La fonction L p-adique de Kubota-Leopold

Colas BARDAVID et Pierre FIMA

exposé proposé par Gaëtan CHENEVIER

Nous tenons à remercier Gaëtan Chenevier pour son aide, ses explications, ses exposés et sa patience.

Table des matières

Introduction

Le but de cet exposé est d'expliquer la construction de la fonction L de Kubota-Leopold, généralisation p-adique de la fonction ζ de Riemann, et d'en exposer quelques propriétés. On fera donc en introduction de l'analyse complexe, afin d'exposer les résultats nécessaires pour établir l'analogie. On construira ensuite $\mathbb{C}_p$ qui est le cadre privilégié de l'analyse p-adique. Avant de trouver l'analogue de ζ, on chercher ceux de l'exponentiel et du logarithme réel. Munis de ces outils, on pourra alors construire et étudier la fonction L de Kubota-Leopold.

La partie 4 et surtout la partie 5, faute de référence, sont originales.

1 La fonction ζ complexe et les nombres de Bernoulli

1.1 Définitions

Définition 1 *Soit $s \in \mathbb{C}$ tel que $\Re es > 1$. La fonction ζ est donnée par :*

$$\zeta(s) : = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Considérons la fonction complexe $\frac{z}{e^z-1}$, elle est holomorphe au voisinage de zéro. On peut donc la développer en série entière et on pose :

Définition 2 *Soit B_n le n-ieme nombre de Bernoulli défini par :*

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

Plus généralement, on peut même poser :

Proposition-Définition 3 *On note B_k et on appelle n-ième polynôme de Bernoulli le polynôme défini par*

$$\frac{te^{xt}}{e^t-1} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}. \tag{1}$$

On a l'expression suivante :

$$B_k(x) = \sum_{i=0}^{k} \mathrm{C}_k^i B_i x^{k-i}.$$

Démonstration. C'est un polynôme d'après l'écriture, qui découle du produit de Cauchy,

$$\frac{te^{xt}}{e^t-1} = \left(\sum_{k=0}^{\infty} B_k \frac{t^k}{k!}\right)\left(\sum_{k=0}^{\infty} \frac{(xt)^k}{k!}\right) = \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} \frac{B_i}{i!}\frac{x^{k-i}}{(k-i)!}\right)t^k.$$

On a donc $B_k(x) = \sum_{i=0}^{k} B_i \frac{k!}{i!(k-i)!}x^{k-i}$, ce qu'on voulait. ■

On a $B_0(x) = 1$, $B_1(x) = x - 1/2$.

Proposition 4 *(1)* $\forall\, n > 1,\ B_n(x+1) - B_n(x) = nx^{n-1}$.

(2) $B_n^{'}(x) = nB_{n-1}(x)$.

Démonstration.

(1)
$$\sum_{n=0}^{\infty} \frac{B_n(x+1) - B_n(x)}{n!} z^n = \frac{ze^{(x+1)z}}{e^z - 1} - \frac{ze^{xz}}{e^z - 1} = ze^{xz} = \sum_{n=1}^{\infty} nx^{n-1} \frac{z^n}{n!}$$

D'où le résultat par identification.

(2)
$$\sum_{n=0}^{\infty} B_n^{'}(x) \frac{z^n}{n!} = \frac{d}{dx}\left(\frac{ze^{zx}}{e^z - 1}\right) = \frac{z^2 e^{zx}}{e^z - 1} = \sum_{n=0}^{\infty} nB_{n-1}(x) \frac{z^n}{n!}$$

D'où le résultat par identification.

■

Remarque : On déduit facilement en évaluant (1) en $x = 0$ que $\forall\, n \neq 1,\ B_n(1) = B_n(0) = B_n$.

Proposition 5
$$\forall\, k \in \mathbb{N}^*, \quad \zeta(2k) = (-1)^k \pi^{2k} \frac{2^{2k-1}}{(2k-1)!} \left(\frac{-B_{2k}}{2k}\right)$$

Démonstration. Soit $\bar{B}_n$ la fonction 1-périodique qui coincide avec B_n sur $]0,1[$ et telle que $\bar{B}_n(0) = \frac{B_n(0)+B_n(1)}{2}$.

Soit $n \in \mathbb{N}^*$, on calcule les coefficients de Fourier $c_k(\bar{B}_n)$ de $\bar{B}_n$: par la proposition 4 on a immédiatement $c_0(\bar{B}_n) = 0$ puis à l'aide de la remarque **??** et d'une intégration par parties on trouve $c_k(\bar{B}_1) = \frac{-1}{2i\pi k}$. On trouve, également en intégrant par parties : $\forall\, n > 1\ c_k(\bar{B}_n) = \frac{n}{2i\Pi k} c_k(\bar{B}_{n-1})$, et en terminant par récurrence on obtient :

$$c_k(\bar{B}_n) = \frac{-n!}{(2i\pi k)^n} \quad \text{puis} \quad \forall\, n \in \mathbb{N}^*,\ \bar{B}_n = \sum_{k \in \mathbb{Z}^*} \frac{n!}{(2i\Pi k x)^n} e^{2i\pi kx}$$

Enfin, en posant $n = 2l$ avec $l \in \mathbb{N}^*$ et en évaluant en $x = 0$ obtient le résultat souhaité. ■

1.2 Prolongement

Théorème 6 *La fonction ζ admet un prolongement méromorphe sur $\mathbb{C}$ avec un unique pôle en $s = 1$ qui est simple.*

Démonstration. On utilise les fonctions $\bar{B_n}(X)$ définies dans la démonstration précédente.

Lemme 7 *On a, pour $s \neq 1$, $\zeta(s) = \frac{1}{s-1} + \frac{1}{2} - s\int_1^{\infty} \frac{\bar{B_1}(u)}{u^{s+1}} du$.*
Et l'intégrale converge pour $\Re es > 0$

Démonstration. On a $\bar{B_1}(u) = u - [u] - \frac{1}{2}$, on écrit :

$$\begin{aligned}
s\int_1^n \frac{u-[u]}{u^{s+1}} du &= \left[-\frac{s}{(s-1)u^{s-1}}\right]_1^n + \sum_{k=1}^{n-1} k\left[\frac{1}{u^s}\right]_k^{k+1} \\
&= \frac{s}{s-1} - \frac{s}{(s-1)n^{s-1}} + (-1 + \frac{1}{2^s}) + \cdots + (n-1)(-\frac{-1}{(n-1)^s} + \frac{1}{n^s}) \\
&= \frac{s}{s-1} - 1 - \frac{1}{2^s} - \cdots - \frac{1}{n^s} + \frac{1}{n^{s-1}} - \frac{s}{(s-1)n^{s-1}} \\
&= 1 + \frac{1}{s-1} - \sum_{k=1}^{n} \frac{1}{k^s} - \frac{1}{(s-1)n^{s-1}}
\end{aligned}$$

Puis il suffit de faire tendre n vers l'infini et de remarquer que :

$$\frac{1}{2} - s\int_1^\infty \frac{u-[u]-\frac{1}{2}}{u^{s+1}}du = \lim_{n\to\infty}(-s\int_1^n \frac{u-[u]}{u^{s+1}}du) + 1$$

■

On a maintenant le lemme suivant :

Lemme 8 *Soit $n \in \mathbb{N}^*$ et s tel que $\Re es > 0$. On a :*

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \frac{s}{2!}B_2 + \frac{s(s+1)}{3!}B_3 + \ldots + \frac{s(s+1)\cdots(s+n-2)}{n!}B_n - \frac{s(s+1)\cdots(s+n-1)}{n!}\int_1^n \frac{\bar{B_n}(u)}{u^{s+n}}du$$

Démonstration. Par récurrence, pour $n = 1$ c'est le lemme précédent. Pour $n > 1$ on a :

$$\begin{aligned}\int_1^n \frac{\bar{B_n}(u)}{u^{s+n}} &= \left[\frac{\bar{B_{n+1}}(u)}{(n+1)u^{s+n}}\right]_1^\infty + \int_1^\infty \frac{\bar{B_{n+1}}(u)(s+n)}{(n+1)u^{s+n+1}}du \\ &= -\frac{B_{n+1}}{n+1} + \frac{s+n}{n+1}\int_1^\infty \frac{\bar{B_{n+1}}(u)}{u^{s+n+1}}du.\end{aligned}$$

■

On en déduit que $\forall\, n \geq 1$, $\zeta(s)$ admet un prolongement méromorphe sur $\{s \in \mathbb{C},\ /\ \Re es > 1-n\}$ donc sur $\mathbb{C}$ avec un unique pôle en $s = 1$ qui est simple. ■

1.3 Equation fonctionnelle

Proposition-Définition 9 *Soit $s \in \mathbb{C}$, $\Re es > 0$. On pose :*

$$\Gamma(s) : = \int_0^\infty e^{-t}t^s\frac{dt}{t}.$$

On a $\Gamma(s+1) = s\Gamma(s)$, $\Gamma'(1) = 1$ et pour $k \in \mathbb{N}$, $k > 1$, $\Gamma(k) = (k-1)!$

Théorème 10 *La fonction Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$ dont les pôles sont les entiers négatifs ou nul.*

Démonstration. On voit facilement que Γ est holomorphe pour $\Re es > 0$. En utilisant la relation $\Gamma(s) = \frac{\Gamma(s+1)}{s}$, on obtient pour $n \in \mathbb{N}^*$, $\Gamma(s) = \frac{\Gamma(s+n)}{s(s+1)\ldots(s+n-1)}$ d'où un prolongement méromorphe sur $\mathbb{C}$ avec des pôles en les entiers négatifs. ■

Définition 11 $\Lambda(s) : = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$.

Théorème 12 *On a pour $s \in \mathbb{C}$, $\Lambda(1-s) = \Lambda(s)$.*

Démonstration. Posons pour $t \in \mathbb{R}$, $\Theta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}$.

Lemme 13 *On pour $\Re es > 1$,*

$$\Lambda(s) = \frac{1}{2}\int_0^\infty (\Theta(t)-1)t^{\frac{s}{2}}\frac{dt}{t}.$$

Démonstration. Tout étant positif, par le théorème de convergence monotone on a :

$$\begin{aligned}\int_0^\infty \left(\sum_{n=1}^\infty e^{-n^2\pi t}\right) t^{\frac{s}{2}}\frac{dt}{t} &= \sum_{n=1}^\infty \int_0^\infty e^{-n^2\pi t} t^{\frac{s}{2}}\frac{dt}{t} \\ &= \sum_{n=1}^\infty \frac{1}{(n^2\pi)^{\frac{s}{2}}}\int_0^\infty e^{-u}u^{\frac{s}{2}}\frac{du}{u} = \Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) = \Lambda(s),\end{aligned}$$

en posant $u = n^2\pi t$. ■

Lemme 14 *Si $t \in \mathbb{R}_+^*$, $\Theta(t) = t^{\frac{1}{2}}\Theta(\frac{1}{t})$.*

Démonstration. Soit t fixé, posons $g(x) = \sum_{m\in\mathbb{Z}} e^{-\pi(x+m)^2 t}$ qui est C^2 et 1-périodique. On a $g(x) = \sum_{n\in\mathbb{Z}} c_n e^{2i\pi nx}$ où les c_n sont les coefficients de fourier. On a par le théorème de convergence dominée :

$$c_n = \int_0^1 \sum_{m\in\mathbb{Z}} e^{-\pi(x+m)^2 t}e^{-2i\pi nx}dx = \sum_{m\in\mathbb{Z}}\int_0^1 e^{-\pi(x+m)^2 t}e^{-2i\pi nx}dx.$$

Losrque x parcourt $[0,1]$ et m parcourt $\mathbb{Z}$, $x+m$ parcourt $\mathbb{R}$. D'où :

$$\begin{aligned}c_n &= \int_{-\infty}^\infty e^{-\pi x^2 t}e^{-2i\pi nx}dx \quad \text{si on pose} \quad w^2 = x^2 t \\ &= \int_{-\infty}^\infty e^{-\pi w^2}e^{-2i\pi\frac{xw}{t^{\frac{1}{2}}}}\frac{dw}{t^{\frac{1}{2}}} = e^{-\pi\left(\frac{x}{t^{\frac{1}{2}}}\right)^2}\frac{1}{t^{\frac{1}{2}}}\end{aligned}$$

On a $g(0) = \Theta(t) = \sum_{n\in\mathbb{Z}} \frac{e^{-\pi n^2\frac{1}{t}}}{t^{\frac{1}{2}}} = \frac{1}{t^{\frac{1}{2}}}\Theta(t)$. ■

On peut maintenant démontrer le théorème. On a :

$$\begin{aligned}\Lambda(s) &= \frac{1}{2}\int_1^\infty (\Theta(t)-1)t^{\frac{s}{2}}\frac{dt}{t} + \frac{1}{2}\int_0^1 \Theta(t)t^{\frac{s}{2}}\frac{dt}{t} - \frac{1}{2}\int_0^1 t^{\frac{s}{2}}\frac{dt}{t} \\ &= \frac{1}{2}\int_1^\infty \Theta\left(\frac{1}{t}\right)t^{1-\frac{s}{2}}\frac{dt}{t^2} - \frac{1}{s}\end{aligned}$$

grâce au changement de variable $t \mapsto \dfrac{1}{t}$

$$\begin{aligned}&= \frac{1}{2}\int_1^\infty \Theta(t)t^{-\frac{s}{2}-\frac{1}{2}}dt - \frac{1}{s}\end{aligned}$$

car $\Theta(t) = t^{\frac{1}{2}}\Theta\left(\dfrac{1}{t}\right)$

$$\begin{aligned}&= \frac{1}{2}\int_1^\infty (\Theta(t)-1)t^{-\frac{s}{2}-\frac{1}{2}}dt - \frac{1}{s} + \frac{1}{2}\int_1^\infty t^{-\frac{1}{2}-\frac{s}{2}}dt \\ &= \frac{1}{2}\int_1^\infty (\Theta(t)-1)t^{-\frac{s}{2}-\frac{1}{2}}dt - \frac{1}{s} - \frac{1}{1-s} \\ &= \frac{1}{2}\int_1^\infty (\Theta(t)-1)(t^{\frac{s}{2}} + t^{\frac{1-s}{2}})\frac{dt}{t} - \frac{1}{1-s} - \frac{1}{s}.\end{aligned}$$

L'intégrale converge uniformément sur toute la bande verticale car :

$$\left|\frac{\Theta(t)-1}{2}\right| = \left|\sum_{n=1}^\infty e^{-\pi n^2 t}\right| \leq \sum_{n=1}^\infty e^{-\pi nt} = \frac{e^{-\pi t}}{1-e^{-\pi t}}$$

Donc $\Lambda(s)$ est méromorphe sur $\mathbb{C}$ avec des pôles, simples, en $s=0$ et $s=1$ et comme la formule est invariante par $s \mapsto 1-s$ c'est gagné. ■

Corollaire 15

$$\forall\, k \in \mathbb{N}^*, \qquad \zeta(1-2k) = -\frac{B_{2k}}{k}$$

Démonstration. En utilisant les formules $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$ et $\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) = 2^{\frac{1}{2}-s}(2\pi)^{\frac{1}{2}}\Gamma(s)$ et l'équation fonctionnelle on trouve le résultat souhaité. ■

2 Les fonctions de Dirichlet

2.1 Les caractères de Dirichlet

Proposition-Définition 16 *Un caractère est un morphisme de groupes $\chi : (\frac{\mathbb{Z}}{n\mathbb{Z}})^* \to \mathbb{C}^*$.*

Si $m|n$ alors χ induit un morphisme $(\frac{\mathbb{Z}}{m\mathbb{Z}})^* \to \mathbb{C}^*$ par composition avec l'application naturelle $(\frac{\mathbb{Z}}{m\mathbb{Z}})^* \to (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. Alors χ peut être définit mod n ou mod m si les deux définitions sont les mêmes. On choisi le n minimum qui permet de définir χ et on l'appelle le conducteur de χ.

Remarque : On considèrera χ, de conducteur f, comme une application $\mathbb{Z} \to \mathbb{C}$ en posant $\chi(a) = 0$ si $(a, f) \neq 1$. χ est alors périodique de période f.

2.2 Les L-séries de Dirichlet

Définition 17 *Soit χ un caractère de Dirichlet de conducteur f. La L-série attachée à χ est définie par :*

$$L(s,\chi) \ := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad \textit{si } \Re e(s) > 1.$$

Remarque : On sait que $L(s,\,\chi)$ admet un prolongement holomorphe sur $\mathbb{C}$, sauf en un pôle simple en $s=1$ quand $\chi = 1$.

Définition 18 *On définit la fonction Hurwitz zeta par :*

$$\zeta(s,b) \ := \sum_{n=0}^{\infty} \frac{1}{(b+n)^s} \qquad \textit{si } \Re e(s) > 1 \textit{ et } 0 < b \leq 1.$$

Proposition 19 *Soit χ un caractère de conducteur f on a :*

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

Démonstration. Le résultat est évident par périodicité de χ. ■

Définition 20 *On définit les nombres de Bernouilli généralisés par :*

$$\sum_{n=0}^{\infty} \mathbb{B} \frac{t^n}{n!} \ := \sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft}-1}.$$

Proposition 21 *Soit F un multiple de f. Alors :*

$$\mathbb{B} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

Démonstration.

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

Posons $g = \frac{F}{f}$ et $a = b + cf$. Alors on a :

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

Le résultat suit. ■

Théorème 22 *Si $n \geq 1$, $L(1-n,\chi) = \frac{-B_{n,\chi}}{n}$.*
On a, de facon plus générale, $\zeta(1-n,b) = \frac{-B_n(b)}{n}$ si $0 < b \leq 1$.

Démonstration. Posons :

$$F(t) = \frac{te^{(1-b)t}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(1-b) \frac{t^n}{n!}.$$

On définit $H(s) = \int_D F(z) z^{s-2} dz$, où l'intégrale porte sur le domaine D définit par la partie supérieure de l'axe des réel positifs, le cercle C_ϵ autour de zéro de rayon ϵ, et la partie inférieure de l'axe des réels positifs. $z \mapsto z^s$ est définit par $\exp(s\mathrm{Log}(z))$, où la fonction Log complexe est définit par $\mathrm{Log}(z) = \mathrm{Log}(R + i\theta)$ si $z = Re^{i\theta}$ avec $R > 0$ et $\theta \in [0,\, 2\pi[$. $H(s)$ est analytique pour tout s. On écrit :

$$H(s) = (e^{2\pi i s} - 1) \int_{\epsilon}^{\infty} F(t) t^{s-2} dt + \int_{C_\epsilon} F(z) z^{s-2} dz.$$

Prenons un s tel que $\Re e(s) > 1$ alors $\int_{C_\epsilon} \to 0$ quand $\epsilon \to 0$ et :

$$\begin{aligned} H(s) &= (e^{2\pi i s} - 1) \int_0^{\infty} F(t) t^{s-2} dt = (e^{2\pi i s} - 1) \int_0^{\infty} t^{s-1} \sum_{m=0}^{\infty} e^{-(b+m)t} dt \\ &= (e^{2\pi i s} - 1) \sum_{m=0}^{\infty} \int_0^{\infty} t^{s-1} e^{-(b+m)t} dt = (e^{2\pi i s} - 1) \sum_{m=0}^{\infty} \frac{1}{(m+b)^s} \Gamma(s) \\ &= (e^{2\pi i s} - 1) \Gamma(s) \zeta(s,\, b). \end{aligned}$$

D'où $\zeta(s,b) = \frac{H(s)}{(e^{2\pi i s}-1)\Gamma(s)}$, ce qui nous donne un prolongement analytique de $\zeta(s,\, b)$, pour tout $s \neq 1$.

On se donne maintenant un s tel que $s = 1 - n$, où $n \in \mathbb{N}^*$. On a $e^{2\pi i s} = 1$ et,

$$H(1-n) = \int_{C_\epsilon} F(z) z^{-n-1} dz = (2\pi i) \frac{B_n(1-b)}{n!}.$$

On voit facilement que :

$$\lim_{s \to 1-\pi} (e^{2\pi i s} - 1) \Gamma(s) = \frac{(2\pi i)(-1)^{n-1}}{(n-1)!}.$$

et donc :

$$\zeta(1-n,b) = (-1)^{n-1} \frac{B_n(1-b)}{n} = -\frac{B_n(b)}{n}.$$

Par conséquent :

$$\begin{aligned} L(1-n,\,\chi) &= \sum_{a=1}^{f}\chi(a)f^{n-1}\zeta(1-n,\,\frac{a}{f}) = -\frac{1}{n}\sum_{a=1}^{f}\chi(a)f^{n-1}B_n\left(\frac{a}{f}\right) \\ &= -\frac{B_{n,\chi}}{n}. \end{aligned}$$

■

3 Étude de $\mathbb{Q}_p$

3.1 Construction de $\mathbb{Q}_p$

On étend la valuation p-adique notée v_p, déjà définie sur $\mathbb{Z}$, à $\mathbb{Q}$ par : $v_p(\frac{n}{d}) = v_p(n) - v_p(d)$. On peut alors définir la valeur absolue p-adique sur $\mathbb{Q}$ en posant $|x|_p = p^{-v_p(x)}$ avec les conventions $p^{-\infty} = 0$ et $v_p(0) = \infty$. En fait, cette valeur absolue est ultramétrique, c'est-à-dire que

$$|x+y|_p \leq \max\{|x|_p\,,\,|y|_p\}.$$

En tant que telle, elle vérifie la propriété suivante. Si x et y ont des valeurs absolues p-adiques distinctes, $|x-y|_p = \max\{|x|_p\,,\,|y|_p\}$. Autrement dit, tout triangle est isocèle. Cette propriété est évidemment vraie dans tout corps valué ultramétrique.

De même :

Proposition 23 *Soit K un corps valué hypermétrique complet. Alors une série $\sum x_n$ converge si et seulement si $x_n \to 0$ quand $n \to \infty$.*

Démonstration. Si $x_n \to 0$, alors la suite des sommes partielles est de Cauchy. En effet, si $\varepsilon > 0$ et $N \in \mathbb{N}$ tel que si $n \geq N$, $|x| \leq \varepsilon$, alors si $n > m \geq N$, on a $|\sum_{i=0}^{n} x_i - \sum_{i=0}^{m} x_i| = \left|\sum_{i=m+1}^{n} x_i\right| \leq \max_{i=m+1}^{n} |x_i| \leq \varepsilon$. Donc elle converge. ■

Proposition-Définition 24 *On peut étendre la valeur absolue ultramétrique $|\cdot|_p$ à un unique surcorps (à isomorphisme isométrique près) $\mathbb{Q}_p$ de $\mathbb{Q}$, de telle façon que l'espace métrique $(\mathbb{Q}_p,\,|\cdot|_p)$ soit complet et que $\mathbb{Q}$ soit dense dans $\mathbb{Q}_p$. Ce corps est appelé le corps p-adique.*

Démonstration. Soit E l'ensemble des suites de rationnels qui sont de Cauchy pour $|\cdot|_p$, muni de la structure naturelle d'anneau commutatif, l'idéal I des suites qui tendent vers zéro est maximal. On sait alors que $\mathbb{Q}_p := E/I$ est un corps ; c'est lui notre candidat : c'est un surcorps de $\mathbb{Q}$ si on considère l'injection i qui à x associe la suite constante (x). Si $(x_n) \in E$ et $(\epsilon_n) \in I$ et si l'on note $\varphi : E \to \mathbb{Q}_p$ le morphisme surjectif canonique, alors $|x_n|_p - |\epsilon_n|_p \leq |x_n + \epsilon_n|_p \leq |x_n|_p + |\epsilon_n|_p$, $||x_n|_p - |y_n|_p| \leq |x_n - y_n|_p$, et donc, comme $(\mathbb{R},\,|\cdot|)$ est complet, on peut étendre $|\cdot|_p$ par $|\varphi((x_n)_n)|_p = \lim\limits_{n\to\infty}^{(\mathbb{R},\,|\cdot|)} |x_n|_p$. Par passage à la limite, c'est une valeur absolue ultramétrique. Pour montrer que $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$, on prend $x = \varphi((x_n)_n)$ dans $\mathbb{Q}_p$ et il suffit de vérifier que $(i(x_n))_n$ converge vers x.

En ce qui concerne la complétude, si $(x_n) \in \mathbb{Q}_p^{\mathbb{N}}$ est une suite de Cauchy, il suffit de trouver, par densité, pour tout n un rationnel y_n tel que $|x_n - y_n|_p \leq n^{-1}$. On vérifie facilement que cette suite est de Cauchy et, si on note $y = \varphi((y_n)_n)$, que y est la limite de (x_n) dans $\mathbb{Q}_p$.

Montrons l'unicité. Soient $(K, |\cdot|_K)$ et $(L, |\cdot|_L)$ deux corps vérifiant les hypothèses. On définit ϕ en disant que si $x \in K$ et $(x_n) \in \mathbb{Q}^{\mathbb{N}}$ tel que $x = \overset{(K,|\cdot|_K)}{\lim\limits_{n\to\infty}} x_n$, on pose $\phi(x) = \overset{(L,|\cdot|_L)}{\lim\limits_{n\to\infty}} x_n$. Clairement, ϕ est un morphisme injectif ; il est surjectif car $\mathbb{Q}$ est dense dans L. Enfin, on a $|\phi(x)|_L = \lim\limits_{n\to\infty} |x_n|_L$ par continuité ; or, $|x_n|_L = |x_n|_K$ et donc ϕ est une isométrie. ■

Définition 25 *On appelle anneau des entiers p-adiques et on note $\mathbb{Z}_p$ la boule unité fermée de $\mathbb{Q}_p$.*

En fait, cette construction est la même que celle du complété pour toute valeur absolue de $\mathbb{Q}$. C'est donc ainsi que l'on construit $\mathbb{R}$. On dit que valeurs absolues sont équivalentes si elles induisent les mêmes topologies. Le théorème d'Ostrowski ([1]) affirme que les valeurs absolues p-adiques sont les seules autres valeurs absolues non triviales sur $\mathbb{Q}$ (à équivalence près) que $|\cdot|$. $\mathbb{Q}_p$ est donc l'analogue générique de $\mathbb{R}$, si l'on voit $\mathbb{R}$ comme complété de $\mathbb{Q}$, et c'est le seul.

La bonne façon de voir $\mathbb{Q}_p$ (c'est la première construction historique, donnée par Hensel) est décrite dans la :

Proposition 26 *Soit $x \in \mathbb{Q}_p$, il existe une unique suite $(a_n) \in [\![0, p-1]\!]^{\mathbb{Z}}$ et un entier n_0 tels que si $n < n_0$, $a_n = 0$ et $x = \sum\limits_{n\geq n_0} a_n p^n$. Cette série est appelée développement de Hensel de x.*

Démonstration. Commençons par l'unicité. Si $a = \sum\limits_{n\geq n_0} a_n p^n$ et $b = \sum\limits_{n\geq n_1} b_n p^n$ sont deux telles séries différentes, notons n_2 le plus petit relatif tel que $a_{n_2} \neq b_{n_2}$. Alors, $0 = |a-b|_p = \left|(a_{n_2} - b_{n_2})p^{n_2} + \sum\limits_{n\geq n_2+1}(a_n - b_n)p^n\right|_p = p^{-n_2}$, d'après le principe des triangles isocèles. En effet, $|(a_{n_2} - b_{n_2})p^{n_2}|_p = p^{-n_2}$ et $\left|\sum\limits_{n\geq n_2+1}(a_n - b_n)p^n\right|_p \leq p^{-(n_2+1)}$, car $|\cdot|_p$ est ultramétrique. C'est absurde.

On se ramène au cas où $|x|_p = 1$, en multipliant x par une puissance convenable de p ; en effet, l'ensemble des valeurs absolues p-adiques des rationnels est $\{p^n,\, n \in \mathbb{Z}\} \cup \{0\}$, qui est un fermé pour $(\mathbb{R}, |\cdot|)$ et est donc égal à l'ensemble des valeurs absolues de $\mathbb{Q}_p$. Ainsi, si $x \neq 0$, $|x|_p = p^m$, pour m bien choisi, et on multiplie x par p^m. On montre alors qur l'on peut approcher x par une suite d'entiers positifs $(n_i)_{i\geq 1}$ tels que $|x - n_i|_p \leq p^{-i}$ et $x_i \leq p^i - 1$.

Démontrons d'abord le résultat pour $x = \frac{a}{b} \in \mathbb{Q}$. Si l'on choisit a et b premiers entre eux, comme $|x|_p = 1$, $p \nmid b$ et donc p^i et b sont premiers entre eux, et on choisit une relation de Bezout $kp^i + lb = 1$ (on choisit l de telle sorte que al soit un entier positif). Dès lors, $\left|\frac{a}{b} - al\right|_p = \left|\frac{a}{b}(1 - lb)\right|_p = \left|kp^i\right|_p \leq p^{-i}$. On peut alors écrire la décomposition de al en base p : $al = \sum\limits_{j<i} c_j p^j + \sum\limits_{j\geq i} c_j p^j$. On a bien $d = \sum\limits_{j<i} c_j p^j \leq p^i - 1$ et $|x-d|_p = |x - al + (al - d)|_p \leq \max\left\{|x - al|_p\,,\, \left|\sum\limits_{j\geq i} c_j p^j\right|_p\right\} = p^{-i}$.

Maintenant, si $x \in \mathbb{Q}_p$, on choisit $y \in \mathbb{Q}$ tel que $|x - y|_p \leq p^{-i}$ et $n_i \leq p^i - 1$ tel que $|y - n_i|_p \leq p^{-i}$. On obtient que $|x - n_i|_p = |(x-y) + (y - n_i)|_p \leq p^{-i}$.

Pour finir, il suffit de voir, si $x \in \mathbb{Q}_p$ et $(n_i)_{i\geq 1}$ la suite d'entiers associés, alors n_i et n_{i+1} ont leur i premiers termes de la décomposition en base p égaux. Cela est vrai car $|n_i - n_{i+1}|_p \leq p^{-i}$ et donc, dans le décompositon en base p, les termes en p^j, où $j < i$ se simplifient. Par conséquent, les n_i sont les sommes partielles d'une série de la forme $\sum a_n p^n$, avec $a_n \leq p - 1$, qui converge vers x. ■

3.2 Lemme de Hensel

Nous présentons maintenant un même résultat, exprimé sous deux formes équivalentes, analogue à le méthode de Newton en ce qui concerne $\mathbb{R}$, qui permet de trouver des racines d'équations polynômiales dans $\mathbb{Q}_p$.

Avant de continuer, introduisons une notation. Si x, y, $z \in \mathbb{Q}_p$, on écrit $x \equiv_{\mathbb{Z}_p} y \mod z$ si z divise $x - y$ dans $\mathbb{Z}_p$, c'est-à-dire s'il existe $z' \in \mathbb{Z}_p$ tel que $zz' = x - y$. La plupart du temps, on écrira $x \equiv_{\mathbb{Z}_p} y \mod p^N$, ce qui signifie $|x - y|_p \leq p^{-N}$.

Théorème 27 (Lemme de Hensel analytique) *Soient $P \in \mathbb{Z}_p[X]$ et $a_0 \in \mathbb{Z}_p$ tels que $|P(a_0)|_p \leq 1/p$ et $P'(a_0) \in \mathbb{Z}_p^\times$. Alors il existe $a \in \mathbb{Z}_p$ tel que $|a - a_0|_p \leq 1/p$ et $P(a) = 0$.*

Notons que $\chi_p : \begin{array}{c} \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z} \\ x \mapsto \{x\}_1 \end{array}$ est un morphisme d'anneaux.

Théorème 28 (Lemme de Hensel algébrique) *Soient $P \in \mathbb{Z}_p[X]$ et $a_0 \in \mathbb{Z}_p$ tels que $\chi_p(P)(\chi_p(a_0)) = 0$ et $\chi_p(P)'(\chi_p(a_0)) \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$. Alors, il existe $a \in \mathbb{Z}_p$ tel que $a \equiv_{\mathbb{Z}_p} a_0 \mod p$ et $P(a) = 0$.*

Démonstration. On s'inspire directement de la méthode de Newton pour définir par récurrence la suite a_n telle que $a_n = a_{n-1} - \frac{P(a_{n-1})}{P'(a_{n-1})}$. Justifions cette définition en montrant par récurrence sur n que $a_{n+1} \equiv_{\mathbb{Z}_p} a_n \mod p^{n+1}$, $|P(a_n)|_p \leq p^{-(n+1)}$ et $P'(a_n) \in \mathbb{Z}_p^\times$.

Pour $n = 0$, on doit juste montrer que $|a_1 - a_0|_p = \left|\frac{P(a_0)}{P'(a_0)}\right|_p = \frac{|P(a_0)|_p}{|P'(a_0)|_p} \leq p^{-1}$, ce qui est clair écrit sous cette forme.

Supposons le résultat vrai au rang n. Alors, en refaisant ce que l'on vient de faire, il est clair que $a_{n+2} \equiv_{\mathbb{Z}_p} a_{n+1} \mod p^{n+2}$. Par ailleurs, si l'on note $P = \sum_{i=0}^n c_i X^i$, alors, en notant $\frac{P(a_n)}{P'(a_n)} = \lambda p^{n+1}$ (avec $\lambda \in \mathbb{Z}_p$),

$$\begin{aligned} P(a_{n+1}) = P(a_n - \lambda p^{n+1}) &= \sum_{i=0}^n c_i(a_n - \lambda p^{n+1})^i = \sum_{i=0}^n c_i (a_n)^i - i(a_n)^{i-1}\lambda p^{n+1} + p^{n+2}\mu \quad \text{avec } \mu \in \mathbb{Z}_p \\ &= P(a_n) - P'(a_n)\lambda p^{n+1} + p^{n+2}\mu \\ &\equiv_{\mathbb{Z}_p} 0 \mod p^{n+2}, \end{aligned}$$

ce qu'on voulait. Enfin, en faisant le même calcul avec P', on s'aperçoit que $P'(a_{n+1}) = P'(a_n - \lambda p^{n+1}) = P'(a_n) - \lambda p^{n+1} P''(a_n) + p^{n+2}\mu \equiv_{\mathbb{Z}_p} P'(a_n) \mod p$.

Finalement, les propriétés démontrées par récurrence montrent que la suite a_n converge vers a tel que $P(a) = 0$ et $a \equiv_{\mathbb{Z}_p} a_0 \mod p$. ■

Remarque : Il existe en fait une version plus forte du lemme de Hensel algébrique qui dit que si $P \in \mathbb{Z}_p[X]$ se décompose en produit de deux polynômes premiers entre eux dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors on peut relever cette décomposition en une décomposition dans $\mathbb{Z}_p[X]$.

3.3 Représentants de Teichmüller

En application du lemme de Hensel, on définit les représentants $(\alpha_i)_{0 \leq i \leq p-1}$ de Teichmüller.

Considérons le polynôme $X^{p-1} - 1$. Il est scindé à racines simples dans $znzp$ et $(p-1)x \neq 0$ si x est racine de $X^{p-1} - 1$. Donc ses racines $(\alpha_i = i + px_i)_{1 \leq i \leq p-1}$ se relèvent en des racines $p-1$-

ièmes de l'unité dans $\mathbb{Z}_p$. On a évidemment $\alpha_1 = 1$. On pose aussi $\alpha_0 = 0$ et donc, finalement, on peut caractériser les représentants de Teichmüller ainsi :

Proposition-Définition 29 (Représentants de Teichmüller) *Il existe une unique famille $(\alpha_i)_{0\leq i\leq p-1} \in (\mathbb{Z}_p)^p$ appelée famille des représentants de Teichmüller telle que, pour tout $i \in [\![0, p-1]\!]$, $\alpha_i \equiv_{\mathbb{Z}_p} i \mod p$ et $\alpha_i^p = \alpha_i$.*

Par ailleurs, on a $\alpha_0 = 0$ et $\alpha_1 = 1$.

On note $\mu_{p-1} = \{\alpha_1, \ldots, \alpha_{p-1}\} \subset \mathbb{Z}_p$ le groupe de racines $(p-1)$-ièmes de l'unité.

3.4 Polynômes irréductibles

On aura besoin dans la suite de savoir que quelques polynômes sont irréductibles. Voici un critère simple et classique d'irréductibilité.

Théorème 30 (Critère d'irréductibilité d'Eisenstein) *Soit $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}_p[X]$ tel que*

- $a_n \not\equiv_{\mathbb{Z}_p} 0 \mod p$;
- $\forall\, 0 \leq i < n,\ a_i \equiv_{\mathbb{Z}_p} 0 \mod p$;
- $a_0 \not\equiv_{\mathbb{Z}_p} 0 \mod p^2$.

Alors, P est irréductible dans $\mathbb{Q}_p[X]$.

Démonstration. Comme $\mathbb{Z}_p$ est factoriel, d'irréductible p, on sait (en utilisant les contenus de Gauß) que si P est réductible sur $\mathbb{Q}_p[X]$, il l'est sur $\mathbb{Z}_p[X]$. Écrivons donc $P = QR$, avec $R,\, Q \in \mathbb{Z}_p[X]$. On peut réduire cette écriture modulo p, et on obtient $\chi_p(P) = \chi_p(Q)\chi_p(R) = \lambda X^n$. Donc $\chi_p(Q)$ comme $\chi_p(R)$ s'écrivent μX^l, donc $Q(0)$ et $R(0)$ sont divisible par p donc $P(0) = Q(0)R(0)$ est divisible par p^2 : c'est absurde. ■

Application 31 *Pour tout $n \geq 1$, le polynôme*

$$\frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = \sum_{i=0}^{p-1} X^{ip^{n-1}}$$

est irréductible dans $\mathbb{Z}_p[X]$.

Démonstration. Notons P_n le polynôme à considérer. Si P_n est réductible, il en est de même pour $Q_n = P_n(X+1)$. Il suffit donc de montrer l'irréductiblité de $Q_n \in \mathbb{Z}[X]$. Étudions la réduction modulo p de Q_n. On a :

$$\begin{aligned}
\chi_p(Q_n) &= \sum_{i=0}^{p-1} \left((X+1)^i\right)^{p^{n-1}} = \left(\sum_{i=0}^{p-1} (X+1)^i\right)^{p^{n-1}} \quad \text{dans } \mathbb{F}_p \\
&= \left(\frac{(X+1)^p - 1}{X+1-1}\right)^{p^{n-1}} = X^{p^{n-1}(p-1)} \quad \text{dans } \mathbb{F}_p.
\end{aligned}$$

Ainsi, tous les coefficients sauf le coefficient principal de Q_n sont divisibles par p. Comme le coefficient constant, qui se calcule aisément, vaut p, le critère d'Eisenstein s'applique, et le résultat en découle. ■

Remarque : Il se passe la même chose dans $\mathbb{Z}[X]$. C'est d'ailleurs un corollaire de cette application.

3.5 Construction de $\mathbb{C}_p$

Donnons-nous dès maintenant le meilleur cadre pour faire de l'analyse p-adique : l'équivalent p-adique de $\mathbb{C}$, $\mathbb{C}_p$.

3.5.1 Extension de valeur absolue

On considère un corps K muni d'une valeur absolue notée $|\cdot|$. Soit V un K-ev de dimension n et soit $(e_1, \dots, e_n)$ une base. On définit :

$$|a_1e_1 + \cdots + a_ne_n|_\infty = \max_{1\leq i\leq n} |a_i|$$

Lemme 32 *Si K est localement compact et V un K-ev de dimension finie muni de $|.|_\infty$ alors V est localement compact et la boule $\bar{B}_V := \{x \in V \ / \ |x|_\infty \leq 1\}$ est compacte.*

On prouvera plus loin (voir la proposition 48) que $\mathbb{Q}_p$ est localement compact.

Démonstration. On remarque que les homothéties de K sont des applications continues. Soit $\epsilon > 0$ tel que la boule $\bar{B}_K(0, \epsilon) := \{x \in K \ / \ |x| \leq \epsilon\}$ soit compacte. On choisit une homothétie h de K de rapport suffisamment grand telle que h($\bar{B}_K(0, \epsilon)$) contienne la boule $\bar{B}_K(0, 1)$ qui est donc compacte.

Soit maintenant $(e_1, \dots, e_m)$ une base de V et $(x_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\bar{B}_V(0, 1)$.On pose $x_n = a_1^n e_1 + \ldots + a_m^n e_m$. Comme $|x|_\infty \leq 1$, on a, $\forall\, i \in [\![1, m]\!]$, $a_i^n \in \bar{B}_K(0, 1)$. $\bar{B}_K(0, 1)$ étant compacte, on extrait Φ croissante telle que $\forall\, i$, $a_i^{\Phi(n)} \to a_i \in \bar{B}_K(0, 1)$. On a alors $x_{\Phi(n)} \to a_1e_1 + \cdots + a_ne_n$ pour $||\cdot||_\infty$ et $|a_1e_1 + \ldots + a_me_m|_\infty \leq 1$. ■

Théorème 33 *Si K est localement compact et si V est un K-ev de dimension finie alors toutes les normes sur V sont équivalentes.*

Démonstration. Soit $(e_1, \dots, e_n)$ une base de V et $|\cdot|_V$ une norme sur V. On a pour $x = a_1e_1 + \cdots + a_ne_n$:

$$|x|_V \leq |a_1|\,|e_1|_V + \cdots + |a_n|\,|e_n|_V \leq n \left(\max_{1\leq i\leq n} |a_i|\right)\left(\max_{1\leq i\leq n} |e_i|_V\right),$$

donc $|.|_V \leq c_1\,|.|_\infty$ en posant $c_1 = n\ \max_{1\leq i\leq n}(|e_i|_V)$.

Posons $U = \{x \in V \ / \ |x|_\infty = 1\}$. On sait que $\exists \epsilon > 0$ tel que $\forall\, x \in U$, $|x|_V \geq \epsilon$, car sinon il existe une suite (x_n) d'éléments de U telle que $|x_n|_V \to 0$. Par le lemme 32, U étant fermé dans un compact est compact, et il existe une sous suite (x_{n_k}) qui converge pour $|\cdot|_\infty$ vers $x \in U$ mais pour tout k,

$$|x|_V \leq |x - x_{n_k}|_V + |x_{n_k}|_V \leq c_1\,|x - x_{n_k}|_\infty + |x_{n_k}|_V$$

Or, $|x - x_{n_k}|_\infty \to 0$ et $Nox_{n_k}V \to 0$ donc $x = 0$; contradiction car $0 \notin U$.

Soit maintenant $x = a_1e_1 + \cdots + a_ne_n$ et j tel que $|a_j| = \max_{1\leq i\leq n} |a_i| = |x|_\infty$ alors $\frac{x}{a_j} \in U$ et donc $\left|\frac{x}{a_j}\right|_V \geq \epsilon$. En posant $c_2 = \frac{1}{\epsilon}$ on a alors $|x|_\infty = |a_j| \leq c_2\,|x|_V$ ■

Corollaire 34 *Si K est localement compact et L une extension finie de K alors il existe au plus une valeur absolue sur L qui étend la valeur absolue sur K (telle que $\forall\, x \in K$, $|x|_L = |x|$).*

Démonstration. Soit $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur L qui étendent celle de K. Ce sont donc également des normes sur L vu comme un K-ev de dimension finie. Par le théorème elles

sont équivalentes. On a $|.|_2 \leq c_1 |.|_1$. Soit x tel que $|x|_1 \neq |x|_2$, par exemple $|x|_1 < |x|_2$ (quitte à prendre l'inverse). Mais pour n assez grand, $c_1 |x^n|_1 < |x^n|_2$, contradiction. ■

Soit L une extension finie du corps K. Soit α un élément de L de degré n et soit $P(X) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[X]$ le polynôme minimal de α sur K.

Définition 35 *En considérant L comme un K-ev de dimension finie, la multiplication par α est une application K-linéaire ayant pour matrice A_α (à similitude près). On pose $\mathbb{N}_{L/K}(\alpha) := det(A_\alpha)$*

Proposition 36 *On note α_i les conjugués de α. On a :*

$$\mathbb{N}_{K(\alpha)/K}(\alpha) = (-1)^n a_0 = \prod_{i=1}^{n} \alpha_i$$

$$et \qquad \mathbb{N}_{L/K}(\alpha) = (\mathbb{N}_{K(\alpha)/K}(\alpha))^{[L:K(\alpha)]}$$

Démonstration. Pour le premier résultat on écrit la matrice de la multiplication par α dans la base $(1, \alpha, \ldots, \alpha^{n-1})$ et on calcule le déterminant. La seconde égalité s'obtient par les relations coefficients-racines.

Pour la dernière égalité on choisit $(1, \alpha, \ldots, \alpha^{n-1})$ comme base de $K(\alpha)$ sur K puis une base de L sur $K(\beta)$.On peut prendre pour base de L sur K tous les produits des éléments des deux bases. En posant $\tilde{A}_\alpha$ la matrice de la multiplication par α dans K(α) on a dans la base ainsi construite :

$A_\alpha = \begin{pmatrix} \tilde{A}_\alpha & 0 & & \\ 0 & \tilde{A}_\alpha & & \\ & & \ddots & \\ & & & \tilde{A}_\alpha \end{pmatrix}$ où $[L : K(\alpha)]$ est le nombre de blocs. ■

Remarque : Comme $\mathbb{N}_{L/K}(\beta)$ est définie comme le déterminant de la matrice de la multiplication par β dans L on a,

$$\forall\, \beta,\, \beta' \in L, \quad \mathbb{N}_{L/K}(\beta\beta') = \mathbb{N}_{L/K}(\beta)\mathbb{N}_{L/K}(\beta').$$

Théorème 37 *Soit K une extension finie de $\mathbb{Q}_p$, il existe une unique valeur absolue ultramétrique sur K qui étend la valeur absolue p-adique de $\mathbb{Q}_p$.*

Démonstration. On pose $n = [K : \mathbb{Q}_p]$ et on définit $|.|_p$ sur K par :

$$\forall\, \alpha \in K \quad |\alpha|_p = \left|\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p^{\frac{1}{n}}.$$

On remarque immédiatement que cette définition est cohérente avec l'ancienne définition pour $\alpha \in \mathbb{Q}_p$. On a remarqué que $\forall\, \beta,\, \beta' \in K,\, \mathbb{N}_{K/\mathbb{Q}_p}(\beta\beta') = \mathbb{N}_{K/\mathbb{Q}_p}(\beta)\mathbb{N}_{K/\mathbb{Q}_p}(\beta')$ et il est facile de voir que $|\alpha|_p = 0 \Leftrightarrow \alpha = 0$. Le seul point délicat est l'inégalité $|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p)$. Supposons que $|\beta|_p = \max(|\alpha|_p, |\beta|_p)$ et posons $\gamma = \frac{\alpha}{\beta}$, il suffit de montrer que :

$$|1 + \gamma|_p \leq 1 \quad \text{dès que} \quad |\gamma|_p \leq 1.$$

1. Si $K = \mathbb{Q}_p(\gamma)$. On prend $(1, \gamma, \ldots, \gamma^{n-1})$ comme base de K sur $\mathbb{Q}_p$. Soit A la matrice de la multiplication par γ. On a $|\gamma|_p = |det(A)|_p^{\frac{1}{n}}$ et $|1 + \gamma|_p = |det(I + A)|_p^{\frac{1}{n}}$.

   Lemme 38 *La suite $(\left|A^i\right|_\infty)_{i\in\mathbb{N}}$ est bornée.*

Démonstration. Sinon, on peut extraire une sous suite $(\left|A^{i_j}\right|_\infty)$ telle que $\left|A^{i_j}\right|_\infty = b_j > j$. Soit β_j le coefficient de A^{i_j} le plus grand en norme p-adique. On considère maintenant la suite :

$$B_j = \frac{A^{i_j}}{\beta_j}$$

Il est clair que $|B_j|_\infty = 1$. Comme $\mathbb{Q}_p$ est localement compact on sait par le lemme 32 qu'il existe une sous suite $(B_{j_k})_k$ qui converge vers B, appartenant à la sphère unité, pour $|.|_\infty$. De plus, on a :

$$|det(B_j)|_p < \frac{\left|det(A^{i_j})\right|_p}{j^n} = \frac{|\gamma|_p^{ni_j}}{j^n} \leq \frac{1}{j^n} \to_{j\to\infty} 0.$$

Mais comme $|B_{j_k} - B|_\infty \to 0$, on a $|det(B_{j_k}) - det(B)|_p \to 0$ donc $|det(B)|_p = 0 \iff det(B) = 0$. Il existe donc $l \in K$ non nul tel que $B(l) = 0$. On a :

$$B(\gamma^i l) = \lim_{k\to\infty} B_{j_k}(\gamma^i l) = \gamma^i \lim_{k\to\infty} B_{j_k}(l) = \gamma^i B(l) = 0 \ \ \forall\, i \in \{1, \dots, n-1\}.$$

Mais $(l, l\gamma, \dots, l\gamma^{n-1})$ est encore une base de K ce qui implique B=0 et contredit $|B|_\infty = 1$.
■

Pour terminer la démonstration on remarque que pour toute matrice $A = (a_{ij})$ on a $|det(A)|_p \leq (\max_{i,j} |a_{ij}|_p)^n = |A|_\infty^n$ en utilisant les propriétés de la valeur absolue ultramétrique.

Soit N grand: $(1+A)^N = 1 + C_N^1 A + \dots + C_N^{N-1} + A^N$.On a :

$$|1+\gamma|_p^N = \left|det(I+A)^N\right|_p^{\frac{1}{n}} \leq \left|(I+A)^N\right|_\infty \leq \max_{0\leq i\leq N}(\left|A^i\right|_\infty) \leq C$$

Donc $|1+\gamma|_p \leq C^{\frac{1}{N}} \to 1$ quand $N \to \infty$.

2. Si γ n'est pas un élément primitif on a :

$$|1+\gamma|_p = \left|\mathbb{N}_{K/\mathbb{Q}_p}(1+\gamma)\right|_p^{\frac{1}{n}} = \left|\mathbb{N}_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(1+\gamma)\right|_p^{\frac{1}{[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]}} \leq 1$$

L'existence et démontrée et comme $\mathbb{Q}_p$ est localement compact l'unicité provient du corollaire 34.

■

3.5.2 La cloture algébrique de $\mathbb{Q}_p$

On peut maintenant définir une valeur absolue ultramétrique sur $\overline{\mathbb{Q}_p}$ qui étend la valeur absolue p-adique par :

Définition 39 *Soit $\alpha \in \overline{\mathbb{Q}_p}$ de polynôme minimal $x^n + a_{n-1}x^{n-1} + \dots + a_0$ on pose :*

$$|\alpha|_p = |a_n|_p^{\frac{1}{n}}.$$

Lemme 40 *Soit α un nombre algébrique de degré n sur $\mathbb{Q}_p$ alors $\forall\, k \in \mathbb{N}$, $\exists\, N > k$ tel que α ne satisfait aucune congruence du type :*

$$a_{n_0}\alpha^{n_0} + \dots + a_1\alpha + a_0 \equiv 0 \mod p^N$$

où les a_i sont dans $\mathbb{Z}_p$ non tous divisibles par p et $n_0 < n$.

Démonstration. Sinon $\exists k \in \mathbb{N}$ tel que $\forall N > k$, $\exists n_0 < n$ et $a_0^N, \ldots, a_{n_0}^N$ dans $\mathbb{Z}_p$, non tous divisibles par p tels que :

$$a_{n_0}^N \alpha^{n_0} + \ldots + a_1^N \alpha + a_0^N \equiv_{\mathbb{Z}_p} 0 \mod p^N.$$

$\mathbb{Z}_p$ étant compact, on peut trouver une extraction Φ croissante telle que $\forall i$, $a_i^{\Phi(N)} \to_{N\to\infty} a_i \in \mathbb{Z}_p$. On a alors :

$$a_{n_0}\alpha^{n_0} + \ldots + a_1\alpha + a_0 = 0.$$

Ce qui contredit l'hypothèse car $n_0 < n$. ■

Théorème 41 *$\overline{\mathbb{Q}_p}$ n'est pas complet.*

Démonstration. Soit b_i une racine primitive p^i-ième de l'unité dans $\overline{\mathbb{Q}_p}$ et soit $a_i = \sum_{j=0}^{i} b_j p^{N_j}$ où N_j est une suite d'entiers strictement croissante et $N_0 = 0$. La suite (a_i) ainsi définie est clairement de Cauchy. On définit maintenant les N_j par récurrence.

Supposons que l'on ait défini N_j pour $j \leq i$. Posons $K = \mathbb{Q}_p(b_i)$. K est une extension de $\mathbb{Q}_p$ de degré $p^{i-1}(p-1)$ (*cf.* l'application 31). On remarque que $K = \mathbb{Q}_p(a_i)$ car sinon on peut trouver un automorphisme non-trivial σ de K qui laisse a_i fixe, puisque $K(a_i)(b_i)/K(a_i)$ est galoisienne. Mais $\sigma(a_i) = \sum_{j=0}^{i} \sigma(b_j)p^{N_j}$; notons note i_0 le plus petit entier tel que $\sigma(b_j) \neq b_j$. N_j est une suite strictement croissante et $|b_{i_0} - \sigma(b_{i_0}|_p = |(b_{i_0} - 1) + (1 - b_{i_0})|_p = p^{-\frac{1}{(p-1)p^m}} > 1/p$, pour un certain m. Donc on a $|\sigma(a_i) - a_i|_p = p^{-N_{i_0}} |b_{i_0} - \sigma(b_{i_0})|_p \neq 0$. C'est absurde.

Ensuite, par le lemme 40, il existe $N_{i+1} > N_i$ tel que a_i ne satisfait aucune congruence du type :

$$\alpha_n a_i^n + \cdots + \alpha_1 a_i + \alpha_0 \equiv 0 \mod p^{N_{i+1}}$$

pour $n < (p-1)p^{i-1}$ et $\alpha_j \in \mathbb{Z}_p$ non tous divisibles par p.

Supposons que $a \in \overline{\mathbb{Q}_p}$ soit la limite de la suite (a_i). Alors si a est de degré n, a satisfait une équation polynômiale, de degré n, à coefficient dans $\mathbb{Q}_p$. En multipliant par la bonne puissance de p on peut supposer que a satisfait l'équation

$$\alpha_n a^n + \ldots + \alpha_1 a + \alpha_0 = 0,$$

où les α_i sont dans $\mathbb{Z}_p$ non tous divisibles par p. Choisissons i tel que $n < (p-1)p^{i-1}$. Comme $a \equiv_{\mathbb{Z}_p} a_i \mod p^{N_{i+1}}$, on a :

$$\alpha_n a_i^n + \cdots + \alpha_1 a_i + \alpha_0 \equiv 0 \mod p^{N_{i+1}}.$$

Contradiction. ■

3.5.3 Construction de $\mathbb{C}_p$

On construit $\mathbb{C}_p$ en complétant $\mathbb{Q}_p$ pour $|\cdot|_p$, de la même facon qu'on a construit $\mathbb{Q}_p$ en complétant $\mathbb{Q}$.

On étend la valeur absolue p-adique de $\overline{\mathbb{Q}_p}$ sur $\mathbb{C}_p$ en posant pour $x \in \mathbb{C}_p$, $|x|_p = \lim_{i\to\infty} |x_i|_p$ où (x_i) est une suite de Cauchy d'éléments de $\overline{\mathbb{Q}_p}$ qui est dans la classe d'équivalence de x.

Lemme 42 *Soit $Q(X) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$, $\in \mathbb{C}_p[X]$. Soit $C_0 = \max_{0\leq i\leq n-1}(|b_i|_p)$. Alors il existe une constante C_1 qui ne dépend que de C_0 telle que pour toute racine β de Q, $|\beta|_p < C_1$*

Démonstration. On pose $M_\beta = \max(1, |\beta|_p)$, on a $\beta^n = -b_{n-1}\beta^{n-1} - \ldots - b_0$ et donc :

$$|\beta|_p^n \leq \max_{0\leq i\leq n-1}(\left|b_i\beta^i\right|_p) \leq C_0 \max_{0\leq i\leq n-1}(\left|\beta^i\right|_p) \leq C_0(M_\beta)^{n-1}$$

d'où $\frac{|\beta|_p^n}{(M_\beta)^{n-1}} \leq C_0$. On pose $C_1 = \max(C_0, (C_0)^{\frac{1}{n}})$ et on a $|\beta|_p \leq C_1$. ■

Théorème 43 *$\mathbb{C}_p$ est algébriquement clos.*

Démonstration. Soit $P(X) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{C}_p[X]$. Pour $0 \leq i \leq n-1$ soit $(a_{ij})_j$ une suite d'éléments de $\overline{\mathbb{Q}_p}$ qui converge vers a_i. Soit $P_j(X) = X^n + a_{n-1,j}X^{n-1} + \ldots + a_{1,j}X + a_{0,j}$. Soit r_{ij} les racines de P_j ($i = 1, 2, \ldots, n$). On veut trouver $i_j \in \{1, \ldots, n\}$ tels que la suite $(r_{i_j,j})_j$ soit de Cauchy. On construit $(r_{i_j,j})_j$ par récurrence. Supposons que l'on ait $r_{i_j,j}$ et posons $\delta_j = \max_i(|a_{i,j} - a_{i,j+1}|_p)$ et $A_j = \max(1, \left|r_{i_j,j}\right|_p^n)$. Par le lemme 42 il est clair qu'il existe une constante A telle que $A_j \leq A \quad \forall\, j$. Alors,

$$\prod_i \left|r_{i_j,j} - r_{i,j+1}\right|_p = \left|P_{j+1}(r_{i_j,j})\right|_p = \left|P_{j+1}(r_{i_j,j}) - P_j(r_{i_j,j})\right|_p \leq \delta_j A$$

Il y a forcément au moins l'un des $\left|r_{i_j,j} - r_{i,j+1}\right|_p$ qui est majoré par $(\delta_j A)^{\frac{1}{n}}$. Soit $r_{i_{j+1},j+1}$ un tel $r_{i,j+1}$. Ainsi définie, la suite $(r_{i_j,j})_j$ est de Cauchy car $\delta_j \to 0$. On pose $r = \lim_{j\to\infty} r_{i_j,j} \in \mathbb{C}_p$ et on a :

$$P(r) = \lim_{j\to\infty} P(r_{i_j,j}) = \lim_{j\to\infty} P_j(r_{i_j,j}) = 0$$

■

3.6 Intégration abstraite dans $\mathbb{Q}_p$

Définition 44 *On appelle intervalle (de $\mathbb{Q}_p$) tout ensemble du type $a + p^N\mathbb{Z}_p$, où $a \in \mathbb{Q}_p$ et $N \in \mathbb{Z}$.*

Lemme 45 *Deux boules de même rayon, dans $\mathbb{Q}_p$, sont soit disjointes soit égales.*

Démonstration. On fait la démonstration pour deux boules ouvertes B_1 et B_2 de rayon r et de centres respectifs a_1 et a_2. Si, par exemple, $x \in B_1$ et $a \in B_1 \cap B_2$, alors $|a_2 - x|_p = |(a_2 - a) + (a - x)|_p \leq \max\left\{|(a_2 - a)|_p, |(a - x)|_p\right\} < r$. ■

Proposition 46 *Soit $X \subset \mathbb{Q}_p$. X est compact et ouvert si et seulement s'il est union finie disjointe d'intervalles.*

Démonstration. Pour montrer qu'une union finie disjointe d'intervalles est compacte et ouverte, il suffit de le montrer pour $\mathbb{Z}_p$. $\mathbb{Z}_p$ est ouvert, grâce au lemme précédent, car pour tout $x \in \mathbb{Z}_p$, la boule ouverte de centre x et de rayon 1 est incluse dans $\mathbb{Z}_p$. On prouve la compacité séquentiellement en remarquant que

$$\mathbb{Z}_p = \left\{\sum_{n=0}^{\infty} a_n p^n,\ (a_n) \in [\![0,\, p-1]\!]^{\mathbb{N}}\right\} \ :$$

se donner une suite (x_i) d'entiers p-adiques, c'est se donner une famille $(a_n(i)) \in [\![0,\, p-1]\!]^{\mathbb{N}}$, indexée par $i \in \mathbb{N}$. Le processus diagonal permet alors de trouver ϕ telle que pour tous $j \geq i$ et $n \leq i$, $a_n(\phi(i)) = a_n(\phi(j))$. La suite $(x_{\phi(i)})$ est convergente.

Dans l'autre sens, il suffit de voir que nos intervalles constituent des bases de voisinage et qu'une union finie d'intervalles est une union finie disjointe d'intervalles : pour cela on redécoupe les intervalles selon le diamètre minimal des intervalles initiaux. Un intervalle peut toujours se découper ainsi et comme deux boules distinctes sont disjointes, c'est gagné. ■

On retiendra en particulier :

Proposition 47 *$\mathbb{Z}_p$ et $\mathbb{Z}_p^\times$ sont compacts.*

On en déduit :

Proposition 48 *$\mathbb{Q}_p$ est localement compact.*

Démonstration. En effet, si $x \in \mathbb{Q}_p$, $X + \mathbb{Z}_p = \left\{ y \in \mathbb{Q}_p \ / \ |x-y|_p \leq 1 \right\}$ est un voisinage compact de x. ■

Définition 49 (Distributions et mesures) *Une distribution p-adique μ sur $X \subset \mathbb{Q}_p$ est une fonction définie sur l'ensemble $co(X)$ des ouverts compacts inclus dans X, à valeurs dans $\mathbb{C}_p$, telle que si $U, U_1, \ldots, U_n \in co(X)$ et U est la réunion disjointe des U_i, alors $\mu(U) = \sum_{i \leq n} \mu(U_i)$.*

Une distribution μ sur X est une mesure si elle bornée, c'est-à-dire si $\exists\, M \in \mathbb{R} \ / \ \forall\, U \in co(X),\ |\mu(U)|_p \leq M$.

Théorème-Définition 50 *Soit $X \subset \mathbb{Z}_p$ un ouvert compact. Soient μ une mesure p-adique sur X et $f : X \to \mathbb{C}_p$ une fonction continue. Alors, la somme de Riemann associée au pointage $(x_{a,M})$ ($x_{a,M} \in a + p^M\mathbb{Z}_p$), prise au rang N*

$$S_N = S_{(x_{a,M}),\,N} = \sum_{\substack{0 \leq a < p^N \\ a + p^N\mathbb{Z}_p \subset X}} f(x_{a,N})\mu(a + p^N\mathbb{Z}_p)$$

converge dans $\mathbb{C}_p$ quand $N \to \infty$ vers une limite qui ne dépend pas du pointage.

Cette limite est notée $\int f\mu$.

Démonstration. Notons B un majorant de μ. Comme f est continue et X est compact, f est uniformément continue. On va utiliser le critère de Cauchy pour montrer que (S_N) converge.

Prenons tout d'abord $N < M$ assez grand, de telle façon qu'un intervalle $a + p^N\mathbb{Z}_p$ soit inclus dans X ou disjoint de X (on utilise le fait que X est union finie d'intervalles).

Grâce à l'additivité de μ, on peut homogéniser la différence $S_N - S_M$. Vu que $M > N$, S_N peut s'écrire :

$$S_N = \sum_{\substack{0 \leq a < p^M \\ a + p^M\mathbb{Z}_p \subset X}} f(x_{\{a\}_N,N})\mu(a + p^M\mathbb{Z}_p),$$

où $\{a\}_N$ désigne l'entier compris entre 0 et $p^N - 1$ et distant de a de moins de p^N.

Dès lors, si l'on prend N tel que, si $|x-y|_p \leq p^{-N}$, alors $|f(x) - f(y)|_p \leq \varepsilon$, on obtient que

$$|S_N - S_M|_p \leq \max_{\substack{0 \leq a < p^M \\ a + p^M\mathbb{Z}_p \subset X}} \left|f(x_{\{a\}_N,N}) - f(x_{a,M})\right|_p B \leq \varepsilon B.$$

On voit donc que S_N converge et que si l'on change de pointage, sans même devoir homogénéiser la différence, par les mêmes arguments de valeur absolue hypermétrique et d'uniforme continuité, les deux sommes ont la même limite. ■

Théorème 51 *Soit $X \subset \mathbb{Z}_p$ un ouvert compact. Soient μ une mesure p-adique sur X bornée par A et $f : X \to \mathbb{C}_p$ une fonction continue bornée par M. Alors,*

$$\left| \int_X f\mu \right|_p \leq AM.$$

Démonstration. C'est évident. ■

Exemple : La mesure la plus évidente sur $\mathbb{Q}_p$ est la mesure μ_{haar}, dite mesure de Haar, telle que $\mu\left(a + p^N\mathbb{Z}_p\right) := 1/p^N$. Cependant, elle n'est pas bornée.

Il n'est pas évident *a priori* de construire des mesures bornées. C'est l'objet du paragraphe suivant.

3.7 Construction de mesures p-adiques

3.7.1 Distributions de Bernoulli

On va dans cette partie utiliser les polynômes de Bernoulli défini dans le paragrahe 1.1. On rappelle que

$$B_k(x) = \sum_{i=0}^{k} \mathrm{C}_k^i B_i x^{k-i}$$

et $B_0(x) = 1$, $B_1(x) = x - 1/2$.

Lemme 52 *Soit $X \subset \mathbb{Q}_p$. Une application μ définie sur l'ensemble des intervalles contenus dans X à valeurs dans $\mathbb{Q}_p$ et qui vérifie*

$$\mu(a + p^N\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^N + p^{N+1}\mathbb{Z}_p)$$

définit une unique distribution par additivité.

Démonstration. Tout ce qu'on doit vérifier est la légitimité de la définition.

Prenons U réunion finie d'intervalles inclue dans X. On écrit X de deux façons : $U = \bigcup I_i = \bigcup I'_j$, où les unions sont finies et disjointes. En redécoupant U selon une partition plus fine que (I_i) (on considère l'intervalle de diamètre d le plus petit parmi les intervalles des *deux* partitions et on coupe tous les I_i en intervalles I''_k de ce diamètre d), c'est gagné. En effet, grâce à l'additivité (utilisée autant de fois que nécessaire), on a $\sum \mu(I_i) = \sum \mu(I''_k)$; reste à calculer alors $\sum \mu(I'_j)$. On peut faire le même découpage que pour les I_i en intervalles I'''_l de diamètre d, mais cette fois pour les I'_j. Vérifions que I''_k et les I'''_l forment une même partition. On se sert du lemme 45 : si $x \in I''_k \subset U$, il existe l tel que $x \in I'''_l$ et donc $I''_k = I'''_l$. Comme le raisonnement est symétrique, le résultat est vrai et on peut écrire, $\sum \mu(I'_j) = \sum \mu(I'''_l) = \sum \mu(I''_k) = \sum \mu(I_i)$. ■

Compte tenu de la propositon précédente, on peut définir la famille de distributions suivantes :

Proposition-Définition 53 *L'application $\mu_{B,k}$ qui à un intervalle $a+p^N\mathbb{Z}_p \subset \mathbb{Z}_p$ (cela implique $a \in \mathbb{Z}_p$ et $N \geq 0$), où a est choisi entre 0 et $p^N - 1$ (c'est toujours possible de faire un tel, on considérant si nécessaire $\{a\}_N$),*

$$\mu_{B,k}\left(a + p^N\mathbb{Z}_p\right) = p^{N(k-1)} B_k\left(\frac{a}{p^N}\right)$$

définit une distribution sur $\mathbb{Z}_p$.

Dans toute la suite, sauf mention contraire, lorsqu'on parlera d'un intervalle $a + p^N\mathbb{Z}_p$, on choisira $N \in \mathbb{N}$ et a entre 0 et $p^N - 1$.

Démonstration. Nous devons montrer

$$\mu_{B,k}(a + p^N\mathbb{Z}_p) =^? \sum_{b=0}^{p-1} \mu_{B,k}(a + bp^{N-1} + p^{N-1}\mathbb{Z}_p),$$

ce qui se réécrit, après avoir posé $\alpha = \frac{a}{p^{N+1}}$,

$$B_k(p\alpha) =^? p^{k-1} \sum_{b=0}^{p-1} B_k\left(\alpha + \frac{b}{p}\right).$$

Or, par définition, le membre de droite est le coefficient, multiplié par $k!$, de t^k dans

$$p^{k-1} \sum_{b=0}^{p-1} \frac{te^{(\alpha+b/p)t}}{e^t - 1} = \frac{p^{k-1}te^{\alpha t}}{e^t - 1} \sum_{b=0}^{p-1} e^{bt/p},$$

c'est-à-dire

$$\frac{p^{k-1}te^{\alpha t}}{e^t - 1} \frac{e^t - 1}{e^{t/p} - 1} = p^k \frac{(t/p)e^{(t/p)p\alpha}}{e^{(t/p)} - 1} = p^k \frac{B_k(p\alpha)}{p^k}.$$

■

3.7.2 Mesures de Bernoulli

Les distributions de Bernoulli dont on dispose ne sont pas des mesures et il va falloir les transformer.

Lemme 54 *Si μ est une distribution (resp. une mesure) sur X et $\alpha \in \mathbb{Z}_p^\times = \left\{x \in \mathbb{Q}_p \ / \ |x|_p = 1\right\}$, alors $\mu' : U \mapsto \mu(\alpha U)$ est une distribution (resp. une mesure).*

Démonstration. La seule chose à vérifier est que $\alpha\left(a + p^N\mathbb{Z}_p\right)$ est encore un intervalle, ce qui est vrai : c'est $\alpha a + p^N\mathbb{Z}_p$. ■

Définition 55 *Soient $\alpha \in \mathbb{N}$ un entier différent de 1 non-divisible par p et $k \in \mathbb{N}$. On définit la distribution $\mu_{k,\alpha}$ par*

$$\mu_{k,\alpha}(U) = \mu_{B,k}(U) - \alpha^{-k}\mu_{B,k}(\alpha U).$$

Proposition 56 *$\mu_{1,\alpha}$ est une mesure. Plus précisément, pour tout ouvert compact $U \subset \mathbb{Z}_p$, $|\mu_{1,\alpha}(U)|_p \leq 1$.*

Démonstration. On calcule

$$\begin{aligned}
\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) &= \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha}\left(\frac{\{\alpha a\}_N}{p^N} - \frac{1}{2}\right) \\
&= \frac{(1/\alpha) - 1}{2} + \frac{a}{p^N} - \frac{1}{\alpha}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right) \\
&\quad \text{(où } [\cdot] \text{ représente la fonction partie entière)} \\
&= \frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{(1/\alpha) - 1}{2}.
\end{aligned}$$

En effet, α et a sont des entiers positifs et si $\alpha a = \sum_{i=0}^{m} a_i p^i$ (décomposition en base p), on a : $\{\alpha a\}_N = \sum_{i=0}^{N-1} a_i p^i = \alpha a - \sum_{i=N}^{m} a_i p^i$. Or,

$$\frac{\alpha a}{p^N} = \underbrace{\sum_{i=0}^{N-1} a_i p^{i-N}}_{\leq \frac{p^{N-1}}{p^N} < 1} + \underbrace{\sum_{i=N}^{m} a_i p^{i-N}}_{\in \mathbb{N}}$$

Donc on a bien

$$\boldsymbol{\{\alpha a\}_N = \alpha a - p^N \left[\frac{\alpha a}{p^N}\right].}$$

Ensuite, on peut remarquer que $(\alpha^{-1} - 1)/2 \in \mathbb{Z}_p$, vu que $\alpha^{-1} \in \mathbb{Z}_p$ et $1/2$ aussi si $p \neq 2$. Si $p = 2$, alors $\left|\alpha^{-1} - 1\right|_p \leq 1/2$, et c'est bon aussi. Finalement, on voit que $\mu_{1,\alpha}(a + p^N\mathbb{Z}_p) \in \mathbb{Z}_p$. Or, tout ouvert compact est union disjointe d'intervalles ; la norme p-adique étant ultramétrique, on a bien que pour tout U ouvert compact de $\mathbb{Z}_p$, $|\mu_{1,\alpha}(U)|_p \leq 1$. ■

Prouvons dès maintenant le

Lemme 57 *Si a, b, c, $d \in \mathbb{Z}_p$, $a \equiv_{\mathbb{Z}_p} b \mod p^{N+1}$, $c \equiv_{\mathbb{Z}_p} d \mod p^{N+1}$, alors $ac \equiv_{\mathbb{Z}_p} bd \mod p^{N+1}$.*
Si a, $b \in \mathbb{Z}_p^\times$ et si $a \equiv_{\mathbb{Z}_p} b \mod p^N$, alors $a^{-1} \equiv_{\mathbb{Z}_p} b^{-1} \mod p^N$.

Démonstration. Pour la première partie du lemme, cela vient du fait que $ac - bd = (a - b)c + (c - d)b$.
Pour la seconde, on multiplie la congruence $a \equiv_{\mathbb{Z}_p} b \mod p^N$ par $\frac{1}{ab}$. ■

Théorème 58 *En notant d_k le plus petit dénominateur commun des coefficiens de $B_k(X)$, on a :*

$$d_k \mu_{k,\alpha}\left(a + p^N\mathbb{Z}_p\right) \equiv_{\mathbb{Z}_p} d_k k a^{k-1} \mu_{1,\alpha}\left(a + p^N\mathbb{Z}_p\right) \mod p^N$$

Démonstration. On a vu plus haut que le polynôme B_k commence ainsi : $B_k(x) = B_0 x^k + kB_1 x^{k-1} + \cdots = x^k - (k/2)x^{k-1} + \ldots$. Par ailleurs, $d_k B_k$ est un polynôme à coefficients entiers ; par conséquent, lorsqu'on l'évalue en $\frac{a}{p^N}$, les termes correspondant aux x^i, où $i < k-1$, combinés au facteur $p^{N(k-1)}$ seront des facteurs de p^N, et à ce titre négligeables. Algébriquement,

$$\begin{aligned}
d_k \mu_{k,\alpha}\left(a + p^N\mathbb{Z}_p\right) &\equiv_{\mathbb{Z}_p} d_k p^{N(k-1)} \left(\frac{a^k}{p^{Nk}} - \frac{k}{2}\frac{a^{k-1}}{p^{N(k-1)}} - \alpha^{-k}\left(\frac{\left(\{\alpha a\}_N\right)^k}{p^{Nk}} - \frac{k}{2}\frac{\left(\{\alpha a\}_N\right)^{k-1}}{p^{N(k-1)}}\right)\right) \mod p^N \\
&= d_k \left(\frac{a^k}{p^N} - \alpha^{-k} p^{N(k-1)}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^k - \frac{k}{2}\left(a^{k-1} - \alpha^{-k} p^{N(k-1)}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^{k-1}\right)\right) \\
&\equiv_{\mathbb{Z}_p} d_k \left(\frac{a^k}{p^N} - \alpha^{-k}\left(\frac{(\alpha a)^k}{p^N} - k(\alpha a)^{k-1}\left[\frac{\alpha a}{p^N}\right]\right) - \frac{k}{2}\left(a^{k-1} - \alpha^{-k}(\alpha a)^{k-1}\right)\right) \mod p^N \\
&= d_k k a^{k-1}\left(\frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{1/\alpha - 1}{2}\right) \\
&= d_k k a^{k-1} \mu_{1,\alpha}(a + p^N\mathbb{Z}_p),
\end{aligned}$$

ce qu'on voulait. ■

Corollaire 59 *Pour tout $k \in \mathbb{N}^\times$ et $\alpha \in \mathbb{N} \setminus (p\mathbb{N} \cup \{1\})$, $\mu_{k,\alpha}$ est une mesure sur $\mathbb{Z}_p$.*

Démonstration. D'après ce qui précède, on a $\mu_{k,\alpha}(a+p^N\mathbb{Z}_p) = ka^{k-1}\mu_{1,\alpha}(a+p^N\mathbb{Z}_p) + \frac{bp^N}{d_k}$, où $b \in \mathbb{Z}_p$. Par conséquent,

$$\left|\mu_{k,\alpha}(a+p^N\mathbb{Z}_p)\right|_p \leq max\{\underbrace{\left|\mu_{1,\alpha}(a+p^N\mathbb{Z}_p)\right|_p}_{\leq 1}, \underbrace{\left|\frac{p^N}{d_k}\right|_p}_{\leq \left|\frac{1}{d_k}\right|_p}\} \leq B.$$

■

4 Fonctions puissance et logarithme dans $\mathbb{C}_p$

4.1 Petit détour chez les fonctions puissance

Dans cette partie, on va voir qu'on a plein de façons d'interpoler la fonction puissance $\begin{array}{c}\mathbb{N} \to \mathbb{Z}_p \\ k \mapsto x^k\end{array}$. Malheureusement, si on veut bien l'interpoler, on doit réduire l'espace où vit x. Si, très généralement, on prend $x \in \mathbb{Z}_p$, on obtient des fonctions "puissance" très bancales, qui, tous comptes faits, n'en sont pas.

D'abord un petit lemme :

Lemme 60 *(1) Soient $x \in 1+p\mathbb{Z}_p$ et $k,\ k' \in \mathbb{N}$ tels que $k \equiv_{\mathbb{Z}} k'p^N$. Alors, $x^k \equiv_{\mathbb{Z}_P} x^{k'} \mod p^{N+1}$.*

(2) Plus généralement, si $x \in \mathbb{Z}_p^\times$ et $k,\ k' \in \mathbb{N}$ tels que $k \equiv_{\mathbb{Z}} k' \mod (p-1)p^N$. Alors, $x^k \equiv_{\mathbb{Z}_P} x^{k'} \mod p^{N+1}$.

Démonstration. (1) On écrit $k' = k + Mp^N$. Calculons $x^{p^N M} - 1 = (1+ap)^{p^N M} - 1$, où $a \in \mathbb{Z}_p$:

$$(1+ap)^{p^N M} - 1 = p^N Map + \frac{p^N M(p^N M-1)}{2}(ap)^2 + \cdots + (ap)^{p^N M}.$$

Pour que le dénominateur de $C^k_{p^N M}$ puisse manger p^l ($l \geq 1$) au premier facteur p^N, il faut $v_p(k!) \geq l$ *ie* que k soit supérieur à pl ; mais, dans ce cas, le facteur p^{pl} aura compensé la perte, en apportant $p^{pl-1} \geq p^l$ comme facteur supplémentaire. Par conséquent, la puissance initiale (du premier terme) de p ne sera pas réduite dans les termes suivants : $(1+ap)^{p^N M} - 1 = p^{N+1}b$, où $b \in \mathbb{Z}_p$

Donc $\left|x^{p^N M} - 1\right|_p \leq p^{-(N+1)}$ et $x^k \equiv_{\mathbb{Z}_p} x^{k'} \mod p^{N+1}$.

(2) On écrit $k' = k + M(p-1)p^N$. On a $x \equiv_{\mathbb{Z}_p} \{x\}_1 \mod p$, donc $x^{p-1} \equiv_{\mathbb{Z}_p} \{x\}_1^{p-1} \equiv_{\mathbb{Z}_p} 1 \mod p$, car $\{x\}_1 \neq 0$. Donc la première partie du lemme s'applique à x^{p-1} et $\left|x^k - x^{k'}\right|_p = \left|(x^{p-1})^{Mp^N} - 1\right|_p \leq p^{-(N+1)}$. ■

4.1.1 La bonne interpolation de la fonction puissance sur $1+p\mathbb{Z}_p$

Continuons ce chapitre par la présentation de la star de l'élévation à la puissance dans $\mathbb{Z}_p$:

Proposition-Définition 61 *Soit $x \in 1+p\mathbb{Z}_p$.*

Alors, la fonction $\begin{array}{c}\mathbb{N} \to 1+p\mathbb{Z}_p \\ k \mapsto x^k\end{array}$ *est uniformément continue. On peut ainsi définir, par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$, une fonction uniformément continue* $\begin{array}{c}\mathbb{Z}_p \to 1+p\mathbb{Z}_p \\ s \mapsto x^s\end{array}$.

En fait on a mieux puisque $\begin{array}{c}(1+p\mathbb{Z}_p)\times\mathbb{Z}_p \to 1+p\mathbb{Z}_p \\ (x,\, s) \mapsto x^s\end{array}$ *est uniformément continue.*

On a:

$$\forall\, x \in 1+p\mathbb{Z}_p,\, \forall\, s,\, s' \in \mathbb{Z}_p,\, x^{s+s'} = x^s x^{s'}\ ;$$

$$\forall\, x \in 1+p\mathbb{Z}_p,\, \forall\, s,\, s' \in \mathbb{Z}_p,\, x^{ss'} = (x^s)^{s'}\ ;$$

$$\forall\, x \in 1+p\mathbb{Z}_p,\, x^0 = 1.$$

Enfin, notons qu'on peut écrire, pour tous $x \in 1+p\mathbb{Z}_p$ et $s \in \mathbb{Z}_p$:

$$x^s = \sum_{n=0}^{\infty} \mathrm{C}_s^n (x-1)^n,$$

où l'on note

$$\mathrm{C}_s^n = \frac{\prod_{i=0}^{n-1}(s-i)}{n!} \in \mathbb{Z}_p.$$

Démonstration. L'uniforme continuité découle du lemme précédent. Les fonctions introduites sont bien définies car d'une part $B(1,\,1)^\circ$ est stable par multiplication et d'autre part, $1+p\mathbb{Z}_p$ est fermé.

Soient $s,\, s' \in \mathbb{Z}_p$ et $(k_n),\, (k'_n)$ deux suites d'entiers convergeant respectivement vers s et s'. On a

$$x^{s+s'} = \lim_{n\to\infty} x^{k_n+k'_n} = \lim_{n\to\infty} x^{k_n} x^{k'_n} = \lim_{n\to\infty} x^{k_n} \lim_{n\to\infty} x^{k'_n} = x^s x^{s'}.$$

On a aussi $x^{ss'} = \lim_{n\to\infty} x^{k_n k'_n} = \lim_{n\to\infty} (x^{k_n})^{k'_n}$. Évaluons

$$\left|(x^{k_n})^{k'_n} - (x^s)^{s'}\right|_p = \left|\underbrace{(x^{k_n})^{k'_n} - (x^s)^{k'_n}}_{A_n} + \underbrace{((x^s)^{k'_n} - (x^s)^{s'}}_{B_n}\right|_p .$$

On a $|A_n|_p = \left|(x^{k_n} - x^s)\sum_{i=0}^{k'_n-1}(x^{k_n})^i (x^s)^{k'_n-1-i}\right|_p \leq \left|x^{k_n} - x^s\right|_p$, qui tend vers 0 quand $n \to \infty$. Par ailleurs, par défintion, on a aussi $|B_n|_p \to 0$ quand $n \to \infty$.

Par conséquent, $x^0 = x^0 x^0 \neq 0$ donc $x^0 = 1$.

Vérifions que f : $\begin{array}{c}(1+p\mathbb{Z}_p)\times\mathbb{Z}_p \to 1+p\mathbb{Z}_p \\ (x,\, s) \mapsto \sum_{n=0}^{\infty} \mathrm{C}_s^n (x-1)^n\end{array}$ est une fonction bien définie, uniformément continue et qui coïncide, à x fixé, sur $\mathbb{N}$ avec la fonction précédente. On aura alors l'égalité voulue, le fait que l'ensemble d'arrivée est le bon et une propriété de continuité des deux variables. La coïncidence, à x fixé, des deux fonctions sur $\mathbb{N}$ est la formule du binôme. Fixons $k \geq 0$. La fonction qui à $n \in \mathbb{N}$ associe C_n^k est polynômiale donc continue à valeurs dans $\mathbb{Z} \subset \mathbb{Z}_p$. Donc, si $s \in \mathbb{Z}_p$ et si $k_n \to s$, on a $\mathrm{C}_{k_n}^k \to \mathrm{C}_s^k$. Donc la fonction qui à s associe C_s^k est à valeurs dans $\mathbb{Z}_p$, polynômiale donc uniformément continue. Comme $x \mapsto (x-1)^k$ est aussi uniformément continue, pour tout $n \in \mathbb{N}$, $(x,\, s) \mapsto \mathrm{C}_s^k (x-1)^k$ est uniformément continue. Il nous suffit maintenant de vérifier qu'il y a convergence normale : c'est clair puisque $\left|\mathrm{C}_s^k (x-1)^k\right|_p \leq p^k$. ■

4.1.2 Les mauvaises interpolations de la fonction puissance sur $\mathbb{Z}_p$

Le lemme 60 se traduit par l'uniforme continuité, pour tous $s_0 \in [\![0,\, p-2]\!]$ et $x \in \mathbb{Z}_p^\times$ de la fonction

$$f_{x,\,s_0} \;:\; \begin{array}{l} \mathbb{N} \to \mathbb{Z}_p \\ k \mapsto x^{s_0+(p-1)k} \end{array}.$$

On peut donc l'interpoler en une fonction uniformément continue définie sur $\mathbb{Z}_p$, que l'on appelera encore $f_{x,\,s_0}$. On obtient $p-1$ interpolations continues de la fonction puissance.

On fera attention aux faits suivants, qui distinguent les propriétés de ces fonctions de la fonction interpolée :

Fait 62 *Soit $x \in \mathbb{Z}_p^\times$. Alors, $f_{x,\,s_0}\left(-\frac{s_0}{p-1}\right) = \alpha_{\{x^{s_0}\}_1}$.*

Cela signifie que l'on n'a pas toujours "$x^0 = 1$". En particulier, on a :

Fait 63 *Soient $x \in \mathbb{Z}_p^\times$ et $s_0 \in [\![0,\, p-2]\!]$ tels que $x^{s_0} \not\equiv_{\mathbb{Z}_p} 1 \mod p$. Alors $\exists\, s,\, s' \in \mathbb{Z}_p$, $f_{x,\,s_0}\left(\frac{s+s'-s_0}{p-1}\right) \neq f_{x,\,s_0}\left(\frac{s-s_0}{p-1}\right) f_{x,\,s_0}\left(\frac{s'-s_0}{p-1}\right)$.*

Ainsi, il existe des x, des s_0 et des $s,\, s'$ tels que "$x^{s+s'}$"$\neq$"x^s" "$x^{s'}$".

Fait 64 (Cas particulier de $f_{x,\,0}$) *Soient $x \in \mathbb{Z}_p^\times$ et $s,\, s' \in \mathbb{Z}_p$. Alors,*

(1) $f_{x,\,0}(0) = 1$.

(2) $f_{x,\,0}\left(\frac{s+s'}{p-1}\right) = f_{x,\,0}\left(\frac{s}{p-1}\right) f_{x,\,0}\left(\frac{s'}{p-1}\right)$.

(3) $f_{x,\,0}\left(\frac{ss'}{p-1}\right) = f_{f_{x,0}\left(\frac{s}{p-1}\right),\,0}\left(\frac{s'}{p-1}\right)$.

Pour cette interpolation, *(1)* signifie que "x^0"$= 1$; *(2)* signifie que "$x^{s+s'}$"="x^s" "$x^{s'}$" ; *(3)* signfie que "$x^{ss'}$"="$(x^s)^{s'}$".

Démonstration du fait 62. Il nous suffit d'étudier la suite $x_n = x^{s_0+(p-1)s_0\sum_{i=0}^{n-1} p^i}$. En effet, l'exposant de x_n vaut $s_0 + s_0(p^n-1) = p^n s_0$, qui tend vers 0.

Deux remarques. La première est que si l'on note l la limite de x_n, on a donc $l^p = l$. La deuxième est qu'on a, pour tout $n \in \mathbb{N}$, on a $x_n \equiv_{\mathbb{Z}_p} x^{s_0} \mod p$. En effet, $x_{n+1} = (x_n)^p \equiv_{\mathbb{Z}_p} x_n \mod p$.

Ainsi, l est tel que $l^p = l$ et $l \equiv_{\mathbb{Z}_p} x^{s_0} \mod p$: l est le $\{x^{s_0}\}_1$-ième représentant de Teichmüller. ■

Démonstration du fait 64.

(1) C'est direct puisque $x^{s_0} = 1$.

(2) Là aussi, c'est facile, il suffit de prendre deux suites (k_n) et (k'_n) tendant vers s et s'.

(3) D'après le (2), pour tous $k \in \mathbb{N}$, $x \in \mathbb{Z}_p^\times$ et $s \in \mathbb{Z}_p$, on a $f_{x,\,0}\left(k_n \frac{s}{p-1}\right) = \left(f_{x,\,0}\left(\frac{s}{p-1}\right)\right)^{k_n}$. En faisant tendre k_n vers s', comme $f_{x,\,0}\left(k_n \frac{s}{p-1}\right) \in 1 + p\mathbb{Z}_p$ et comme les fonctions sont continues, on peut écrire : $f_{x,\,0}\left(\frac{ss'}{p-1}\right) = \left(f_{x,\,0}\left(k_n \frac{s}{p-1}\right)\right)^{s'}$.

Il nous reste donc plus qu'à montrer que si $y \in 1 + p\mathbb{Z}_p$ et $t \in \mathbb{Z}_p$, alors $y^t = f_{y,\,0}\left(\frac{t}{p-1}\right)$. Soit k_n une suite d'entiers positifs tendant vers $-t$. Alors, $k_n \sum_{i=0}^{n} p^i$ tend vers $\frac{t}{p-1}$ et donc

$y^{(p-1)k_n \sum_{i=0}^{n} p^i}$ tend vers $f_{y,\,0}\left(\frac{t}{p-1}\right)$. Cependant, vu sous un autre angle, $y^{(p-1)k_n \sum_{i=0}^{n} p^i} = y^{k_n p^{n+1}} y^{-k_n}$, qui tend vers y^t.

■

En conclusion de cette étude, on se souviendra que l'on s'autorisera à écrire x^s seulement, dans un premier temps, si $x \in 1 + p\mathbb{Z}_p$ et si $s \in \mathbb{Z}_p$.

Les fonctions $f_{x,\,s_0}$ sont à éviter, surtout si $s_0 \neq 0$. Dans tous les cas, on écrira jamais $f_{x,\,s_0}(s) = x^{s_0+(p-1)s}$ sans prendre la précaution de décomposer l'exposant selon s_0 et $p-1$.

4.1.3 Extension de la bonne fonction puissance à $\mathbb{B}_p$

On pose $\mathbb{B}_p = B_{\mathbb{C}_p}(1,\,1)^\circ$.

On a vu précédemment qu'on pouvait interpoler très efficacement la fonction $x \mapsto x^k$ quand $x \in 1 + p\mathbb{Z}_p$. En fait, on peut faire plus général en prenant $x \in \mathbb{B}_p$.

Proposition 65 *La fonction*

$$\begin{aligned} \mathbb{B}_p \times \mathbb{Z}_p &\to \mathbb{B}_p \\ (x,\,s) &\mapsto x^s = \sum_{n=0}^{\infty} \mathrm{C}_s^n (x-1)^n \end{aligned}$$

est continue et interpole la fonction puissance définie sur $\mathbb{B}_p \times \mathbb{N}$.

Elle vérifie :

$$\forall\, x \in \mathbb{B}_p,\, \forall\, s,\, s' \in \mathbb{Z}_p,\, x^{s+s'} = x^s x^{s'}\ ;$$

$$\forall\, x \in \mathbb{B}_p,\, \forall\, s,\, s' \in \mathbb{Z}_p,\, x^{ss'} = (x^s)^{s'}\ ;$$

$$\forall\, x \in \mathbb{B}_p,\, x^0 = 1.$$

Démonstration. La démonstration se fait comme pour la proposition-définition 61, en montrant que la série est normalement convergente sur les boules $B(1,\,r)^\circ$ où $r < 1$ puis en utilisant la densité de $\mathbb{N}$ dans $\mathbb{Z}_p$. ■

4.2 Petit détour par la fonction logarithme

Maintenant définie(s) la(les) fonction(s) puissance, il est légitime de se demander si on peut construire une fonction logarithme pour les nombres p-adiques. On a vu que le point de vue le plus fertile était le point de vue sériel. C'est ce point de vue que l'on va ici encore adopter.

Pour démontrer la propriété fondamentale du logarithme, on va se servir de la théorie des identités formelles, qu'on présente dès maintenant.

4.2.1 Identités formelles

Définition 66 (Séries formelles) *Soit A un anneau. On appelle série formelle sur A un élément quelconque de $A^{\mathbb{N}}$. On munit $A^{\mathbb{N}}$ de l'addition habituelle et d'une multiplication définie par : $(u_n)_n (v_n)_n = (\sum_{i+j=n} u_i v_i)_n$. Ces opérations munissent $A^{\mathbb{N}}$ d'une structure d'anneau, appelé anneau des séries formelles sur A et noté $A[[X]]$.*

On note X la suite $(0,\,1,\,0,\,\dots)$. Ainsi, toute série formelle peut s'écrire : $\sum_{i=0}^{\infty} u_i X^i$.

On définit par récurrence $A[[X_1,\,\dots,\,X_n]] := A[[X_1,\,\dots,\,X_{n-1}]][[X]]$.

Dans toute la suite A est un anneau. On fixe $n > 0$ et on note $A[[\mathbf{X}]] = A[[X_1, \ldots, X_n]]$.

Définition 67 *Soit $f = r_{i_1,\ldots,i_n} \in A[[\boldsymbol{X}]]$. Si f est non-nul, on définit le degré de f, $\deg f$, comme le plus petit d tel qu'il existe $i_1, \ldots, i_n$ avec $\sum_j i_j = d$ et $r_{i_1,\ldots,i_n} \neq 0$. Si f est nul, on pose $\deg f = -\infty$.*

Proposition 68 *Pour tous $f, g \in A[[\boldsymbol{X}]]$,*
$\deg(f+g) \geq \min\{\deg f, \deg g\}$;
$\deg(fg) \geq \deg f + \deg g$.

Démonstration. Supposons f et g non nulles (auquel cas les propositions sont évidentes) ; si $d < \min\{\deg f, \deg g\}$, alors il est clair que les coefficients des termes de degré d seront nuls.

Si $\mathbf{i} = (i_1, \ldots, i_n)$, on définit $\mathbf{X^i} := X_1^{i_1} \cdots X_n^{i_n}$. Dès lors le coefficient de $\mathbf{X^i}$ dans fg, si l'on note $f = \sum_{\mathbf{i}\in\mathbb{N}^n} a_\mathbf{i} \mathbf{X^i}$ et $g = \sum_{\mathbf{i}\in\mathbb{N}^n} b_\mathbf{i} \mathbf{X^i}$, est $\sum_{\mathbf{j},\,\mathbf{k}\ /\ \mathbf{j}+\mathbf{k}=\mathbf{i}} a_\mathbf{j} b_\mathbf{k}$. Ce coefficient est nul si $\deg \mathbf{X^i} < \deg f + \deg g$: en effet, on a alors soit $\deg \mathbf{X^j} < \deg f$ soit $\deg \mathbf{X^k} < \deg g$, et donc $a_\mathbf{j} b_\mathbf{k} = 0$. D'où le résultat. ■

Définition 69 *Soit $f \in A[[\boldsymbol{X}]]$. Si on pose $|f|_{\boldsymbol{X}} = e^{-\deg f}$ si $f \neq 0$ et $|0|_{\boldsymbol{X}} = 0$, alors $|\cdot|_{\boldsymbol{X}}$ est une "norme" ultramétrique pour $A[[\boldsymbol{X}]]$.*

En effet, si $f, g \in A[[\mathbf{X}]]$, $|f+g|_\mathbf{X} = e^{-\deg(f+g)} \leq e^{-\min\{\deg f, \deg g\}} = \max\{|f|_\mathbf{X}, |g|_\mathbf{X}\}$.

Proposition 70 *$(A[[\boldsymbol{X}]], |\cdot|_{\boldsymbol{X}})$ est un espace complet.*

Démonstration. Soit $(f_m)_m$ une suite de Cauchy ; il nous faut montrer qu'elle converge. Si on note $c_\mathbf{i}(m)$ le coefficient du monôme $\mathbf{X^i}$ dans f_m, alors on peut montrer dans un premier temps que $c_\mathbf{i}(m)$ est une suite stationnaire.

En effet, si l'on fixe $\mathbf{i}$ et si l'on note $d = \sum_j i_j$, alors, pour $p,\ m \geq N$, on a $|f_m - f_p|_\mathbf{X} \leq e^{-(d+1)}$. Donc $\deg(f_m + f_p) > d$. Donc les coefficients de tous les monômes de degré d sont nuls et $c_\mathbf{i}(m) = c_\mathbf{i}(p)$, ce qu'on voulait.

Notons donc $c_\mathbf{i}$ la valeur à laquelle la suite $(c_\mathbf{i}(m))$ stationne et montrons que $f = \sum_{\mathbf{i}\in\mathbb{N}^n} c_\mathbf{i} \mathbf{X^i}$ est la limite de $(f_m)_m$. C'est très naturel. Soit $\varepsilon > 0$. Soit d tel que $e^{-d} < \varepsilon$. Soit N tel que pour tout $\mathbf{i} \in \mathbb{N}^n$ vérifiant $\sum_j i_j \leq d$ la suite $(c_\mathbf{i}(m))_m$ ait atteint son état stationnaire au rang N. Alors, pour tout $m \geq N$, $f - f_m$ a tous les coefficients de ses monômes de degré $\leq d$ nul. Ainsi, $\deg(f - f_m) > d$ et $|f - f_m|_\mathbf{X} < e^{-d} < \varepsilon$. ■

Nous allons maintenant donner un sens à $f \circ (g_1, \ldots, g_n)$ si f et les g_i sont des séries formelles.

Soit f une série formelle à n indéterminées. Dans la suite on notera $f|_d$ le polynôme à n indéterminées obtenu en ne gardant dans f que les monômes de degré $\leq d$.

Pour tout d on peut ainsi définir $f|_d(g_1(\mathbf{X}), g_2(\mathbf{X}), \ldots, g_n(\mathbf{X}))$ qui est une somme finie de produits de séries formelles.

Proposition-Définition 71 *Soient $f, g_1, \ldots, g_n \in A[[\boldsymbol{X}]]$ tels que les g_i n'aient pas de coefficient constant.*

Alors la suite $(f|_d(g_1(\boldsymbol{X}), g_2(\boldsymbol{X}), \ldots, g_n(\boldsymbol{X})))_{d\in\mathbb{N}}$ est une suite de Cauchy. Sa limite est notée $f \circ (g_1, \ldots, g_n)$.

Démonstration. Notons la suite étudiée $(h_d)_d$ et montrons que ses coefficients sont stationnaires. En effet, le passage de f_m à f_{m+1} se fait par l'ajout de produits $\lambda_\mathbf{i} g_1^{i_1} \cdots g_n^{i_n}$ où $\sum_j i_j = m+1$. Chacun des produits est donc de degré supérieur ou égal à $m+1$, et la somme aussi. Au total, on

passe de f_m à f_{m+1} par l'ajout d'une série entière de degré supérieur ou égal à $m+1$. $(h_d)_d$ est donc de Cauchy. ■

Enfin, on définit l'évaluation d'une série formelle en une famille $(x_1, \ldots, x_n)$.

Définition 72 *On suppose que A est un sous-anneau d'un anneau A' muni d'une topologie. Soient $f \in A[[\boldsymbol{X}]]$ et $(x_1, \ldots, x_n) \in (A')^n$. On note $f(x_1, \ldots, x_n)$ l'élément de A', s'il existe, limite de la suite $(f|_d(x_1, \ldots, x_n))_{d\in\mathbb{N}}$.*

4.2.2 La fonction logarithme : définition et propriété fondamentale

On s'inspire de la définition du logarithme réel pour poser :

Proposition-Définition 73 *On définit la fonction continue :*

$$\log_p \ : \ \begin{array}{c} \mathbb{B}_p \to \mathbb{C}_p \\ x \mapsto \sum\limits_{n=1}^{\infty} (-1)^{n-1} \frac{(x-1)^n}{n} \end{array} .$$

Démonstration. On va montrer qu'il y a convergence normale sur toute boule du type $B(1, r)^\circ$ où $r < 1$. Soit $x \in B(1, r)^\circ$. Alors, on a : $\left|(-1)^{n-1} \frac{(x-1)^n}{n}\right|_p \leq r^n |n|_p^{-1}$. Or, si $n = p^m q$ où q est premier à p, on a $p^m \leq n$ donc $|1/n|_p = p^m \leq n$. Donc $\left|(-1)^{n-1} \frac{(x-1)^n}{n}\right|_p \leq r^n n \in o(r^{n/2})$ ■

D'après le paragraphe sur les séries formelles, si l'on se place dans $\mathbb{Z}[[X, Y]]$ et si l'on considère

$$f(X, Y) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{X^i}{i}, \quad g_1(X, Y) = X + Y + XY \quad \text{et} \quad g_2(X, Y) = X,$$

on peut définir $f \circ (g_1, g_2)$, qu'on notera abusivement par la suite

$$f(X + Y + XY) = f \circ (g_1, g_2) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(X + Y + XY)^i}{i}.$$

Lemme 74 *Soient $x, y \in]-1/3\,;\,1/3[$. Alors,*

$$\ln((1 + x)(1 + y)) = \left(\sum_{i=1}^{\infty} (-1)^{i+1} \frac{(X + Y + XY)^i}{i} \right)(x, y).$$

Démonstration. Soit $r < 1/3$ tel que $|x|, |y| < r$.

Par définition,

$$\ln((1 + x)(1 + y)) = \sum_{i=1}^{\infty} (-1)^i \frac{(x + y + xy)^i}{i} = \lim_{d\to\infty} \sum_{i=1}^{d} (-1)^i \frac{(x + y + xy)^i}{i}.$$

Par définition, $f(X+Y+XY)(x, y) = \lim\limits_{d\to\infty} (f(X + Y + XY))|_d(x, y)$. Cependant, on sait que tous les monômes intervenant dans $f(X+Y+XY)$ de degré au plus d sont dans $f|_d(X+Y+XY)$. Donc $(f(X + Y + XY))|_d = f|_d(X + Y + XY)|_d$. Or,

$$\begin{aligned} f|_d(X + Y + XY)|_d &= \sum_{i=1}^{d} \frac{(-1)^{i+1}}{i} \sum_{\substack{a+b+c=i \\ a+b+2c\leq d}} \frac{i!}{a!b!c!} X^{a+c} Y^{b+c} \\ &= \sum_{i=1}^{d} (-1)^{i+1} \frac{(X + Y + XY)^i}{i} - \underbrace{\sum_{i=1}^{d} \frac{(-1)^{i+1}}{i} \sum_{\substack{a+b+c=i \\ a+b+2c>d}} \frac{i!}{a!b!c!} X^{a+c} Y^{b+c}}_{R_d} \end{aligned}$$

Pour conclure, il suffit donc de voir que $R_d(x,\, y)$ tend vers 0. On calcule :

$$R_d = \sum_{i=1}^{d} \frac{(-1)^{i+1}}{i} \sum_{\substack{a+b+c=i \\ i+c>d}} \frac{i!}{a!b!c!} X^{a+c}Y^{b+c} = \sum_{i=1}^{d} \frac{(-1)^{i+1}}{i} \sum_{\substack{a+b+c=i \\ c>d-i}} \frac{i!}{a!b!c!} X^{a+c}Y^{b+c}.$$

D'où

$$\begin{aligned} |R_d(x,\, y)| &\leq \sum_{i=1}^{d} \sum_{\substack{a+b+c=i \\ c>d-i}} \frac{i!}{a!b!c!} r^{a+c}r^{b+c} \leq \sum_{i=1}^{d} \sum_{\substack{a+b+c=i \\ c>d-i}} \frac{i!}{a!b!c!} r^{i}r^{c} \\ &\leq \sum_{i=1}^{d} \sum_{\substack{a+b+c=i \\ c>d-i}} \frac{i!}{a!b!c!} r^{i}r^{d-i} \leq r^d \sum_{i=1}^{d} \sum_{a+b+c=i} \frac{i!}{a!b!c!} = r^d \sum_{i=1}^{d} 3^i \\ &\leq 3\frac{3^d-1}{2} r^d \end{aligned}$$

Comme on a pris la précaution de choisir $r < 1/3$, on a bien $R_d \to 0$. ■

Lemme 75 *Soit $g \in \mathbb{R}[[X,\, Y]]$ tel qu'il existe ε vérifiant : $\forall\, x,\, y \in]-\varepsilon,\, \varepsilon[,\, g(x,\, y) = 0$, avec convergence absolue. Alors $g = 0$.*

Démonstration. Notons qu'on sait le faire si $g \in \mathbb{R}[[X]]$: c'est la théorie des séries entières qui nous le dit. Ramenons-nous à ce cas-là.

On note $g = \sum_{i,\, i\in\mathbb{N}} a_{i,\, j} X^i Y^j$. Fixons $x,\, y \in]-\varepsilon,\, \varepsilon[$. Les hypothèses du théorème implique que la famille $\left(a_{i,\, j} x^i y^j\right)_{(i,\, j)\in\mathbb{N}^2}$ est sommable. La théorie des familles sommables (*cf.* par exemple [3]) nous autorise alors à réordonner la somme : $g(x,\, y) = \sum_{i=1}^{\infty} x^i \left(\sum_{j=1}^{\infty} a_{i,\, j} y^j\right)$. Ainsi, si l'on fixe y et l'on fait varier x, par la théorie des séries entières, on a $\forall\, y \in]\varepsilon,\, \varepsilon[,\, \forall\, i \in \mathbb{N},\, \sum_{j=1}^{\infty} a_{i,\, j} y^j = 0$. En refaisant le même raisonnement, on a : $\forall\, i,\, j \in \mathbb{N},\, a_{i,\, j} = 0$, ce qu'on voulait. ■

Remarque : Ce résultat se généralise à $\mathbb{R}[[\mathbf{X}]]$.

Lemme 76 (Identité logarithmique formelle)

$$\sum_{i=1}^{\infty} (-1)^{i+1} \frac{(X+Y+XY)^i}{i} = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(X)^i}{i} + \sum_{i=1}^{\infty} (-1)^{i+1} \frac{(Y)^i}{i}$$

Démonstration. On connaît le logarithme réel : pour tout $x,\, y \in]-1/3,\, 1/3[$, on a $\ln\left((1+x)(1+y)\right) = \ln(1+x)+\ln(1+y)$. Cela signifie que sur cet intervalle, les séries formelles $\sum_{i=1}^{\infty}(-1)^{i+1}\frac{(X+Y+XY)^i}{i}$ et $\sum_{i=1}^{\infty}(-1)^{i+1}\frac{(X)^i}{i} + \sum_{i=1}^{\infty}(-1)^{i+1}\frac{(Y)^i}{i}$ ont les mêmes évaluations. Le lemme 75 permet de conclure. ■

Théorème 77

$$\forall\, x,\, y \in \mathbb{B}_p,\, \log_p(xy) = \log_p(x) + \log_p(y)$$

Démonstration. On note $x = 1+\alpha$ et $y = 1+\beta$ et on choisit $r < 1$ tel que $|\alpha|_p\,,\, |\beta|_p < r$.

On a

$$\log_p(xy) = \lim_{d\to\infty} \sum_{i=1}^{d} (-1)^{i+1} \frac{(\alpha+\beta+\alpha\beta)^i}{i} = f(\alpha+\beta+\alpha\beta).$$

D'après tout ce qui précède, il suffit de montrer que $f(\alpha+\beta+\alpha\beta) = f(X+Y+XY)(\alpha,\, \beta)$.

Or, on a déjà vu que

$$\begin{aligned}(f(X+Y+XY))|_d &= f|_d(X+Y+XY)|_d \\ &= \sum_{i=1}^{d}(-1)^{i+1}\frac{(X+Y+XY)^i}{i} - \underbrace{\sum_{i=1}^{d}\frac{(-1)^{i+1}}{i}\sum_{\substack{a+b+c=i\\ c>d-i}}\frac{i!}{a!b!c!}X^{a+c}Y^{b+c}}_{R_d}.\end{aligned}$$

Et il nous suffit donc de montrer que $R_d(\alpha,\,\beta)\to 0$ quand $d\to\infty$. Si $1\leq i\leq d$ et si a, b, c sont des entiers tels que $a+b+c=i$ et $c>d-i$, on a

$$\left|\frac{(-1)^{i+1}}{i}\underbrace{\frac{i!}{a!b!c!}}_{\in\mathbb{N}}\alpha^{a+c}\beta^{b+c}\right|_p \leq \left|\frac{\alpha^{a+c}\beta^{b+c}}{i}\right|_p \leq r^{a+b+c}r^c\,|1/i|_p \leq r^d i \leq r^d d.$$

Par ultramétricité, on a $|R_d|_p\leq r^d d$, et le résultat est donc acquis. ■

4.2.3 Quelques propriétés de $\log_p$ sur $\mathbb{Z}_p$

Dans la suite, on s'intéresse à la restriction de $\log_p$ à $1+p\mathbb{Z}_p$, que l'on notera toujours $\log_p$.

Lemme 78 *Si $p>2$ et $x\in p\mathbb{Z}_p$ ou si $p=2$ et $x\in 4\mathbb{Z}_2$,*

$$\left|\log_p(1+x)\right|_p = |x|_p$$

Démonstration. Il nous faut évaluer les valeurs absolues p-adiques des termes de la somme et chercher la plus grande.

On a $\left|(-1)^{n+1}\frac{x^n}{n}\right|_p \leq np^{-an}$, si l'on pose $|x|_p=p^{-a}$. On veut $np^{-an}<p^{-a}$, donc $np^{-a(n-1)}<1$, donc $\frac{\ln(n)}{a(n-1)}<\ln(p)$. Or la fonction $x\mapsto\frac{\ln(x)}{x-1}$ est décroissante sur $[2\,;\,\infty[$. Il nous suffit donc d'étudier l'inégalité $\frac{\ln(2)}{a}<\ln(p)$: elle toujours vraie sauf dans le cas $p=2$ et $a=1$. ■

Proposition 79

$$\left\{\log_p\ :\ \begin{array}{c}(1+p\mathbb{Z}_p,\,\times)\to(p\mathbb{Z}_p,\,+)\\ 1+x\mapsto\log_p(1+x)\end{array}\right\}_{p>2} \textit{ et } \log_2\ :\ \begin{array}{c}(1+4\mathbb{Z}_2,\,\times)\to(4\mathbb{Z}_2,\,+)\\ 1+x\mapsto\log_2(1+x)\end{array}$$

sont des isomorphismes continus de groupes.

Démonstration. Il nous faut juste montrer l'injectivité et la surjectivité. Montrons-le pour $\log_2$, ce qui présente plus de difficulté. Soient $a=1+4\alpha$ et $b=1+4\beta$ tels que $\log_2(a)=\log_2(b)$. Écrivons $\frac{a}{b}=1+A$ ($A\in\mathbb{Z}_2$). On a alors : $1+4\alpha=1+A+4\beta+4\beta A$, donc $A=4\gamma$, avec $\gamma\in\mathbb{Z}_2$. Par ailleurs, on a $\log_2(\frac{a}{b})=\log_2(1+4\gamma)=0$. D'après le lemme précédent, $\gamma=0$ et donc $a=b$.

Pour la surjectivité, on sait que $\log_2(1+4\mathbb{Z}_2)\subset 4\mathbb{Z}_2$ est un sous-groupe additif compact de $4\mathbb{Z}_2$. Soit $x\in 1+4\mathbb{Z}_2$ tel que $|\log_2(x)|_2=1/4$. On écrit donc : $\log_2(x)=4\alpha$, où $\alpha\in\mathbb{Z}_2^\times$. Soient $\beta\in\mathbb{Z}_2$ et $(k_n)\in\mathbb{N}^n$ telle que $k_n\to\beta$. Alors, $\log_2\left(x^{k_n}\right)=k_n\log_2(x)\to 4\alpha\beta$. Comme le sous-groupe est compact, il existe $y\in 1+4\mathbb{Z}_2$ et une suite extraite k_{n_p} de k_n tels que $k_{n_p}\log_2(x)\to\log_2(y)$. Donc : il existe $y\in 1+4\mathbb{Z}_2\ /\ \log_2(y)=4\alpha\beta$. Finalement : $\log_2(1+4\mathbb{Z}_2)=4\mathbb{Z}_2$. ■

Remarque : Le résultat est faux si l'on prend $|x|_2=1/2$ et $p=2$. On a par exemple $|\log_2(1+2)|_2\leq 1/4$. C'est essentiellement ce fait qui différencie $\mathbb{Z}_2$ de $\mathbb{Z}_p$ pour $p>2$. On pourra ainsi observer, dans la suite, la singularité du comportement en $p=2$.

4.3 Lien entre la fonction puissance et la puissance logarithme

Proposition 80

$$\forall\, s \in \mathbb{Z}_p,\ \forall\, x \in p\mathbb{Z}_p, \quad \log_p\left((1+x)^s\right) = s\log_p(1+x)$$

Démonstration. On procède simplement et comme d'habitude par continuité et par densité de $\mathbb{N}$ dans $\mathbb{Z}_p$. ■

Définition 81 *Si $p > 2$, on pose* $\ln_p(x) = \frac{\log_p(x)}{\ln_p(1+p)}$.
Pour $p = 2$, on pose $\ln_4(x) = \frac{\log_2(x)}{\ln_2(1+4)}$.

Corollaire 82

$$\forall\, x \in 1 + p\mathbb{Z}_p,\ x = (1+p)^{\ln_p(x)}$$

$$\forall\, x \in 1 + 4\mathbb{Z}_2,\ x = (1+4)^{\ln_4(x)}$$

5 L'analogue p-adique de la fonction ζ et la fonction L de Kubota-Leopold

5.1 L'analogue p-adique de la fonction ζ

On a vu plus haut que $\zeta(1-2k) = \left(\frac{-B_{2k}}{2k}\right)$. On cherche à construire dans ce paragraphe une fonction continue qui prenne les valeurs $\left(\frac{-B_{2k}}{2k}\right)$ en les entiers $1-2k$. En fait, on construira une famille de fonctions continues qui prendront ces valeurs, modulo un facteur, en les entiers $1-2k$.

Plus précisément, les valeurs prises par ces fonction, en les entiers, seront parmi $(1-p^{k-1})\left(\frac{-B_k}{k}\right)$. La présence du facteur $(1-p^{k-1})$ peut être justifiée en cherchant l'analogue p-adique de ζ écrite sous forme de produit eulérien (*cf.* [1]).

Si μ est une mesure p-adique sur X et Y un compact ouvert de X, f une fonction continue définie sur Y, on note $\int_Y f\mu$ l'intégrale $\int f\mu^\star$, où $\mu^\star$ est la mesure définie sur les compact ouverts U de Y par $\mu^\star(U) = \mu(U)$.

5.1.1 Un lemme fondamental

Définition 83 *Pour tout entier positif k, on pose*

$$\zeta_p(1-k) = (1-p^{k-1})(-\frac{B_k}{k}).$$

Voici un résultat fondamental ; une expression intégrale de $(1-p^{k-1})(-\frac{B_k}{k})$.

Lemme 84

$$\forall\, k \in \mathbb{N}, \quad \forall\, \alpha \in \mathbb{N} \setminus (p\mathbb{N} \cup \{1\}), \qquad \zeta_p(1-k) = \boldsymbol{(1-p^{k-1})(-\frac{B_k}{k}) = \frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}}$$

C'est cette forme intégrale qui nous permettra d'interpoler les $\frac{-B_{2k}}{2k}$ convenablement.

Démonstration. Remarquons que $\mathbb{Z}_p^\times = \bigcup_{b=1}^{p-1} b + p\mathbb{Z}_p$ est un ouvert compact.

Notons $f : \mathbb{Z}_p^\times \to \mathbb{Q}_p$ la fonction qui x associe x^{k-1}. On a, si $N \geq 1$:

$$\begin{aligned}\mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = \int_{\mathbb{Z}_p^\times} 1\mu_{k,\alpha} \quad &= \sum_{0<a<p^N} \mu_{k,\alpha}\left(a+p^N\mathbb{Z}_p\right) \\ &\equiv_{\mathbb{Z}_p} \quad k \sum_{0<a<p^N} f(a)\mu_{1,\alpha}\left(a+p^N\mathbb{Z}_p\right) \mod p^{N-v_p(d_k)},\end{aligned}$$

d'après le théorème 58. En faisant tendre $N \to \infty$, on a donc $k\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} = \mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right)$.

Or, $\mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = \mu_{k,\alpha}\left(\mathbb{Z}_p\right) - \mu_{k,\alpha}\left(p\mathbb{Z}_p\right)$. Par ailleurs, $\mu_{k,\alpha}\left(\mathbb{Z}_p\right) = \mu_{B,k}\left(\mathbb{Z}_p\right) - \alpha^{-k}\mu_{B,k}\left(\mathbb{Z}_p\right) = (1-\alpha^{-k})B_k(0)$. Cependant, en injectant $x = 0$ dans la relation fondamentale (1), on obtient $B_k(0) = B_k$. De plus, $\mu_{k,\alpha}\left(p\mathbb{Z}_p\right) = \mu_{B,k}\left(p\mathbb{Z}_p\right) - \alpha^{-k}\mu_{B,k}\left(p\mathbb{Z}_p\right) = (1-\alpha^{-k})p^{k-1}B_k(0)$.

Finalement, $\mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = (1-\alpha^{-k})\left(1-p^{k-1}\right)B_k$, et le résultat suit. ■

5.1.2 Deux théorèmes de Kummer

Théorème 85 (Kummer) *Soient $k,\ k' \in \mathbb{N}$:*

(1) si $p-1 \nmid k$, alors $\left|\frac{B_k}{k}\right|_p \leq 1$;

(2) si $p-1 \nmid k$ et si $k \equiv_{\mathbb{Z}} k' \mod (p-1)p^N$, alors

$$\left(1-p^{k-1}\right)\frac{B_k}{k} \equiv_{\mathbb{Z}_p} \left(1-p^{k'-1}\right)\frac{B_{k'}}{k'} \mod p^{N+1}.$$

Démonstration. On choisit judicieusement $\alpha \in \mathbb{Z}_p^\times$ un représentant dans $[\![2,\ p-1]\!]$ d'un générateur de $\left(\mathbb{Z}/p\mathbb{Z}^\times,\ \times\right)$.

(1) Vu que $p-1 \nmid k$, $\alpha^k \not\equiv_{\mathbb{Z}} 1 \mod p$, $\alpha^{-k} \not\equiv_{\mathbb{Z}_p} 1 \mod p$ et $\alpha^{-k}-1 \in \mathbb{Z}_p^\times$ et $\left(\alpha^{-k}-1\right)^{-1} \in \mathbb{Z}_p$.
Si $k = 1$, le résultat est vrai. Sinon,

$$\left|\frac{B_k}{k}\right|_p = \left|\frac{1}{\alpha^{-1}-1}\right|_p \left|\frac{1}{1-p^k-1}\right|_p \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,\alpha}\right|_p = \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,\alpha}\right|_p \leq 1$$

(2) D'après le lemme précédent, la congruence désirée s'écrit

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv_{\mathbb{Z}_p} \frac{1}{\alpha^{-k'}-1}\int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \mod p^{N+1}.$$

Or, $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \in \mathbb{Z}_p$. $\left(\alpha^{-k}-1\right)^{-1}$ aussi.
Par ailleurs, comme $|\mu_{1,\alpha}(U)|_p \leq 1$ si $U \in co(\mathbb{Z}_p)$, on a, d'après le lemme 60

$$\left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} - \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha}\right|_p \leq p^{-(N+1)}.$$

Pareillement, $\alpha^k \equiv_{\mathbb{Z}_p} \alpha^{k'} \mod p^{N+1}$, donc $\alpha^{-k} \equiv_{\mathbb{Z}_p} \alpha^{-k'} \mod p^{N+1}$ puis

$$\frac{1}{\alpha^{-k}-1} \equiv_{\mathbb{Z}_p} \frac{1}{\alpha^{-k'}-1} \mod p^{N+1}.$$

En appliquant le lemme 57, on conclut.

■

5.1.3 L'analogue p-adique de la fonction ζ

Théorème-Définition 86 *Soient $s_0 \in [\![0,\, p-2]\!]$ et $\alpha \in \mathbb{N} \setminus p\mathbb{N} \cup \{1\}$.*
Si $s_0 \in [\![1,\, p-2]\!]$ et $\alpha^{s_0} \not\equiv_{\mathbb{Z}} 1 \mod p$ et si $s \in \mathbb{Z}_p$, ou si $s_0 = 0$ et $s \neq 0$, on définit, en posant

$$\zeta_{p,s_0}(s) = \frac{1}{\alpha^{-(s_0+(p-1)s)} - 1} \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)s-1} \mu_{1,\alpha},$$

une fonction continue, qui ne dépend pas de α, telle que

$$\zeta_{p,s_0}(k_0) = \zeta_p(1-k) = (1-p^{k-1}) \left(-\frac{B_k}{k}\right),$$

où $k = s_0 + (p-1)k_0$.

Démonstration. Fixons $s_0 \in [\![0,\, p-2]\!]$.

On a déjà contruit dans le paragraphe 4.1.2 une interpolation $f_{x,\,s_0}$ de $x \mapsto x^{s_0+(p-1)k}$. À peu de choses près, on a donc interpolé ζ_p.

Tout d'abord, vérifions que sous les hypothèses de l'énoncé, on a bien $f_{\alpha,\,s_0}(s) \neq 1$. Si $\alpha^{s_0} \not\equiv_{\mathbb{Z}} 1 \mod p$, alors, si $\mathbb{N}^{\mathbb{N}} \ni (k_n)_n \to s$, on a : $\alpha^{s_0+(p-1)k_n} = \alpha^{s_0} \left(\alpha^{p-1}\right)^{k_n} \equiv_{\mathbb{Z}} \alpha^{s_0} \not\equiv 1 \mod$, d'après le petit théorème de Fermat. Donc, on ne peut avoir $f_{\alpha,\,s_0}(s) = 1$. Si $s_0 = 0$ et $f_{\alpha,\,0}(s) = 1$, alors, en passant au $\log_p$, on obtient $s\alpha^{p-1} = 0$, ce qui n'est possible que si $s = 0$.

Maintenant, montrons que

$$h \;:\; \begin{array}{c} \mathbb{Z}_p \to \mathbb{Z}_p \\ s \mapsto \displaystyle\int_{\mathbb{Z}_p^\times} f_{x,\,s_0}(s)\mu_{1,\,\alpha} \end{array}$$

est bien définie et continue. Elle est bien définie car $\begin{array}{c} \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times \\ x \mapsto f_{x,\,s_0}(s) \end{array}$ est continue. En effet, on sait (proposition-définition 61) que

$$g \;:\; \begin{array}{c} \mathbb{Z}_p \to 1 + p\mathbb{Z}_p \\ (s,\, x) \mapsto x^s \end{array}$$

est uniformément continue. Il en est donc de même pour $(s,\, x) \mapsto g(s,\, x^{p+1})x^{s_0} = f_{x,\,s_0}(s)$. C'est cette même uniforme continuité qui permet de voir que h est continue.

Les constructions faites ne dépendent pas de α car les fonctions coïncident sur $\mathbb{N}$, qui est dense dans $\mathbb{Z}_p$. ■

Remarque : Les conditions que l'on a imposées à α, s_0 et s sont en fait nécessaires si l'on veut que $f_{\alpha,\,s_0}$ soit différent de 1. Si $s_0 = 0$, la condition $s \neq 0$ correspond en quelque sorte à un pôle, que l'on retrouvera en faisant une construction différente.

5.2 La fonction L de Kubota-Leopold

La fonction ζ complexe se généralise, *via* les caractères à valeurs dans $\mathbb{C}$, aux fonctions dite L de Dirichlet. On va procéder dans ce paragraphe à la même généralisation.

5.2.1 Groupe des caractères p-adiques

Définissons d'abord ce que sont les caractères p-adiques et étudions quelques propriétés du groupe qu'ils forment.

Définition 87 *On appelle groupe des caractères p-adiques, et on le note $\mathfrak{X}$:*

$$\mathfrak{X} = \mathrm{Hom}_{\mathrm{gr,\,cont}}\left(\mathbb{Z}_p^\times,\, \mathbb{C}_p^\times\right) = \left\{\chi \,:\mathbb{Z}_p^\times \to \mathbb{C}_p^\times \;/\; \chi \textit{ est un morphisme continu de groupes }\right\}.$$

On sait dévisser $\mathbb{Z}_p^\times$ ainsi, ce qui simplifie l'étude de $\mathfrak{X}$.

Proposition 88

$$\begin{array}{ccccc} \mathbb{Z}_p^\times & \xrightarrow{\sim} & \mu_{p-1} & \times & 1+p\mathbb{Z}_p \\ x & \longmapsto & \alpha_{\{x\}_1} & , & <x>=\frac{x}{\alpha_{\{x\}_1}} \end{array}$$

est un isomorphisme de groupes multiplicatifs.

Démonstration. C'est clairement un morphisme injectif. La surjectivité aussi est évidente. ■

Nous aurons aussi besoin des deux lemmes suivants ;

Lemme 89 *Soit K une extension finie de $\mathbb{Q}_p$. Soit $\sigma \in Gal\,(K/\mathbb{Q}_p)$. Alors, pour tout $x \in K$, on a $|\sigma(x)|_p = |x|_p$.*

Démonstration. On vérifie que $x \mapsto |\sigma(x)|_p$ est une valeur absolue prolongeant la valeur absolue p-adique de $\mathbb{Q}_p$ sur K. Or, on a montré en construisant $\mathbb{C}_p$ qu'il y avait une unique valeur absolue sur K vérifiant cette propriété. D'où l'égalité. ■

Lemme 90 *Soit ξ une racine primitive p^n-ième ($n > 0$) dans $\mathbb{C}_p$. Alors, $|\xi - 1|_p = p^{-\frac{1}{(p-1)p^{n-1}}}$.*

Démonstration. ξ est racine de $X^{p^n} - 1$ mais n'est pas racine de $X^{p^{n-1}} - 1$, donc est racine de $Q_n = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$, qui est irréductible d'après l'application 31. Les conjugués de $\xi - 1$ sont donc les racines de $Q_n(X+1)$, et on a donc :

$$p^{-1} = \left|\prod_{\sigma\in \mathrm{Gal}(\mathbb{Q}_p(\xi)/\mathbb{Q}_p)} \sigma(\xi-1)\right|_p = \prod_{\sigma\in \mathrm{Gal}(\mathbb{Q}_p(\xi)/\mathbb{Q}_p)} |\sigma(\xi-1)|_p = |\xi-1|_p^{p^{n-1}(p-1)},$$

d'après le lemme précédent. Donc, on a bien : $|\xi - 1|_p = p^{-\frac{1}{p^{n-1}(p-1)}}$. ■

Limitons-nous, jusqu'à la fin du paragraphe, au cas $p > 2$. On traitera le cas $p = 2$ à part.

Dès lors on peut aussi énoncer la

Proposition 91

$$\begin{array}{ccc} \mathrm{Hom}_{\mathrm{gr,\,cont}}\left(1+p\mathbb{Z}_p,\, \mathbb{C}_p^\times\right) & \xrightarrow{\sim} & \mathbb{B}_p \\ \chi & \longmapsto & \chi(1+p) \end{array}$$

est un isomorphisme de groupes multiplicatifs.

Notons qu'il nous est tout à fait légitime pour étudier la structure de $\mathfrak{X}$ de nous restreindre à $\mathrm{Hom}_{\mathrm{gr,\,cont}}\left(1+p\mathbb{Z}_p,\, \mathbb{C}_p^\times\right)$. Si on note β une racine primitive $(p-1)$-ième de l'unité, un caractère est en effet entièrement déterminé par le couple $(\chi(\beta),\, \chi(1+p))$. Réciproquement, on peut définir un caractère par la donnée de $(\gamma,\, y) = (\chi(\beta),\, \chi(1+p)) \in \mu_{p-1} \times \mathbb{B}_p$, en posant

$$\boldsymbol{\chi_{y,\gamma}(x) :\, = \chi(x) = \chi(1+p)^{\ln_p(<x>)}\chi(\beta)^{n(x)} = x^{\ln_p(<x>)}\gamma^{n(x)}},$$

où $n(x)$ est le plus petit entier tel que $\beta^{n(x)} = \frac{x}{<x>}$. On vérifie que les fonctions n et $< \cdot >$ sont continues et que χ, ainsi défini est un morphisme.

Notons aussi que $\chi(\beta) \in \mu_{p-1}$.

On transporte alors la topologie de $\mathbb{B}_p$ sur $\mathrm{Hom}_{\mathrm{gr,\,cont}}\left(1+p\mathbb{Z}_p,\, \mathbb{C}_p^\times\right)$. C'est pourquoi on peut représenter $\mathfrak{X}$ par $p-1$ boules $\mathbb{B}_p$.

Démonstration. D'abord, montrons que si $\chi \in A = \mathrm{Hom}_{\mathrm{gr,\,cont}}\left(1+p\mathbb{Z}_p,\, \mathbb{C}_p^\times\right)$, alors on a $\chi(1+p) \in \mathbb{B}_p$. Posons

$$A_N = \left|\chi(1+p)^{p^N} - \chi(1+p)^{p^{N+1}}\right|_p = |\chi(1+p)|_p^{p^N} \underbrace{|1-\chi(1+p)^p|_p}_{a}.$$

Si $|\chi(1+p)-1|_p > 1$, a est forcément non-nul car $|\chi(1+p)|_p > 1$ et car une racine de l'unité est de valeur absolue 1. On obtient ainsi une contradiction : $A_N \to \infty$, alors que A_N est sensé tendre vers $\chi(1) - \chi(1)$.

Si $|\chi(1+p)-1|_p = 1$, alors forcément, $|\chi(1+p)|_p = 1$. En effet, sinon, on a $|\chi(1+p)|_p \leq r < 1$ et pour tout $n \in \mathbb{N}$,

$$|\chi\left((1+p)^n\right) - 1|_p = |\chi(1+p)-1|_p \left|1 + \sum_{i=1}^{n-1} \chi(1+p)^i\right|_p = 1.$$

Par densité, on en déduit que pour tout $x \in 1+p\mathbb{Z}_p$, $|\chi(x)-1|_p = 1$, ce qui est absurde. Donc, $|\chi(1+p)|_p = 1$ et pour les mêmes raisons que dans le paragraphe précédent, $\chi(1+p)^p = 1$. Comme $\chi(1+p) \neq 1$, $\chi(1+p)$ est une racine primitive p-ième de l'unité et donc $|\chi(1+p)-1| = p^{-\frac{1}{p-1}} = 1$, ce qui est absurde.

Réciproquement, si $x \in \mathbb{B}_p$, on définit un élément de A en posant $\chi(1+p) = x$. En effet, si $y \in 1+p\mathbb{Z}_p$, on sait que y s'écrit $y = (1+p)^s$, avec s nécessairement égal à $\ln_p(y) \in \mathbb{Z}_p$. On pose alors : $\chi(y) = x^{\ln_p y}$, qui est un morphisme continu de groupes.

L'injectivité est claire. ■

Notons par ailleurs que

Proposition 92

$$\forall\, \chi \in \mathfrak{X},\, \forall\, x \in 1+p\mathbb{Z}_p, \quad |\chi(x)-1|_p \leq |\chi(1+p)-1|_p < 1$$

Démonstration. En effet, soient $x \in 1+p\mathbb{Z}_p$, $s \in \mathbb{Z}_p$ tel que $(1+p)^s = x$ et une suite (k_n) d'entiers tendant vers s. Alors

$$\begin{aligned}
|\chi(x)-1|_p &= |\chi(1+p)^s - 1|_p \\
&= \lim_{k_n \to s} \left|\chi(1+p)^{k_n} - 1\right|_p = \lim_{k_n \to s} |\chi(1+p)-1|_p \underbrace{\left|\sum_{i=0}^{k_n-1} \chi(1+p)^i\right|_p}_{\leq 1} \\
&\leq |\chi(1+p)-1|_p < 1
\end{aligned}$$

■

Remarque : Cette proposition reste vraie si $p = 2$

5.2.2 La fonction p-adique L de Kubota-Leopold pour $p > 2$

Dans la suite, on note $\mathfrak{X} \setminus \{1\} = \mathfrak{X}^*$.

Le caractère $\chi = 1$ correspond au problème que l'on avait eu pour définir $\zeta_{p,0}(0)$.

Venons-en (enfin) au but de cet exposé. Les expressions précédentes de l'interpolation de la fonction ζ nous inspire la

Proposition-Définition 93 (Fonction de Kubota-Leopold) *Soit $\beta = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ une racine primitive $(p-1)$-ième de l'unité.*
Soient $b \in B = \left\{ n \in \mathbb{N} \ / \ \exists\, a \not\equiv b_1 - b_0 \mod p \text{ et } N \in \mathbb{N},\ b = b_0 + ap + p^2 N \right\}$ et $\alpha = (1+p)b$.

$$L \ : \ \begin{array}{c} \mathfrak{X}^* \to \mathbb{C}_p \\ \chi \mapsto \dfrac{\chi(\alpha)}{1-\chi(\alpha)} \displaystyle\int_{\mathbb{Z}_p^\times} \frac{\chi(x)}{x} \mu_{1,\,\alpha} \end{array}$$

est la fonction L p-adique de Kubota-Leopold.

Cette définition ne dépend en fait pas du choix de α.

Démonstration. D'abord, la fonction que l'on intègre est bien définie et continue sur $\mathbb{Z}_p^\times$. Il nous faut vérifier que $\forall\, \chi \in \mathfrak{X}^*,\ \chi(\alpha) \neq 1$.

On note β la racine $(p-1)$-ième associée à b ; elle est primitive.

On va montrer un peu laborieusement que si $\chi(\alpha) = 1$ alors χ est le morphisme trivial. Si $\chi(\alpha) = \chi\left((1+p)\frac{b}{\beta}\beta\right) = 1$, alors $\chi\left((1+p)\frac{b}{\beta}\right) \in \mu_{p-1}$; or, si $\chi\left((1+p)\frac{b}{\beta}\right) \neq 1$, on a forcément

$$\left| \chi(\underbrace{(1+p)\frac{b}{\beta}}_{\in 1+p\mathbb{Z}_p}) - 1 \right|_p = 1,$$

ce qui est impossible, d'après la proposition 92. Donc $\chi\left((1+p)\frac{b}{\beta}\right) = 1$ et aussi $\chi(\beta) = 1$.

On se demande alors naturellement si $(1+p)\frac{b}{\beta}$ engendre topologiquement $1+p\mathbb{Z}_p$, auquel cas on a gagné. Autrement dit, existe-t-il $s \in \mathbb{Z}_p$ tel que

$$1 + p = \left((1+p)\frac{b}{\beta}\right)^s ?$$

L'existence d'un tel s est équivalente au fait que $1 + \ln_p\left(\frac{b}{B}\right) \in \mathbb{Z}_p^\times$. On se demande donc si $\ln_p\left(\frac{(1+p)b}{\beta}\right) \notin p\mathbb{Z}_p$. Comme on sait que $\left|\log_p(1+p)\right|_p = p^{-1}$, il nous suffit de montrer que $\left|\log_p\left(\frac{(1+p)b}{\beta}\right)\right|_p = \left|\frac{(1+p)b}{\beta} - 1\right|_p = |(1+p)b - \beta|_p = p^{-1}$.

Cette condition est vérifiée grâce aux hypothèses imposées sur α : $(1+p)b - \beta = b_0 + ap + pb_0 - b_0 - b_1 p + p^2 x = (a + b_0 - b_1)p + p^2 x$, où $x \in \mathbb{Z}_p$. Comme $|a + b_0 - b_1|_p = 1$, la condition recherchée est bien acquise et donc $\chi(1+p) = 1$ puis $\chi \equiv 1$.

■

Remarque : D'après ce qui a été dit précédemment, on peut changer l'ensemble de définition de L, et considérer :

$$L \ : \ \begin{array}{c} \mathbb{B}_p \times \mu_{p-1} \setminus \{(1,\,1)\} \to \mathbb{C}_p \\ (y,\,\gamma) \mapsto L(y,\,\gamma) = \dfrac{\chi_{y,\,\gamma}(\alpha)}{1-\chi_{y,\,\gamma}(\alpha)} \displaystyle\int_{\mathbb{Z}_p^\times} \frac{\chi_{y,\,\gamma}(x)}{x} \mu_{1,\,\alpha} \end{array}$$

Lemme 94 *Soient $X \in co(\mathbb{Z}_p)$ et μ une mesure sur X. Soit $f_n : X \to \mathbb{C}_p$ une suite de fonctions qui converge uniformément sur X vers f. Alors,*

$$\lim_{n\to\infty} \int_X f_n \mu = \int_X f\mu.$$

Démonstration. Soit A un majorant de μ. Soient $\varepsilon > 0$ et N tels que $\forall\, n \geq N$, $\forall\, x \in X$, $|f_n(x) - f(x)|_p \leq \frac{\varepsilon}{A}$. D'après le théorème 51, on a bien, si $n \geq N$, $\left|\int_X f_n\mu - \int_X f\mu\right|_p \leq \varepsilon$. ■

Corollaire 95 *Soient $X \in co(\mathbb{Z}_p)$ et μ une mesure sur X. Soit $\sum f_n : X \to \mathbb{C}_p$ une suite de fonctions qui converge normalement sur X. Alors :*

$$\sum_{n=0}^{\infty} \int_X f_n \mu = \int_X \sum_{n=0}^{\infty} f_n \mu.$$

Démonstration. C'est une conséquence immédiate du lemme précédent car les sommes partielles convergent uniformément sur X vers la somme. ■

Remarque : Les deux résultats précédents restent évidemment vrais si $p = 2$.

Théorème 96 *Il existe $p-1$ séries formelles $F_1, \ldots, F_{p-1} \in \mathbb{Z}_p[[X]]$ telles que*

$$\forall\, (y,\, \gamma) \neq (1,\, 1) \in \mathbb{B}_p \times \mu_{p-1}, \qquad L(y,\, \gamma) = \frac{\chi_{y,\gamma}(\alpha)}{1 - \chi_{y,\gamma}(\alpha)} F_{\{\gamma\}_1}(y-1).$$

Ce résultat est remarquable : on a réussi à piéger l'analogue p-adique des fonctions L dans $p-1$ séries formelles.

Démonstration. On note $\chi = \chi_{y,\gamma}$. On calcule :

$$\begin{aligned}
L(y,\,\gamma) &= \underbrace{\frac{\chi(\alpha)}{1-\chi(\alpha)}}_{C_{\alpha,\chi}} \int_{\mathbb{Z}_p^\times} \frac{\chi(x)}{x}\mu_{1,\,\alpha} = C_{\alpha,\chi} \sum_{i=1}^{p-1} \int_{i+p\mathbb{Z}_p} \frac{\chi\left(\frac{x}{\alpha_i}\alpha_i\right)}{x}\mu_{1,\,\alpha} \\
&= C_{\alpha,\chi} \sum_{i=1}^{p-1} \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{\chi\left(\frac{x}{\beta^i}\beta^i\right)}{x}\mu_{1,\,\alpha} = C_{\alpha,\chi} \sum_{i=1}^{p-1} \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{\gamma^i\chi\left(\frac{x}{\beta^i}\right)}{x}\mu_{1,\,\alpha} \\
&= C_{\alpha,\chi} \sum_{i=1}^{p-1} \gamma^i \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{\chi\left((1+p)^{\ln_p\left(\frac{x}{\beta^i}\right)}\right)}{x}\mu_{1,\,\alpha} \\
&= C_{\alpha,\chi} \sum_{i=1}^{p-1} \gamma^i \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{y^{\ln_p\left(\frac{x}{\beta^i}\right)}}{x}\mu_{1,\,\alpha} = C_{\alpha,\chi} \sum_{i=1}^{p-1} \gamma^i \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{(1+(y-1))^{\ln_p\left(\frac{x}{\beta^i}\right)}}{x}\mu_{1,\,\alpha} \\
&= C_{\alpha,\chi} \sum_{i=1}^{p-1} \gamma^i \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{\sum\limits_{k=1}^{\infty} \mathrm{C}^k_{\ln_p\left(\frac{x}{\beta^i}\right)}(y-1)^k}{x}\mu_{1,\,\alpha} \\
&=_{(*)} C_{\alpha,\chi} \sum_{i=1}^{p-1} \gamma^i \sum_{k=1}^{\infty}(y-1)^k \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{\mathrm{C}^k_{\ln_p\left(\frac{x}{\beta^i}\right)}}{x}\mu_{1,\,\alpha} \\
&= C_{\alpha,\chi} \sum_{k=1}^{\infty}(y-1)^k \underbrace{\left(\sum_{i=1}^{p-1} \gamma^i \int_{\{\beta^i\}_1+p\mathbb{Z}_p} \frac{\mathrm{C}^k_{\ln_p\left(\frac{x}{\beta^i}\right)}}{x}\mu_{1,\,\alpha}\right)}_{A_n(\gamma)}
\end{aligned}$$

Justifions l'interversion $(*)$ à l'aide du corollaire 95. On note

$$\begin{array}{rccc} f_n & : & \{\beta^i\}_1 + p\mathbb{Z}_p & \to & \mathbb{C}_p \\ & & x & \mapsto & \frac{\mathrm{C}^k_{\ln_p\left(\frac{x}{\beta^i}\right)}(y-1)^k}{x} \end{array}.$$

On a $|f_n(x)|_p \leq (y-1)^k$: la série est normalement convergente.

Enfin, les coefficients $A_n(\gamma)$ sont dans $\mathbb{Z}_p$ car l'intégrande est dans $\mathbb{Z}_p$ ($x \in \mathbb{Z}_p^\times$) et car la mesure $\mu_{1,\,\alpha}$ est bornée par 1. ■

5.2.3 La fonction p-adique L de Kubota-Leopold pour $p = 2$

Les choses ne marchent pas tout à fait de la même façon, mais les résultats sont les mêmes.

Notons d'abord que $1 + 2\mathbb{Z}_2 = (1 + 2 + 4\mathbb{Z}_2) \cup (1 + 4\mathbb{Z}_2) = -(1 + 4\mathbb{Z}_2) \cup (1 + 4\mathbb{Z}_2)$, puisque $1 + 2 + 4\alpha = -(1 + 4(-1 - \alpha))$.

Par ailleurs, l'analogue de la propositon 91 (qui concerne $\mathrm{Hom}_{\mathrm{gr,\,cont}}(1 + p\mathbb{Z}_p,\, \mathbb{C}_p)$ pour $p > 2$ est :

Proposition 97

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{gr,\,cont}}\left(1 + 4\mathbb{Z}_2,\, \mathbb{C}_2^\times\right) & \xrightarrow{\sim} & \mathbb{B}_2 \\ \chi & \longmapsto & \chi(1+4) \end{array}$$

est un isomorphisme de groupes multiplicatifs.

On adapte la démonstration de la proposition 91.

Démonstration. Vérifions d'abord que le morphisme est bien défini.

Si $|\chi(1+4)-1|_2 > 1$, alors $|\chi(1+4)|_2 > 1$ et vu que

$$\left|\chi\left((1+4)^{2^N}\right) - \chi\left((1+4)^{P^{N+1}}\right)\right|_2 = |\chi(1+p)|_2^{2^N} \left|\chi(1+4)^2 - 1\right|_2,$$

on a forcément $\chi(1+4) = \pm 1$. Cependant, on ne peut avoir ni $\chi(1+4) = 1$ ni $\chi(1+4) = -1$, car $|2|_2 < 1$. C'est absurde.

Si $|\chi(1+4)-1|_2 = 1$, alors $|\chi(1+4)|_2 = 1$. Sinon, pour tout $n \in \mathbb{N}$, $|\chi\left((1+4)^n\right) - 1|_2 = 1$, ce qui est absurde. On a donc $\chi(1+4) = \pm 2$, ce qui est contradictoire.

Comme l'injectivité est claire ($1+4$ engendre topologiquement $1+4\mathbb{Z}_2$, *ie* $\overline{<(1+4)>} = 1 + 4\mathbb{Z}_2$), montrons la surjectivité. Si $x \in \mathbb{B}_2$, et si l'on pose $\chi(1+4) = x$, on doit nécessairement avoir $\chi(y) = \chi\left((1+4)^{\ln_4(y)}\right) = \chi(1+4)^{\ln_4(y)} = x^{\ln_4(y)}$. Cette formule définit le caractère cherché. ■

On en déduit la

Proposition 98

$$\begin{array}{ccc} \mathfrak{X} & \xrightarrow{\sim} & \mathbb{B}_2 \times \pm 1 \\ \chi & \longmapsto & (\chi(1+4),\, \chi(-1)) \end{array}$$

est un isomorphisme de groupes multiplicatifs.

Autrement dit, $\mathfrak{X}$ peut être représenté par deux boules disjointes $\mathbb{B}_2$.

Démonstration. Le morphisme est bien défini ; il est injectif d'après tout ce qui précède. Il est sujectif car si $x \in \mathbb{B}_2$ et $\varepsilon \in \{\pm 1\}$, on définit un caractère en posant sur l'ouvert $1+4\mathbb{Z}_2$, $\chi(y) = x^{\ln_4(y)}$ et sur l'ouvert $1+2+4\mathbb{Z}_2$, $\chi(y) = \varepsilon x^{\ln_4(-y)}$. ■

On ne peut, arrivé à ce point, faire la même chose que pour $p > 2$. En effet, il n'existe pas de $\alpha \in \mathbb{Z}_2^\times$ tel que $\chi(\alpha) = 1 \Longrightarrow \chi \equiv 1$.

On va donc (malheureusement) ôter un point supplémentaire à $\mathfrak{X}$: on pose $\mathfrak{X}^{**} = \mathfrak{X}^* \setminus \{(1,\, -1)\}$, si l'on considère l'identification $\mathfrak{X} = \mathbb{B}_2 \times \pm 1$.

Proposition-Définition 99 *On donne la même défintion de la fonction L, à savoir que si $\chi \in \mathfrak{X}^{**}$, on pose*

$$L(\chi) = \frac{\chi(1+4)}{1-\chi(1+4)} \int_{\mathbb{Z}_2^\times} \frac{\chi(x)}{x} \mu_{1,\, 1+4}.$$

Démonstration. χ est entièrement déterminé par $\chi(1+4) \in \mathbb{B}_2$ et $\chi(-1) = \pm 1$. Donc, si $\chi(1+4) = 1$, on a deux choix possibles pour χ, qui sont les cas exclus. ■

Remarque : Au lieu de $\alpha = 1+4$, on aurait pu prendre, par exemple, $\alpha = 3(1+4)$ et exclure le point $(-1,\, -1)$. Il nous aurait ensuite fallu vérifier que les deux fonctions (continues) coïncident sur l'intersection de leurs domaines et donc que l'on peut définir une fonction L sur $\mathfrak{X}^*$.

En reprenant les mêmes notations que pour $p > 2$, on peut énoncer le

Théorème 100 *Il existe 2 séries formelles $F_1,\, F_{-1} \in \mathbb{Z}_p[[X]]$ telles que*

$$\forall\, (y,\, \varepsilon) \neq (1,\, \pm 1) \in \mathbb{B}_2 \times \pm 1, \qquad L(y,\, \varepsilon) = \frac{\chi_{y,\varepsilon}(1+4)}{1-\chi_{y,\varepsilon}(1+4)} F_\varepsilon(y-1).$$

Démonstration. On calcule :

$$\begin{aligned}
L(\chi) &= \underbrace{\frac{\chi(1+4)}{\chi(1+4)-1}}_{C_\chi}\int_{\mathbb{Z}_2^\times}\frac{\chi(x)}{x}\mu_{1,\,1+4} = C_\chi\left(\int_{1+4\mathbb{Z}_2}\frac{\chi(x)}{x}\mu_{1,\,1+4}+\int_{-(1+4\mathbb{Z}_2)}\frac{\chi(x)}{x}\mu_{1,\,1+4}\right)\\
&= C_\chi\left(\int_{1+4\mathbb{Z}_2}\frac{\chi(1+4)^{\ln_4(x)}}{x}\mu_{1,\,1+4}+\int_{-(1+4\mathbb{Z}_2)}\chi(-1)\frac{\chi(1+4)^{\ln_4(-x)}}{x}\mu_{1,\,1+4}\right)\\
&= C_\chi\left(\int_{1+4\mathbb{Z}_2}\frac{1}{x}\sum_{n=0}^{\infty}\mathrm{C}^n_{\ln_4(x)}\left(\chi(1+4)-1\right)^n\mu_{1,\,1+4}+\right.\\
&\qquad\left.\chi(-1)\int_{-(1+4\mathbb{Z}_2)}\frac{1}{x}\sum_{n=0}^{\infty}\mathrm{C}^n_{\ln_4(-x)}\left(\chi(1+4)-1\right)^n\mu_{1,\,1+4}\right)\\
&= C_\chi\sum_{n=0}^{\infty}\left(\chi(1+4)-1\right)^n\underbrace{\left(\int_{1+4\mathbb{Z}_2}\frac{\mathrm{C}^n_{\ln_4(x)}}{x}\mu_{1,\,1+4}+\chi(-1)\int_{-(1+4\mathbb{Z}_2)}\frac{\mathrm{C}^n_{\ln_4(-x)}}{x}\mu_{1,\,1+4}\right)}_{A_{n,\,\chi(-1)}}
\end{aligned}$$

Enfin, l'interversion $\sum$-$\int$ se justifie comme pour $p>2$, ainsi que le fait $A_{n,\,\chi(-1)}\in\mathbb{Z}_2^\times$. ■

Conclusion

Deux choses en conclusion.

Première chose

La première est que les $p-1$ séries formelles qui apparaissent à la fin de l'exposé sont l'objet d'un théorème. Longtemps (et encore) connu sous le nom de conjecture d'Iwasawa, il a été démontré par Mazur et Wiles. Grossièrement, il affirme que les $p-1$ séries de notre fonction L sont les mêmes $p-1$ séries que celles apparaissant dans une construction de théorie algébrique des nombres relative aux corps cyclotomiques.

Deuxième chose

En outre, voici quelques questions/pistes ouvertes par ce rapport. Nous n'avons pas eu le temps (ni, en fait, la place) de démontrer l'unicité des $p-1$ séries formelles (ou des fonctions L). En fait, nous supposons qu'il faut faire une autre transformation en série entière et utiliser un lemme du type

Lemme 101 *Soit $F\in\mathbb{C}_p[[X]]$ telle que $F(x)$ converge si $x\in D=B_{\mathbb{C}_p}(0,\,r)^\circ$. S'il existe $x\in D$ et $(x_n)_n\in D^{\mathbb{N}}$ tels que $x_n\to x$ et $\forall\, n\in\mathbb{N},\ F(x_n)=0$, alors $F=0$.*

qu'on démontre sûrement par une règle d'intersion des sommes. Au passage, on se demande ce qu'il en est d'un cadre général pour les problèmes de famille sommable et d'interversion de sommes : peut-être peut-on s'inspirer du beau travail fait dans [3] pour au moins étendre les chose à $\mathbb{C}_p$.

Autre problème : le fait que l'on ne puisse définir naturellement L sur $\mathfrak{X}^*$ pour $p=2$. Selon le α que l'on choisit, la formule définit une fonction dont le domaine varie. On se pose la question, donc, d'une autre approche qui permettrait de définir directement L pour $p=2$.

Autre question : est-ce que l'on peut étendre le choix de α pour la définition de L à $\alpha = (1+p)b$ où b génère $\left(\mathbb{Z}/_{p\mathbb{Z}}, \times\right)$?

Références

[1] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, GTM 58, 1977.

[2] Yvette Amice, *Les nombres p-adiques*, PUF, Collection Sup, 1975.

[3] Jean-Marie Arnaudiès, Henri Fraysse, *Cours de mathématiques-2 Analyse*, Dunod Université, 1988.

[4] Hervé Gianella, *Nombres p-adiques*.