Analyse différentielle p-adique et Polynômes à valeurs entières

Enno Nagel *

Ces notes accompagnent mon exposé du 6 octobre 2014 au Séminaire d'Algèbre à l'Université de Picardie Jules Verne à Amiens.

Table des matières

Notation

Soient

*Merci à toute l'équipe de polynômes à valeurs entières

— $\mathbb{Q}_p$ tous les nombres p-adiques et $\mathbb{Z}_p$ tous les nombres p-adiques entiers, et

— $\mathbb{C}_p$ la complétion de la clôture algébrique de $\mathbb{Q}_p$ et $\mathbf{o}_{\mathbb{C}_p}$ tous les nombres entiers dans $\mathbb{C}_p$.

1 Dérivabilité non-Archimédienne

Soit $\mathbf{K}$ un corps *non-Archimédien*, c'est-à-dire un corps avec une valuation qui est non-Archimédienne, complète et non-triviale.

Fonctions d'une variable

A priori, on peut formuler la définition de dérivabilité sur un corps non-Archimédien $\mathbf{K}$ comme sur $\mathbb{R}$.

Définition. Une fonction $f : \mathrm{X} \to \mathbf{K}$ sur un sous-ensemble X de $\mathbf{K}$ est *dérivable* à a dans X s'il y a $f'(a)$ dans $\mathbf{K}$ tel que

$$\frac{f(x_n) - f(a)}{x_n - a} \to f'(a)$$

pour toute suite (x_n) dans X tel que $x_n \to a$.

La complétude de $\mathbf{K}$ assure que le *dérivé* $f'(a)$ toujours existe dans $\mathbf{K}$ et la non-trivialité de sa topologie qu'il est unique.

Pourtant, comme $\mathbf{K}$ est totalement desconnexe, il n'y a pas d'analogue du

— Théorème de la valeur Intermédiaire ou du

— Théorème de la valeur moyenne.

Et alors, nous rencontrons les pathologies suivantes :

— Les fonctions dérivables avec leur norme naturelle ne sont plus complètes,

— il y a une fonction dont le dérivé est partout inversible mais elle n'est localement inversible nulle part, et

— la fonction

$$\begin{aligned} f : \mathbb{Z}_p &\to \mathbb{Q}_p \\ \sum_{n\in\mathbb{N}} a_n p^n &\mapsto \sum_{n\in\mathbb{N}} a_n p^{2n} \end{aligned}$$

* est injective, mais son dérivé est 0 partout, et
* infiniment souvent dérivable mais son polynôme de Taylor de degré plus grand 1 ne converge pas.

Pour exclure ces pathologies, nous renforçons la définition de dérivabilité.

Définition. La fonction $f: \mathrm{X} \to \mathbf{K}$ sur un sous-ensemble X de **K** est continument dérivable si sa *différence divisée*

$$f^{]1[}(x,y) = \frac{f(x) - f(y)}{x - y}$$

définie pour tous x et y dans X distincts, s'étend à une fonction continue sur tout $\mathrm{X} \times \mathrm{X}$.

Pour une fonction à valeurs réelles, le théorème de la valeur moyenne montre que la condition de dérivabilité Archimédienne et non-Archimédienne sont équivalentes.

Fonctions de plusieurs variables

Dérivabilité simple.

Soient V et **E** deux espaces de **K**-Banach et X an sous-ensemble ouvert de V.

Définition. Une fonction $f: \mathrm{X} \to \mathbf{E}$ est $\mathscr{C}^1$ à a dans X s'il y a une application **K**-linéaire $\mathrm{A}\colon \mathrm{V} \to \mathbf{E}$ tel que pour tout $\epsilon > 0$, il y a un voisinage U autour de a inclus dans X tel que pour tous $x + h, x$ dans U vaut

$$\|f(x+h) - f(x) - \mathrm{A}(h)\| \leq \epsilon \|h\|.$$

Rappelons que cette dérivabilité non-Archimédienne est plus stricte que la dérivabilité Archimédienne, parce que

— dans la dérivabilité *non-Archimédienne* le décalage h et le point d'expansion x varient, tandis que

— dans la dérivabilité *Archimédienne* h varie mais x reste fixé.

Pour itérer la définition de dérivabilité non-Archimédienne, on introduit des coordonnées sur V par le choix d'une base ordonnée $(e_1, \dots, e_d)$ de V.

Définition. La *différence divisée* $f^{]1[}(x+h,x)$ d'une fonction $f\colon \mathrm{X}\to\mathbf{E}$ à $x+h,x$ dans X avec h dans $\mathbf{K}^{*d}$ est l'application $\mathbf{K}$-linéaire A définie par

$$\mathrm{A}e_k := \frac{f(x+h_1e_1+\cdots+h_{k-1}e_{k-1}+h_ke_k)-f(x+h_1e_1+\cdots+h_{k-1}e_{k-1})}{h_k}$$

pour chaque $k=1,\ldots,d$. La fonction f est une $\mathscr{C}^1$*-fonction* si $f^{]1[}$ s'étend à une fonction continue $f^{[1]}\colon \mathrm{X}\times\mathrm{X}\to\mathbf{E}$.

Dérivabilité itérée. Comparons le domaine et codomaine de $f^{[1]}$ avec ceux de f.

— Le domaine $\mathrm{X}^{[1]} := \mathrm{X}\times\mathrm{X}$ de $f^{[1]}$ est inclus dans le $\mathbf{K}$-espace vectoriel $\mathrm{V}^{[1]}=\mathrm{V}\times\mathrm{V}$ avec une base ordonnée canonique, comme le domaine X de f, et

— le codomaine $\mathbf{E}^{[1]} := \mathrm{Hom}_{\mathbf{K}}(\mathrm{V},\mathbf{E})$ de $f^{[1]}$ est un $\mathbf{K}$-espace de Banach, comme le codomaine $\mathbf{E}$ de f.

On peut alors itérer la définition de la dérivabilité non-Archimédienne en l'appliquant à $f^{[1]}$ au lieu de f.

Définition. La fonction $f\colon \mathrm{X}\to\mathbf{E}$ est une $\mathscr{C}^2$-fonction si, primo $f^{[1]}$ existe, et secundo sa différence divisée

$$f^{]2[} = (f^{[1]})^{]1[}\colon (\mathrm{X}^{[1]})^{]1[}\to(\mathbf{E}^{[1]})^{[1]}$$

s'étend à une fonction continue $f^{[2]}$ sur $\mathrm{X}^{[2]} := (\mathrm{X}^{[1]})^{[1]} = (\mathrm{X}\times\mathrm{X})\times(\mathrm{X}\times\mathrm{X})$ à valeurs dans $\mathbf{E}^{[2]} := (\mathbf{E}^{[1]})^{[1]}) = \mathrm{Hom}_{\mathbf{K}}(\mathrm{V}\times\mathrm{V},\mathrm{Hom}_{\mathbf{K}}(\mathrm{V},\mathbf{E}))$.

Dérivabilité fractionnelle. En la théorie de représentations de groupes de Lie p-adiques, la notion suivante joue un rôle important. Soit $r\geq 0$ un nombre réel et $r=\nu+\rho$ avec ν un nombre entier et ρ dans $[0,1[$.

Définition. Soient X et Y des espaces métriques et $f\colon\mathrm{X}\to\mathrm{Y}$. La fonction f est une $\mathscr{C}^\rho$*-fonction* si pour tout a dans X et tout $\epsilon>0$ il y a un voisinage U autour de a inclus dans X tel que

$$d(f(x),f(y))\leq\epsilon d(x,y)^\rho$$

pour tous x et y dans U.

Soient V un espace vectoriel et **E** un espace de Banach. Soit X un sous-ensemble ouvert de V et $f\colon X \to \mathbf{E}$. On applique la notion de ρ-fois dérivabilité à la différence divisée itérée de f.

Définition. La fonction f est une *$\mathscr{C}^r$-fonction* si elle est une $\mathscr{C}^\nu$-fonction est $f^{[\nu]}$ est une $\mathscr{C}^\rho$-fonction.

2 Polynômes à valeurs entières comme bases orthonormales

On introduit la base de Mahler, une certaine base de fonctions polynomiales de toutes les fonctions continues (ou localement analytiques) sur $\mathbb{Z}_p$, et sa généralisation, la base Fourier, une certaine base de fonctions polynomiales de toutes les fonctions localement analytiques sur $\mathbf{o_K}$. L'évaluation de notre mesure sur ces fonctions de base donnera les coefficients de ces fonctions analytiques.

La base de Mahler des fonctions continues

Soient $\mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p)$ toutes les fonctions continues $f\colon \mathbb{Z}_p \to \mathbb{C}_p$ et $\mathscr{D}^0(\mathbb{Z}_p,\mathbb{C}_p)$ toutes les applications linéaires continues $\mu\colon \mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p) \to \mathbb{C}_p$.

L'ensemble $\mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p)$ est un espace normé avec la norme de supremum et $\mathscr{D}^0(\mathbb{Z}_p,\mathbb{C}_p)$ est une algèbre normée avec la norme d'opérateur et le *produit de convolution* défini par $\mu * \nu(f) = \mu[x \mapsto \nu f(\cdot + x)]$.

Une *base orthonormale* de $\mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p)$ est une suite des fonctions $(e_n : n \in \mathbb{N})$ tel que l'homomorphisme d'espaces normés

$$\begin{aligned} c^0(\mathbb{N},\mathbb{C}_p) &\to \mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p) \\ (a_n) &\mapsto \sum a_n e_n \end{aligned}$$

entre les suites à zéro de valeurs dans $\mathbb{C}_p$ et $\mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p)$ est un isomorphisme.

La *base de Mahler* est la base orthonormale de $\mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p)$ donnée par la suite des polynômes $\binom{\cdot}{0}, \binom{\cdot}{1}, \binom{\cdot}{2}, \dots$ avec $\binom{\cdot}{n} = x(x-1)\cdots(x-n+1)/n!$ pour tout n dans $\mathbb{N}$.

Elle se distingue entre toutes les bases orthonormales de $\mathscr{C}^0(\mathbb{Z}_p,\mathbb{C}_p)$ par le fait qu'elle est duale à un isomorphisme entre les *$\mathbf{o}_{\mathbb{C}_p}$-algèbres* normées $\mathscr{D}^0(\mathbb{Z}_p,\mathbb{C}_p)$ et $\mathbf{o}_{\mathbb{C}_p}[[t]]$, l'algèbre de séries de puissance de coefficients dans $\mathbf{o}_{\mathbb{C}_p}$, que nous présentons maintenant. (Tandis qu'une base orthonormale quelconque n'est que duale à un isomorphisme entre celles en tant que $\mathbf{o}_{\mathbb{C}_p}$-modules normés)

L'algèbre de groupe complétée (sur $\mathbf{o}_{\mathbb{C}_p}$) de $\mathbb{Z}_p$ est la limite projective

$$\mathbf{o}_{\mathbb{C}_p}[[\mathbb{Z}_p]] := \varprojlim \mathbf{o}_{\mathbb{C}_p}[[\mathbb{Z}/p^n\mathbb{Z}]]$$

des transitions d'algèbres de groupe (sur $\mathbf{o}_{\mathbb{C}_p}$) donnée par

$$\mathbf{o}_{\mathbb{C}_p}[1] \leftarrow \ldots \leftarrow \mathbf{o}_{\mathbb{C}_p}[\mathbb{Z}/p^n\mathbb{Z}] \leftarrow \mathbf{o}_{\mathbb{C}_p}[\mathbb{Z}/p^{n+1}\mathbb{Z}] \leftarrow \ldots.$$

Observation (algèbre de mesures sur un groupe pro-fini comme anneau de groupe profini). L'homomorphisme d'algèbres topologiques

$$\begin{aligned} \mathcal{D}^0(\mathbb{Z}_p, \mathbf{o}_{\mathbb{C}_p}) &\to \mathbf{o}_{\mathbb{C}_p}[[\mathbb{Z}_p]] \\ \mu &\mapsto (\ldots, \mu_{\restriction \mathscr{C}^0(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{C}_p)}, \ldots), \end{aligned}$$

où $\mathscr{C}^0(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{C}_p)$ soient toutes les fonctions constantes sur chaque translate de $p^n\mathbb{Z}_p$, est un isomorphisme.

Démonstration : C'est l'énoncé dual du fait que l'application donnée par l'inclusion naturelle

$$\bigcup \mathbf{o}_{\mathbb{C}_p}[\mathbb{Z}/p^n\mathbb{Z}] \hookrightarrow \mathscr{C}^0(\mathbb{Z}_p, \mathbf{o}_{\mathbb{C}_p})$$

des fonctions localement constantes dans les fonctions continues sur $\mathbb{Z}_p$ a image dense. □

Observation (Isomorphisme d'Iwasawa). L'homomorphisme d'algèbres topologiques

$$\begin{aligned} \mathbf{o}_{\mathbb{C}_p}[[\mathbb{Z}_p]] &\to \mathbf{o}_{\mathbb{C}_p}[[t]] \\ 1 + \mathbf{1} &\mapsto t, \end{aligned}$$

où $\mathbf{o}_{\mathbb{C}_p}[[t]]$ porte la topologie de convergence par coefficient et $\mathbf{o}_{\mathbb{C}_p}$ la topologie de limite projective, est un isomorphisme.

Démonstration : Utilise que $\mathbb{Z}_p$ est en tant que groupe topologique engendré par un seul élément, par exemple $\mathbf{1}$. □

Theorème 2.1 (Mahler). *L'homomorphisme d'algèbres topologiques*

$$\begin{aligned} \mathcal{D}^0(\mathbb{Z}_p, \mathbb{C}_p) &\to \mathbb{C}_p \otimes_{\mathbf{o}_{\mathbb{C}_p}} \mathbf{o}_{\mathbb{C}_p}[[t]] \\ \mu &\mapsto \mu(\binom{\cdot}{0}) + \mu(\binom{\cdot}{1})t + \cdots \end{aligned}$$

entre $\mathcal{D}^0(\mathbb{Z}_p, \mathbb{C}_p)$ et toutes les séries de puissances de coefficients uniformément bornés dans $\mathbb{C}_p$ est un isomorphisme.

Démonstration : Utilise que

(i) $\mathbf{1}$ dans $\mathbf{o}_{\mathbb{C}_p}[[\mathbb{Z}_p]]$ correspond à la mesure δ_0 donnée par $f \mapsto f(0)$ dans $\mathcal{D}^0(\mathbb{Z}_p, \mathbf{o}_{\mathbb{C}_p})$,

(ii) calcule ses convolutions $\delta_0 * \cdots * \delta_0$ itérées, et

(iii) vérifie que $\delta_0^i\binom{\cdot}{j}$ est 1 si et seulement si $i = j$ et 0 sinon. □

Corollaire (Dualité de Schikhof). *L'homomorphisme d'espaces normés*

$$\begin{aligned} c^0(\mathbb{Z}_p, \mathbb{C}_p) &\to \mathcal{C}^0(\mathbb{Z}_p, \mathbb{C}_p) \\ (a_n) &\mapsto \sum a_n \binom{\cdot}{n} \end{aligned}$$

est un isomorphisme.

La base de Mahler de fonctions localement analytiques

Une fonction $f : \mathbb{Z}_p \to \mathbb{C}_p$ est *analytique* s'il y a des coefficients $a_0, a_1, \ldots$ dans $\mathbb{C}_p$ tel que

$$f(h) = a_0 + a_1 h + a_2 h^2 + \cdots$$

pour tout h dans $\mathbb{Z}_p$. Une fonction $f : \mathbb{Z}_p \to \mathbb{C}_p$ est *n-analytique* pour un nombre naturel n si pour toute classe de congruence $a + p^n\mathbb{Z}_p$ de $\mathbb{Z}_p$ modulo p^n la restriction $f(a + \cdot) : p^n\mathbb{Z}_p \to \mathbb{C}_p$ est analytique. Une fonction $f : \mathbb{Z}_p \to \mathbb{C}_p$ est *localement analytique* si elle est n-analytique pour un nombre naturel n.

Soient $\mathcal{C}^{\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p)$ toutes les fonctions localement analytiques $f : \mathbb{Z}_p \to \mathbb{C}_p$ et $\mathcal{D}^{\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p)$ toutes les applications linéaires continues $\mu : \mathcal{C}^{\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p) \to \mathbb{C}_p$ (et analogue pour les fonctions n-analytiques).

L'ensemble $\mathcal{C}^{\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p)$ est un espace de Fréchet par les normes de coefficients sur $\mathcal{C}^{1-\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p), \mathcal{C}^{2-\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p), \ldots$ et $\mathcal{D}^0(\mathbb{Z}_p, \mathbb{C}_p)$ est une algèbre de Fréchet

— par les normes d'opérateur sur $\mathcal{D}^{1-\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p), \mathcal{D}^{2-\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p), \ldots$ et

— par le *produit de convolution* défini par $\mu * \nu(f) = \mu[x \mapsto \nu f(\cdot + x)]$.

Theorème 2.2 (Amice, cf. [Ami64]). *L'homomorphisme d'algèbres topologiques*

$$\begin{aligned} \mathcal{D}^{\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p) &\to \mathcal{O}(\mathrm{B}) \\ \mu &\mapsto \mu(\binom{\cdot}{0}) + \mu(\binom{\cdot}{1})t + \cdots, \end{aligned}$$

entre $\mathcal{D}^{\mathrm{an}}(\mathbb{Z}_p, \mathbb{C}_p)$ et toutes les séries de puissances dans $\mathbb{C}_p[[t]]$ qui convergent sur toute la boule d'unité ouverte B, est un isomorphisme.

Corollaire 2.3 ([Nag15]). *L'homomorphisme d'espaces normés*

$$c^r(\mathbb{Z}_p, \mathbb{C}_p) \to \mathscr{C}^r(\mathbb{Z}_p, \mathbb{C}_p)$$
$$(a_n) \mapsto \sum a_n \binom{\cdot}{n}$$

entre toutes les suites (a_n) *tel que* $|a_n|n^r$ *converge vers* 0 *et* $\mathscr{C}^r(\mathbb{Z}_p, \mathbb{C}_p)$ *est un isomorphisme.*

La base de Fourier

Soit $\mathbf{K}$ une extension finie de $\mathbb{Q}_p$ et $\mathbf{o_K}$ tous les nombres entiers dans $\mathbf{K}$. La base de Mahler $\binom{\cdot}{0}, \binom{\cdot}{1}, \ldots$ comme suite des fonctions continues sur $\mathbf{o_K}$, n'est plus une base orthonormale de $\mathscr{C}^0(\mathbf{o_K}, \mathbb{C}_p)$. (Par exemple, ses fonctions n'ont plus de valeurs entières.) Au lieu d'elle il y a la *base de Fourier* $P_0, P_1, \ldots$ qui, elle, est aussi

- une suite des fonctions polynomiales à valeurs entières tel que
  - le polynôme P_n est du degré n,
  - a comme coefficient plus haut $1/n!$, et
  - son coefficient constant est 0 pour $n \geq 1$.
- est duale à un isomorphisme entre l'algèbre de distributions localement analytiques et toutes les séries de puissance qui convergent sur toute la boule d'unité ouverte.

Si $\mathbf{o_K}$ est $\mathbb{Z}_p$, alors les polynômes de Fourier $P_0, P_1, \ldots$ sont les polynômes de Mahler $\binom{\cdot}{0}, \binom{\cdot}{1}, \ldots$, et en général seront décrits dans la prochaine section. Rendons le deuxième point en haut explicite.

Theorème 2.4 (Schneider et Teitelbaum, cf. [ST01]). *L'homomorphisme d'algèbres topologiques*

$$\mathscr{D}^{\mathrm{an}}(\mathbf{o_K}, \mathbb{C}_p) \to \mathscr{O}(B)$$
$$\mu \mapsto \mu(P_0) + \mu(P_1)t + \cdots$$

entre $\mathscr{D}^{\mathrm{an}}(\mathbf{o_K}, \mathbb{C}_p)$ *et toutes les séries de puissances dans* $\mathbb{C}_p[[t]]$ *qui convergent sur toute la boule d'unité ouverte* B *est un isomorphisme.*

Corollaire 2.5 ([Nag18]). *Soit* $\mathbf{K}$ *une extension finie de* $\mathbb{Q}_p$ *de degré* d *et* $r \geq d$. *L'homomorphisme d'espaces normés*

$$c^r(\mathbf{o_K}, \mathbb{C}_p) \to \mathscr{C}^r(\mathbf{o_K}, \mathbb{C}_p)$$
$$(a_n) \mapsto \sum a_n \mathrm{P}_n$$

entre toutes les suites (a_n) *tel que* $|a_n|n^r$ *converge vers* 0 *et* $\mathscr{C}^r(\mathbf{o_K}, \mathbb{C}_p)$ *est un isomorphisme.*

3 La Transformation de Fourier

Soit G un groupe et $\hat{\mathrm{G}}$ les caractères continus sur G. Soient $\mathscr{C}(\mathrm{G})$ toutes les fonctions continues sur G et $\mathscr{D}(\mathrm{G})$ toutes les mesures sur G. (Une *mesure* est une fonction linéaire continue sur $\mathscr{C}(\mathrm{G})$.) La *transformation de Fourier*, dans le sens de la Théorie de Probabilité par exemple, est le plongement

$$\mathscr{D}(\mathrm{G}) \to \mathscr{C}(\hat{\mathrm{G}})$$
$$\mu \mapsto \mu_{\restriction}\hat{\mathrm{G}}$$

qui restreint une mesure de toutes les fonctions continues sur G à tous les caractères continus sur G. Elle est un homomorphisme d'algèbres topologiques ; en particulier la transformation de Fourier traduit le produit de convolution sur $\mathscr{D}(\mathrm{G})$ au produit point par point de $\mathscr{C}(\hat{\mathrm{G}})$.

Quant à notre Transformation de Fourier p-adique on trouve que

- les caractères sont paramétrés par une boule ouverte, et, ce qui était déjà énoncé,
- l'image de la Transformation de Fourier est donnée par toutes les fonctions analytiques qui convergent sur cette boule ouverte.

Décrivons d'abord l'origine historique de la base Mahler et de Fourier p-adique de la Théorie de Nombres.

Petit Interlude sur la Théorie des Corps de Classes Locales

La Théorie des Corps de Classes Locales paramètre le groupe de Galois de l'extension abélienne maximale $\mathbf{L}$ d'un corps local $\mathbf{K}$ avec $\mathbf{K}^*$. Une extension $\mathbf{E}$ d'un corps valu $\mathbf{F}$ est *totalement ramifiée* si $v(\mathbf{E}) : v(\mathbf{F}) = \mathbf{L} : \mathbf{F}$ et *non-ramifiée* si $v(\mathbf{E}) = v(\mathbf{F})$. Le groupe de Galois de $\mathbf{L}$ abélienne maximale est le produit

$$\mathrm{Gal}(\mathbf{L}) = \mathrm{Gal}(\mathbf{L}') \times \mathrm{Gal}(\mathbf{L}'')$$

des groupes de Galois de son sous-corps totalement ramifié $\mathbf{L}'$ et son sous-corps non-ramifié $\mathbf{L}''$. La partie facile est la paramétrisation du groupe de Galois de $\mathrm{Gal}(\mathbf{L}'')$ qui consiste en des puissances entières de l'homomorphisme qui induit le Frobenius sur les corps résiduels. La partie difficile est la paramétrisation du groupe de Galois de $\mathbf{L}'$.

Théorie des Corps de Classes sur les nombres p-adiques. Si $\mathbf{K} = \mathbb{Q}_p$, on a le théorème de Kronecker-Weber local.

Theorème. *L'extension totalement ramifiée abélienne maximale* $\mathbf{L}$ *de* $\mathbb{Q}_p$ *est obtenue par adjonction de toutes racines* ζ *d'ordre* p^n *pour un* n *dans* $\mathbb{N}$ *et*

$$\begin{aligned} \mathbb{Z}_p^* &\xrightarrow{\sim} \mathrm{Gal}(\mathbf{L}/\mathbb{Q}_p) \\ u &\mapsto [\zeta \mapsto \zeta^u]. \end{aligned}$$

On peut cela interpréter comme suit : L'anneau $\mathbb{Z}_p$ opère sur le groupe multiplicatif $1 + \mathrm{B}$, la boule d'unité ouverte autour de 1 de $\mathbb{C}_p^*$ par

$$z \cdot (1 + x) = (1 + x)^z := \sum \binom{z}{n} x^n.$$

L'extension maximale totalement ramifiée $\mathbf{L}$ de $\mathbb{Q}_p$ est le corps obtenu par adjonction de toute la torsion de l'opération de $\mathbb{Z}_p$ et l'opération de Galois sur $\mathbf{L}$ s'identifie avec l'opération de $\mathbb{Z}_p^*$ sur la torsion de l'opération de $\mathbb{Z}_p$.

Théorie des Corps de Classes sur un corps de nombres p-adiques. Si $\mathbf{K}$ est une extension finie de $\mathbb{Q}_p$, alors Lubin et Tâte dans [LT65] construisent une action $\mathbf{o}_{\mathbb{C}_p}$-analytique de $\mathbf{o}_{\mathbf{K}}$ sur B (et une opération de groupe $\mathbf{o}_{\mathbb{C}_p}$-analytique sur B compatible à l'action de $\mathbf{o}_{\mathbf{K}}$, c'est-à-dire B devient un $\mathbf{o}_{\mathbf{K}}$-module) tel que l'analogue suivant du théorème de Kronecker-Weber local est satisfait.

Theorème. *L'extension totalement ramifiée abélienne maximale* $\mathbf{L}$ *de* $\mathbf{K}$ *est obtenue par adjonction de toute la torsion de l'action de* $\mathbf{o}_{\mathbf{K}}$ *sur* B *et*

$$\begin{aligned} \mathbf{o}_{\mathbf{K}}^* &\xrightarrow{\sim} \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \\ u &\mapsto [t \mapsto [u]t]. \end{aligned}$$

Cette action est inspirée par la Théorie des Corps de Classes pour un corps de nombre quadratique imaginaire $\mathbf{F}$ qui se réalise à travers de l'opération de $\mathbf{F}$

sur une courbe elliptique C. L'extension abélienne maximale $\mathbf{E}$ de $\mathbf{F}$ est obtenue par adjonction de toute la torsion de l'opération de $\mathbf{o_F}$ sur C l'opération de Galois sur $\mathbf{E}$ s'identifie avec l'opération de $\mathbf{o_F^*}$ sur la torsion de l'opération de $\mathbf{o_F}$.

Les caractères du groupe de nombres p-adiques entiers

Theorème (Amice). *L'application*

$$\begin{aligned} \mathrm{B} &\to \hat{\mathbb{Z}}_p \\ z &\mapsto [x \mapsto (1+z)^x] \end{aligned}$$

entre la boule d'unité ouverte de $\mathbb{C}_p$ *et tous les caractères* $\chi\colon \mathbb{Z}_p \to \mathbb{C}_p^*$ *est une bijection.*

Alors les caractères de $\mathbb{Z}_p$ forment une variété analytique par l'identification

$$z \mapsto [x \mapsto (1+z)^x = \sum \binom{x}{n} z^n]$$

et Theorème 2.2 s'interprète comme suit : La transformation de Fourier

$$\mu \mapsto \mu_{\restriction \hat{\mathbb{Z}}_p}$$

a comme image toutes les fonctions analytiques sur B et

$$\mu_{\restriction \hat{\mathbb{Z}}_p} = [z \mapsto \sum \mu(\binom{\cdot}{n}) z^n]$$

Soit $\mathcal{G}$ le groupe B avec l'opération construite par Schneider et Teitelbaum.

Theorème (Schneider et Teitelbaum). *Il y a un homomorphisme* $t_0'\colon \mathcal{G} \to 1 + \mathrm{B}$ *tel que l'application*

$$\begin{aligned} \mathrm{B} &\to \hat{\mathbf{o}}_{\mathbf{K}} \\ z &\mapsto t_0' \circ [x \mapsto [x]z] \end{aligned}$$

entre la boule d'unité ouverte de $\mathbb{C}_p$ *et les caractères* $\chi\colon \mathbf{o_K} \to \mathbb{C}_p^*$ *est une bijection.*

Alors les caractères de $\mathbf{o_K}$ forment une variété analytique par l'identification

$$z \mapsto [x \mapsto t_0' \circ [x \mapsto [x]z] = \sum \mathrm{P}_n(x) z^n]$$

et Theorème 2.4 s'interprète comme suit : La transformation de Fourier

$$\mu \mapsto \mu_{\restriction \hat{\mathbf{o}}_{\mathbf{K}}}$$

a comme image toutes les fonctions analytiques sur B et

$$\mu_{\restriction \hat{\mathbf{o}}_{\mathbf{K}}} = [z \mapsto \sum \mu(P_n) z^n].$$

Remarquons que

— les polynômes $P_0, P_1, \ldots$ ont des valeurs dans $\mathbf{o}_{\mathbb{C}_p}$ parce que toutes les actions décrites sont analytiques sur $\mathbf{o}_{\mathbb{C}_p}$, et

— que le degré de P_n est n et a comme coefficient le plus haut $1/n!$ parce que $t_0' \circ [x \mapsto [x]z]$ est égal à $\exp(x \log_{\mathcal{G}}(z))$, où $\log_{\mathcal{G}} \colon \mathcal{G} \xrightarrow{\sim} \mathbb{G}_a$ est le logarithme du groupe de Lubin-Tate.

Références

[Ami64] Y. Amice, *Interpolation p-adique*, Bull. Soc. Math. France **92** (1964), 117–180. MR 0188199.

[LT65] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387. MR 0172878.

[Nag15] E. Nagel, *Fractional p-adic differentiability under the Amice transform*, Trends in number theory, Contemp. Math., vol. 649, Amer. Math. Soc., Providence, RI, 2015, pp. 185–201. MR 3415273. DOI 10.1090/conm/649/13026. Confer http://www.math.jussieu.fr/~nagel/publications/AmiceTransform.pdf.

[Nag18] ———, *p-adic Fourier theory of differentiable functions*, Doc. Math. **23** (2018), 939–967. MR 3861040. DOI 10.3934/dcdsb.2018049. Confer http://www.math.jussieu.fr/~nagel/publications/pAdicDiffFourier.pdf.

[ST01] P. Schneider and J. Teitelbaum, *p-adic Fourier theory*, Doc. Math. **6** (2001), 447–481 (electronic). MR 1871671.