $\mathscr{A}_{\mu_\chi}(T) - \chi(p)\mathscr{A}_{\mu_\chi}((1 + T)^p - 1)$. D'où on en déduit

$$\mathscr{L}_{Res_{\mathbb{Z}_p^*}(\mu_\chi)}(t) = \mathscr{L}_{\mu_\chi}(t) - \chi(p)\mathscr{L}_{\mu_\chi}(pt) \qquad et \qquad \int_{\mathbb{Z}_p^*} x^n\mu_\chi = (1 - \chi(p)p^n)L(\chi, -n)$$

pour $n \in \mathbb{N}$. □

4.3.3 Comportement en $s = 1$ des L fonction p-adiques

D'après les remarques précédentes faites sur les L fonctions complexes, on a la formule

$$L(\chi, 1) = \frac{1}{G(\chi^{-1})} \sum_{b \, mod\, D} \chi^{-1}(b) \sum_{n=1}^{+\infty} \frac{\varepsilon_D^{nb}}{n}$$

et donc

$$L(\chi, 1) = \frac{-1}{G(\chi^{-1})} \sum_{b \, mod\, D} \chi^{-1}(b) \log(1 - \varepsilon_D^b)$$

Nous allons établir l'analogue p-adique de cette formule. Cela revient précisément à calculer l'intégrale $\int_{\mathbb{Z}_p^*} x^{-1}\mu_\chi$. Nous allons pour ce faire calculer la transformée d'Amice de $x^{-1}\mu_\chi$ puis tuer l'indétermination en se restreignant à $\mathbb{Z}_p^*$.

Proposition 4.3.2. *La transformée d'Amice de $x^{-1}\mu_\chi$ est (à constante près) :*

$$\mathscr{A}_{x^{-1}\mu_\chi}(T) = \frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \chi^{-1}(b) \log((1+T)\varepsilon_D^b - 1)$$

Démonstration. On a la formule

$$(1+T)\frac{d}{dT}\mathscr{A}_{x^{-1}\mu_\chi}(T) = \mathscr{A}_{\mu_\chi}(T)$$

Ensuite, on applique l'oppérateur $(1+T)\frac{d}{dT}$ au membre de droite, puis en utilisant que $\sum_{b \bmod D} \chi^{-1}(b) = 0$, ainsi que $v_p(\varepsilon_D^b - 1) = 0$ puisque $pgcd(D,p) = 1$, on obtient que la série

$$\log((1+T)\varepsilon_D^b - 1) = \log(\varepsilon_D^b - 1) + \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} \left(\frac{\varepsilon_D^b T}{\varepsilon_D^b - 1}\right)^n$$

converge sur $\mathscr{D}(0, 0^+)$ □

Lemme 4.3.1. *La transformée d'Amice de la restriction à $\mathbb{Z}_p^*$ de $x^{-1}\mu_\chi$ est donnnée par la formule*

$$\begin{aligned}\mathscr{A}_{Res_{\mathbb{Z}_p^*}(x^{-1}\mu_\chi)}(T) &= \frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \chi^{-1}(b) \left(\log((1+T)\varepsilon_D^b - 1) - \frac{1}{p}\log((1+T)^p \varepsilon_D^{pb} - 1)\right) \\ &= \mathscr{A}_{x^{-1}\mu_\chi}(T) - \frac{\chi(p)}{p}\mathscr{A}_{x^{-1}\mu_\chi}((1+T)^p - 1)\end{aligned}$$

Démonstration. La preuve repose sur les résultats généraux de la restriction d'une mesure, ainsi que sur l'identité

$$\sum_{\zeta^p=1} \log((1+T)\zeta\varepsilon_D^b - 1) = \log((1+T)^p \varepsilon_D^{pb} - 1)$$

La deuxième égalité se démontre en écrivant $\chi^{-1}(b)$ sous la forme $\chi(p)\chi^{-1}(pb)$ en utilisant que $b \mapsto pb$ est une bijection modulo D comme $pgcd(D,p) = 1$. □

En évaluant en $T = 0$ dans la formule précédente, on obtient

$$L_{p,1}(\chi, 1) = L_p(\chi \otimes x^{-1}) = \int_{\mathbb{Z}_p^*} x^{-1}\mu_\chi = \frac{-1}{G(\chi^{-1})}(1 - \frac{\chi(p)}{p}) \sum_{b \bmod D} \chi^{-1}(b) \log(\varepsilon_D^b - 1)$$

où la formule ne diffère que d'un facteur d'Euler et où le logarithme p-adique a substitué le logarithme usuel.

4.3.4 Torsion par un caractère de conducteur une puissance de p

Dans cette partie, nous allons généraliser les résultats précédents en évaluant la L fonction p-adique de χ en un caractère de la forme $\beta(x)x^n$ où β est caractère de Dirichlet de conducteur une puissance de p. Nous utiliserons la notation $\chi \otimes \beta$ pour désigner le caractère de Dirichlet modulo Dp^k défini par $(\chi \otimes \beta)(a) = \chi(a)\beta(a)$, où χ et β sont vu comme des caractères *mod* Dp^k grâce aux projections respectives de $(\mathbb{Z}/Dp^k\mathbb{Z})^*$ sur $(\mathbb{Z}/D\mathbb{Z})^*$ et $(\mathbb{Z}/p^k\mathbb{Z})^*$

Lemme 4.3.2. *Soit $k \geq 1$, β un caractère de Dirichlet de conducteur p^k et μ une distribution continue sur $\mathbb{Z}_p$. Alors, on a*

$$\int_{\mathbb{Z}_p} \beta(x)(1+T)^x \mu(x) = \frac{1}{G(\beta^{-1})} \sum_{c \mod p^k} \beta^{-1}(c) \mathscr{A}_\mu((1+T)\varepsilon_{p^k}^c - 1)$$

Démonstration. On a

$$\begin{aligned}
\int_{\mathbb{Z}_p} \beta(x)(1+T)^x \mu(x) &= \sum_{a \mod p^k} \beta(a) \int_{a+p^k\mathbb{Z}_p} (1+T)^x \mu \\
&= \sum_{a \mod p^k} \beta(a) \left(\frac{1}{p^k} \sum_{\zeta^{p^k}=1} \zeta^{-a} \mathscr{A}_\mu((1+T)\zeta - 1) \right) \\
&= \sum_{\zeta^{p^k}=1} \mathscr{A}_\mu((1+T)\zeta - 1) \left(\frac{1}{p^k} \sum_{a \mod p^k} \beta(a)\zeta^{-a} \right)
\end{aligned}$$

Si on écrit ζ sous la forme $\varepsilon_{p^k}^c$, on reconnait dans le terme entre parenthèse une somme de Gauss tordue. Par conséquent, il vaut

$$\frac{1}{p^k}\beta^{-1}(-c)G(\beta) = \frac{\beta^{-1}(c)}{G(\beta^{-1})}$$

d'où le résultat. □

Proposition 4.3.3. *Si μ est une mesure sur $\mathbb{Z}_p$ dont la transformée d'Amice est de la forme*

$$\mathscr{A}_\mu(T) = \frac{-1}{G(\chi^{-1})} \sum_{b \mod D} \chi^{-1}(b) F((1+T)\varepsilon_D^b - 1)$$

et si β est un caractère de Dirichlet de conducteur p^k avec $k \geq 1$, alors

$$\int_{\mathbb{Z}_p} \beta(x)(1+T)^x \mu(x) = \frac{-1}{G((\chi \otimes \beta)^{-1})} \sum_{a \mod Dp^k} (\chi \otimes \beta)^{-1}(a) F((1+T)\varepsilon_{Dp^k}^b - 1)$$

Démonstration. D'après le lemme précédent, on a

$$\int_{\mathbb{Z}_p} \beta(x)(1+T)^x \mu(x) = \frac{-1}{G(\chi^{-1})G(\beta)^{-1}} \sum_{b \ mod\, D} \sum_{c \ mod\, p^k} \chi^{-1}(b)\beta^{-1}(c) F((1+T)\varepsilon_D^b \varepsilon_{p^k}^c - 1)$$

Or tout élément de $\mathbb{Z}/Dp^k\mathbb{Z}$ peut s'écrire de manière unique sous la forme $Dc + p^k b$ (théorème chinois), avec $b \in \mathbb{Z}/D\mathbb{Z}$ et $c \in \mathbb{Z}/p^k\mathbb{Z}$. Cela implique les formules suivantes

$$\varepsilon_{Dp^k}^a = \varepsilon_D^b \varepsilon_{p^k}^c$$

$$(\chi \otimes \beta)^{-1}(a) = \chi^{-1}(p^k)\beta^{-1}(D)\chi^{-1}(b)\beta^{-1}(c)$$

$$\begin{aligned} G((\chi \otimes \beta)^{-1})) &= \sum_{a \ mod\, Dp^k} (\chi \otimes \beta)^{-1}(a)\varepsilon_{Dp^k}^a \\ &= \chi^{-1}(p^k)\beta^{-1}(D) \left(\sum_{b \ mod\, D} \chi^{-1}(b)\varepsilon_D^b \right) \left(\sum_{c \ mod\, p^k} \beta^{-1}(c)\varepsilon_{p^k}^c \right) \\ &= \chi^{-1}(p^k)\beta^{-1}(D) G(\chi^{-1}) G(\beta^{-1}) \end{aligned}$$

Ce qui permet de conclure. □

On peut appliquer la proposition précédente à la distribution $x^{-1}\mu_\chi$ avec $F = \log$, ce qui donne, en évaluant en $T = 0$

$$L_p(\chi \otimes (x^{-1}\beta)) = \int_{\mathbb{Z}_p^*} \beta(x) x^{-1} \mu_\chi = \frac{-1}{G((\chi \otimes \beta)^{-1})} \sum_{a \ mod\, Dp^k} (\chi \otimes \beta)^{-1}(a) \log(\varepsilon_{Dp^k}^b - 1)$$

Remarquons que cette formule reste similaire à son analogue complexe.

Proposition 4.3.4. *Si β est un caractère de Dirichlet non trivial de conducteur une puissance de p, et si $n \in \mathbb{N}$, alors*

$$L_p(\chi \otimes (x^n \beta)) = L(\chi \otimes \beta, -n).$$

Démonstration. En appliquant la proposition à la formule donnant la transformée d'Amice μ_χ, on obtient que la transformée d'Amice de $\beta(x)\mu(x)$ est

$$\frac{-1}{G((\chi \otimes \beta)^{-1})} \sum_{b \, mod\, Dp^k} \frac{(\chi \otimes \beta)^{-1}(b)}{(1+T)\varepsilon_{Dp^k}^b - 1}$$

et donc que sa transformée de Laplace est $\mathscr{L}_{\chi \otimes \beta}(t)$, ce qui conclut. □

Conclusion

Comme nous avons pu le constater, les L fonctions p-adiques sont très surprenantes. Bien qu'elles soient construites par interpolation sur les entiers négatifs, leur résidu continue de coïncider avec celui des L fonctions complexe en 1. Mais on comprend véritablement l'importance de ces fonctions grâce au théorème de Mazur-Wiles, qui donne une caractérisation algébrique des zéros de la fonction zêta, et nous montre que les L fonctions p-adiques font parties des fondations de l'arithmétique moderne.

Remerciements

Je souhaite remercier Denis Benoit pour avoir encadré mon stage, mais également pour m'avoir initié au métier de chercheur, que ce soit au travers des conférences auxquelles il a eu la gentillesse de m'inviter ou bien au travers de nos échanges sur la philosophie des nombres et L fonctions p-adiques qui m'ont guidé tout au long de mon stage et ont su m'éclaircir ce domaine si abstrait et magnifique des mathématiques.

Références

[1] Pierre Colmez. Cours de m2. https ://webusers.imj-prg.fr/ pierre.colmez/M2.html, 2005-2009.

[2] Helmut Hasse. *Number theory*. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[3] Neal Kolitz. *p-adic Numbers, p-adic Analysis and Zeta-Functions*. Springer Verlag, New York, Berlin, Heidelberg, Tokyo, second edition.

[4] Alain M. Robert. *A Course in p-adic Analysis*. Graduate Texts in Mathematics. Springer, New York, Berlin, Heidelberg, Tokyo, second edition.

[5] Lawrence C. Washington. *Introduction to cyclotomic fields*. Graduate Texts in Mathematics. Springer Verlag, New York, USA, 1997.