Annales mathématiques du Québec (2024) 48:519–529
https://doi.org/10.1007/s40316-023-00215-2

La matrice de logarithme en termes de chiffres *p*-adiques

Florian Sprung[1]

Received: 7 January 2023 / Accepted: 3 February 2023 / Published online: 21 June 2023

Abstract
We give a new description of the logarithm matrix of a modular form in terms of distributions, generalizing the work of Dion and Lei for the case $a_p = 0$. What allows us to include the case $a_p \neq 0$ is a new definition, that of a distribution matrix, and the characterization of this matrix by p-adic digits. One can apply these methods to the corresponding case of distributions in multiple variables.

Résumé
Nous donnons une nouvelle description de la matrice de logarithme d'une forme modulaire en termes de distributions, généralisant le travail de Dion et Lei pour le cas $a_p = 0$. Ce qui nous permet d'inclure le cas $a_p \neq 0$ est une nouvelle définition, celle d'une matrice de distributions, et la caractérisation de cette matrice par des chiffres p-adiques. On peut appliquer ces méthodes au cas correspondant d'une distribution à plusieurs variables.

Mots Clés (Keywords) Distributions p-adiques (p-adic distributions) · Chiffres p-adiques (p-adic digits) · Théorie d'Iwasawa (Iwasawa theory) · Forme modulaire (modular form) · Courbe elliptique (elliptic curve)

Mathematics Subject Classification 11R23 · 26E30 · 11F85

1 Introduction

Soit $f = \sum_{n\geq 1}^{\infty} a_n q^n$ une forme parabolique de poids 2 propre pour les opérateurs de Hecke telle que $a_1 = 1$ et de Nebentypus ϵ. Soit p un nombre premier tel que p ne divise pas le niveau de f. Par exemple, on peut prendre pour f la forme associée à une courbe elliptique telle qu'elle ait bonne réduction en p (ordinaire ou supersingulière). Une construction due à Mazur–Swinnerton-Dyer, Amice–Vélu et Višik [1, 7, 14] nous permet d'associer des fonctions L p-adiques L_λ pour chaque racine λ du polynôme $X^2 - a_pX + \epsilon(p)p$ telle que $v_p(\lambda) < 1$, où v_p et la valuation p-adique telle que $v_p(p) = 1$.

✉ Florian Sprung
florian.sprung@asu.edu

1 School of Mathematical and Statistical Sciences, Arizona State University, Tempe, AZ 85287-1804, USA

Dans le cas ordinaire, où $v_p(\lambda) = 0$, on peut utiliser L_λ pour formuler une conjecture principale d'Iwasawa, voir par exemple [7]. Dans le cas supersingulier, où $v_p(\lambda) > 0$, la situation n'est pas idéale: Il y a deux choix α et β pour la racine λ, et les deux fonctions L_α et L_β sont analytiques, mais ne sont pas bornées sur le disque compact $\mathbb{Z}_p$ comme dans le cas ordinaire. Néanmoins, il existe une factorisation de type distribution=mesure × distribution

$$(L_\alpha, L_\beta) = (L_\sharp, L_\flat)\mathrm{Log}_{\mathrm{a_p}}$$

où $\mathrm{Log}_{\mathrm{a_p}}$ est une matrice de dimension 2×2. L'idée de considérer le vecteur (L_α, L_β) a ses origines dans les travaux de Perrin-Riou, voir par exemple [8]. Cette factorisation est un analogue de la factorisation

$$\zeta(s) = \widehat{\zeta}(s) \times \left(\pi^{s/2}\Gamma^{-1}(s/2)\right)$$

de la fonction zêta de Riemann en une fonction $\widehat{\zeta}(s)$ plus convenable et une fonction qui est responsable des zéros triviaux. Ce sont les zéros de $\widehat{\zeta}(s)$ qui sont intéressants, et on peut dire de même des fonctions $L_\sharp$ et $L_\flat$.[1] Comme les deux fonctions $L_\sharp$ et $L_\flat$ sont des fonctions analytiques bornées sur $\mathbb{Z}_p$, elles sont plus convenables pour formuler des conjectures principales en théorie d'Iwasawa, voir [4] pour le cas $a_p = 0$ et [13] pour le cas général pour les courbes elliptiques.

Les coefficients de $\mathrm{Log}_{\mathrm{a_p}}$ (la matrice de logarithme) sont des fonctions analytiques p-adiques asymptotiquement équivalentes à celles de L_α et L_β, voir [12, Section 4.3] pour les détails. Le nom de la matrice $\mathrm{Log}_{\mathrm{a_p}}$ provient du fait que

$$\det \mathrm{Log}_{\mathrm{a_p}}(1+T) = \log_p(1+T) \times (\text{un facteur simple}),$$

voir [12, Remark 4.4] pour ce facteur. Rappelons au lecteur que le logarithme p-adique s'écrit comme un produit infini comme suit[2]:

$$\log_p(1+T) = T \prod_{n \geq 1} \frac{\Phi_{p^n}(1+T)}{p},$$

où Φ_{p^n} est le p^n-ième polynôme cyclotomique.

Dans le cas $a_p = 0$, il existe une expression explicite pour les coefficients de $\mathrm{Log}_{\mathrm{a_p}}$ par les logarithmes p-adiques signés dus à Pollack [9] (où l'on considère deux analogues du produit infini comme ci-dessus, mais où l'on multiplie seulement les termes avec n impair ou pair). Dans [3], Dion et Lei ont pris une autre perspective pour ces logarithmes signés, celle des distributions.

On peut comprendre une fonction analytique par la transformée d'Amice–Mahler. Pour une distribution.[3] μ sur $\mathbb{Z}_p$ à valeurs dans $\mathbb{Q}_p(\alpha)$, on peut former une série formelle (convergeant sur $B(0, 1^-)$[4]) par la formule

$$A_\mu(T) = \int_{\mathbb{Z}_p} (1+T)^x \mu(x),$$

la transformée d'Amice–Mahler de μ. La transformée d'Amice–Mahler est l'analogue p-adique de la transformée de Mellin. Rappelons au lecteur que l'on peut exprimer la fonction

[1] Par exemple dans [11, 12], des invariants (d'Iwasawa) attachés aux fonctions $L_\sharp$ et $L_\flat$ contrôlent la croissance du groupe de Šafarevič–Tate le long de l'extension $\mathbb{Z}_p$-cyclotomique.

[2] Cela suit par exemple de [2, Corollaire IV2.20] ou [15, Proposition 5.6].

[3] distribution continue, si on suit la terminologie de [2, V.3.].

[4] c.-à-d. sur chaque boule de rayon < 1, où le centre est 0.

$\zeta(s)$ de Riemann pour $s > 1$ comme

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

et $\Gamma(s)\zeta(s)$ est la transformée de Mellin de $\frac{dt}{e^t-1}$.

Toujours dans le cas $a_p = 0$, Dion et Lei [3] ont donné une description concrète des distributions dont la transformée d'Amice–Mahler sont les logarithmes signés de Pollack.

Dans le cas général supersingulier, on peut définir $\mathrm{Log}_{\mathrm{a_p}}$ comme un produit infini de matrices [12] qui contiennent les polynômes cyclotomiques. Dans le cas ordinaire, seulement les termes de la première colonne convergent dans ce produit, et on définit $\mathrm{Log}_{\mathrm{a_p}}$ comme cette colonne.

Le résultat principal généralise le résultat de Dion–Lei et nous fournit une caractérisation de la matrice de distributions dont la transformée d'Amice–Mahler est $\mathrm{Log}_{\mathrm{a_p}}$. Cette caractérisation est plus simple que la définition de $\mathrm{Log}_{\mathrm{a_p}}$, et en un mot reflète si des chiffres p-adiques sont nuls ou non-nuls.

On sait que la matrice de distributions en question est déterminée par ses valeurs sur les ouverts $b + p^n\mathbb{Z}_p$ dans le disque p-adique. Le théorème de ce travail dit qu'on peut lire ces valeurs des chiffres p-adiques de b, en convertissant chaque chiffre en une matrice de dimension 2×2 (la *représentation chromatique* du chiffre). Pour simplifier la version du théorème dans l'introduction, on suppose ici que $\epsilon(p) = 1$:

Théorème 1.1 *Soit $b \in \mathbb{Z}_p$ tel que*

$$b \equiv b_0 + b_1 p^1 + \cdots b_{n-1} p^{n-1} \pmod{p^n} \text{ avec } b_i \in \{0, \cdots p-1\}.$$

On dénote par $m_1, \cdots, m_l$ les longueurs des chaînes des chiffres nuls[5]:

$$(b_0, \cdots b_{n-1}) = (\underbrace{0, \cdots, 0}_{m_1}, \neq 0, \underbrace{0, \cdots, 0}_{m_2}, \neq 0, \cdots, \neq 0, \underbrace{0, \cdots, 0}_{m_l})$$

Soit μ_{a_p} la matrice de distributions dont la transformée d'Amice–Mahler est $\mathrm{Log}_{\mathrm{a_p}}$.
Si $|a_p| > 0$, on a

$$\mu_{a_p}(b + p^n\mathbb{Z}_p) = \begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}^{m_1} \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}^{m_2} \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}^{m_l} R_n.$$

Si $|a_p| = 0$,

$$\mu_{a_p}(b + p^n\mathbb{Z}_p) = \textit{la première colonne du produit des matrices ci-dessus}.$$

De plus, cela caractérise μ_{a_p}.

Pour la définition de R_n, voir Sect. 2. Si $p \neq 2$, on a $R_n = \frac{1}{p^{2+n}} \begin{pmatrix} -\beta^{n+2} & -\alpha^{n+2} \\ \beta^{n+3+n} & \alpha^{n+3} \end{pmatrix}$.

[5] Par exemple, si les premiers deux chiffres ne sont pas nuls, c.-à-d.

$$(b_0, b_1, \cdots) = (\neq 0, \neq 0, \cdots),$$

on a $m_1 = m_2 = 0$.

Le théorème dit que dans la représentation chromatique du chiffre b, la matrice $\begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$ représente un chiffre non nul et la matrice $\begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}$ représente le chiffre 0.

Quelques observations sur le produit des matrices:

(1) Si b a deux chiffres *non nuls* consécutifs, la matrice $\mu_{a_p}(b + p^n\mathbb{Z}_p)$ est nulle:

$$\mu_{a_p}(b + p^n\mathbb{Z}_p) = \begin{cases} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{si } |a_p| > 0 \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} & \text{si} |a_p| = 0. \end{cases}$$

(2) Si $a_p = 0$, on a $\begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}^{m_i} \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ pour m_i pair. Par conséquent, si un nombre pair de 0s sépare deux chiffres non nuls, on a automatiquement $\mu_{a_p}(b + p^n\mathbb{Z}_p) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Mais si $m_2, \cdots, m_l$ sont tous impairs, le produit n'est pas $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. (On obtient $\begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix} R_n$ ou $\begin{pmatrix} 0 & 0 \\ 0 & \pm 1 \end{pmatrix} R_n$.) C'est-à-dire, la matrice $\mu_{a_p}(b + p^n\mathbb{Z}_p)$ peut être non nulle si et seulement si tous les chiffres de position impaire de b sont 0 ou tous les chiffres de position paire le sont. Cela explique la définition des ensembles $S_n^{\pm}$ dans [3].

Il y existe divers analogues de la matrice de logarithme qui jouent un rôle important dans les travaux de Lei, Loeffler, Zerbes et Büyükboduk (mais la construction est différente – ils utilisent la théorie de modules de Wach). Voir par exemple [10] pour une théorie récente. La question d'étudier leurs matrices de distributions provenant de la théorie des modules de Wach semble très intéressante.

Remerciements. Je remercie Cédric Dion, Antonio Lei, Bernadette Perrin-Riou, Jean-Pierre Serre, Joseph Silverman et la·le lecteur·trice expert·e pour leurs commentaires, en particulier JPS pour des conseils d'écriture.

2 Définition et propriétés de la matrice de logarithme

Nous rappelons la définition de la matrice de logarithme définie dans [12]. Soit $\Phi_{p^n}(X) = \sum_{i \geq 0}^{p-1} X^{ip^{n-1}}$ le p^n-ième polynôme cyclotomique. Nous dénotons $\epsilon(p)$ simplement par ε. On pose

$$\mathrm{Log_{a_p}}^{(n)}(1+T) := \begin{pmatrix} a_p & 1 \\ -\varepsilon\Phi_p(1+T) & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -\varepsilon\Phi_{p^2}(1+T) & 0 \end{pmatrix} \cdots \begin{pmatrix} a_p & 1 \\ -\varepsilon\Phi_{p^n}(1+T) & 0 \end{pmatrix} R_n$$

où R_n dénote la matrice de racines. Cette matrice dépend des racines α et β du polynôme $X^2 - a_pX + \varepsilon p = 0$ que l'on choisit telles que $|\alpha| \geq |\beta|$ pour une valeur absolue p-adique quelconque. La matrice R_n est définie par

$$R_n := \begin{pmatrix} a_p & 1 \\ -\varepsilon p & 0 \end{pmatrix}^{-2-n} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} = \frac{1}{p^{2+n}} \begin{pmatrix} -\beta^{2+n} & -\alpha^{2+n} \\ \beta^{3+n} & \alpha^{3+n} \end{pmatrix}$$

si $p \geq 3$, et

$$R_n := \begin{pmatrix} a_p & 1 \\ -\varepsilon p & 0 \end{pmatrix}^{-3-n} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} = \frac{1}{p^{3+n}} \begin{pmatrix} -\beta^{3+n} & -\alpha^{3+n} \\ \beta^{4+n} & \alpha^{4+n} \end{pmatrix}$$

si $p = 2$.[6]

Définition 2.1 Si $|a_p| > 0$, la matrice de logarithme est

$$\mathrm{Log}_{\mathrm{a_p}}(1+T) := \lim_{n\to\infty} \mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(1+T).$$

Si $|a_p| = 0$, la matrice de logarithme $\mathrm{Log}_{\mathrm{a_p}}(1+T)$ est la première colonne de

$$\lim_{n\to\infty} \mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(1+T).$$

Lemme 2.2 *Les termes de* $\mathrm{Log}_{\mathrm{a_p}}(1+T)$ *convergent vers des séries dans* $\mathbb{Q}_p(\alpha)[[T]]$*. De plus, on sait évaluer* $\mathrm{Log}_{\mathrm{a_p}}(1+T)$ *au point* $T = \zeta_k - 1$*, où* ζ_k *dénote une racine* p^k*-ième primitive:*

Si $|a_p| > 0$*, on a*

$$\mathrm{Log}_{\mathrm{a_p}}(\zeta_k) = \mathrm{Log}_{\mathrm{a_p}}{}^{(k)}(\zeta_k).$$

Si $|a_p| = 0$*, on a*

$$\mathrm{Log}_{\mathrm{a_p}}(\zeta_k) = \text{première colonne de } \mathrm{Log}_{\mathrm{a_p}}{}^{(k)}(\zeta_k).$$

Démonstration [12, Lemma 4.8] ou [13, Lemma 4.4]; l'observation clé est que $\Phi_{p^i}(\zeta_k) = p$ si $i > k$. □

3 Le théorème

Définition 3.1 La **transformée** d'Amice–Mahler d'une distribution μ sur $\mathbb{Z}_p$ à valeurs dans $\mathbb{C}_p$ est une série formelle

$$A_\mu(T) = \int_{\mathbb{Z}_p} (1+T)^x \mu(x).$$

La **transformée d'Amice–Mahler** d'une matrice $M = (\mu_{ij})$ des distributions μ_{ij} comme ci-dessus est la matrice

$$A_M(T) := \left(A_{\mu_{ij}}(T)\right).$$

On rappelle au lecteur qu'une distribution est déterminée par la transformée d'Amice–Mahler, voir [2, ThéorèmeV.3.11].

Théorème 3.2 *Soit* $b \in \mathbb{Z}_p$ *tel que*

$$b \equiv b_0 + b_1 p^1 + \cdots b_{n-1} p^{n-1} \pmod{p^n} \text{ avec } b_i \in \{0, \cdots p-1\}.$$

[6] Dans [3], tous les résultats nécessitent l'hypothèse $p > 2$. (La première formule [3, Formule 1] est incorrecte si $p = 2$. La formule correcte de Pollack est $L_\lambda = \log_p^- L_+ + \frac{1}{2}\log_p^+ L_-$ si $p = 2$, voir [9, Theorem 5.6].)

On dénote par $m_1, \cdots, m_l$ les longueurs des chaînes des chiffres nuls:

$$(b_0, \cdots b_{n-1}) = (\underbrace{0, \cdots, 0}_{m_1}, \neq 0, \underbrace{0, \cdots, 0}_{m_2}, \neq 0, \cdots, \neq 0, \underbrace{0, \cdots, 0}_{m_l})$$

Soit μ_{a_p} la matrice de distributions dont sa transformée d'Amice–Mahler est $\mathrm{Log}_{\mathrm{a_p}}$. *Alors on a, si $|a_p| > 0$,*

$$\mu_{a_p}(b + p^n\mathbb{Z}_p) = \begin{pmatrix} a_p & 1 \\ -\epsilon & 0 \end{pmatrix}^{m_1} \begin{pmatrix} 0 & 0 \\ -\epsilon & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -\epsilon & 0 \end{pmatrix}^{m_2} \begin{pmatrix} 0 & 0 \\ -\epsilon & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 0 \\ -\epsilon & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -\epsilon & 0 \end{pmatrix}^{m_l} R_n,$$

et si $|a_p| = 0$,

$$\mu_{a_p}(b + p^n\mathbb{Z}_p) = \textit{la première colonne du produit des matrices ci-dessus.}$$

De plus, la matrice μ_{a_p} est caractérisée par ce théorème.

Démonstration Soit $\mathbb{1}_{b+p^n\mathbb{Z}_p(x)}$ la fonction caractéristique de $b + p^n\mathbb{Z}_p$. On a

$$\mathbb{1}_{b+p^n\mathbb{Z}_p(x)} = \frac{1}{p^n} \sum_{\zeta \in \mu_{p^n}} \zeta^{x-b}.$$

Par conséquent,

$$\mu_{a_p}(b + p^n\mathbb{Z}_p) = \int_{\mathbb{Z}_p} \mathbb{1}_{b+p^n\mathbb{Z}_p}(x)\mu_{a_p}(x) = \sum_{\zeta \in \mu_{p^n}} \frac{1}{p^n} \int_{\mathbb{Z}_p} \zeta^{x-b} \mu_{a_p}(x)$$

$$= \frac{1}{p^n} \sum_{\zeta \in \mu_{p^n}} \zeta^{-b} \int_{\mathbb{Z}_p} \zeta^x \mu_{a_p}(x) = \frac{1}{p^n} \sum_{\zeta \in \mu_{p^n}} \zeta^{-b} \mathrm{Log}_{\mathrm{a_p}}(\zeta).$$

Pour calculer cette somme, on utilise la Proposition 3.4 ci-dessous. La caractérisation suit du fait que les entrées dans $\mathrm{Log}_{\mathrm{a_p}}$ (dans le cas supersingulier) et les entrées dans la première colonne de $\mathrm{Log}_{\mathrm{a_p}}$ (cas ordinaire) sont des distributions d'ordre $o(\log_p(1 + T))$, voir [12, Proposition 4.20]. □

Définition 3.3 Soit $b = b_0 + b_1 p^1 + \cdots b_{n-1} p^{n-1}$ avec $b_i \in \{0, \cdots, p-1\}$. Pour chaque b_i, on définit sa **représentation chromatique** par

$$Y_i = \begin{cases} \begin{pmatrix} a_p & 1 \\ -\varepsilon & 0 \end{pmatrix} & \mathrm{si} b_i = 0 \mathrm{et} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -\varepsilon & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -\varepsilon & 0 \end{pmatrix} & \mathrm{si} b_i \neq 0. \end{cases}$$

On définit la **représentation chromatique de** $b \pmod{p^n}$ comme le produit des représentations chromatiques des chiffres, c.-à-d.

$$Y_0 Y_1 \cdots Y_{n-1}.$$

Proposition 3.4 *Les valeurs de* $\mathrm{Log}_{\mathrm{a_p}}$ *en les racine d'unité de puissance p sont reliées à la représentation chromatique: On a*

$$\sum_{\zeta \in \mu_{p^n}} \zeta^{-b} \mathrm{Log}_{\mathrm{a_p}}(\zeta) = p^n Y_0 Y_1 \cdots Y_{n-1} R_n.$$

4 Démonstration de la Proposition 3.4

Lemme 4.1 *Soit*

$$P(x) = \sum_{i\geq -(p^n-1)}^{i\leq p^n-1} c_i x^i \in \mathbb{C}_p[x, x^{-1}],$$

où $\mathbb{C}_p$ dénote le corps des nombres complexes p-adiques. On a alors

$$\sum_{\zeta\in\mu_{p^n}} P(\zeta) = c_0 p^n.$$

Démonstration On a $\sum_{\zeta\in\mu_{p^n}} \zeta^k = \begin{cases} p^n & \text{si } k \equiv 0 \mod p^n \\ 0 & \text{sinon.} \end{cases}$ □

Démonstration de la Proposition 3.4 Il suit du Lemme 2.2 que pour $\zeta \in \mu_{p^n}$

$$\zeta^{-b}\mathrm{Log}_{\mathrm{a_p}}(\zeta) = \zeta^{-b}\mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(\zeta),$$

alors chaque terme est de la forme $P(\zeta)$ pour des polynômes de Laurent $P(x)$ comme dans le Lemme 4.1 (où l'on autorise les puissances négatives). En appliquant ce lemme 4.1, on voit que

$$\sum_{\zeta\in\mu_{p^n}} \zeta^{-b}\mathrm{Log}_{\mathrm{a_p}}(\zeta) = p^n \times \text{ matrice des termes constants dans } x^{-b}\mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(x).$$

Montrons alors que les termes constants sont donnés comme dans l'énoncé de la proposition. Posons

$$\phi_i(x) := \begin{pmatrix} 1 & 0 \\ 0 & \Phi_{p^i}(x) \end{pmatrix} \text{ et } Y := \begin{pmatrix} a_p & 1 \\ -\varepsilon & 0 \end{pmatrix}.$$

Par définition, on a

$$\mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(x) = \phi_0(x)Y\phi_1(x)\cdots Y\phi_{n-1}(x)YR_n,$$

et aussi

$$x^{-b} = x^{-b_0}x^{-b_1p}\cdots x^{-b_{n-1}p^{n-1}}.$$

En combinant ces deux observations, on a

$$x^{-b}\mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(x) = x^{-b_0}\phi_0(x)Yx^{-b_1p}\phi_1(x)\cdots Yx^{-b_{n-1}p^{n-1}}\phi_{n-1}(x)YR_n.$$

En notant que

$$x^{-b_ip^i}\phi_{i+1}(x) = \begin{pmatrix} x^{-b_i}p^i & 0 \\ 0 & \sum_{k\geq 0}^{p-1} x^{(k-b_i)p^i} \end{pmatrix},$$

on voit que les termes dans $x^{-b}\mathrm{Log}_{\mathrm{a_p}}{}^{(n)}(x)$ sont des combinaisons linéaires des termes de la forme $x^{j_ip^i}$ avec $j_i \in \{-(p-1), \cdots, 0, \cdots (p-1)\}$.

Mais on cherche les termes constants, c.-à-d. la contribution des (multiples des) termes $x^{j_ip^i}$ avec $j_i = 0$.

Comme il n'y a pas d'annulation des puissances de x dans les divers termes de la forme $x^{-b_i p^i}\phi_i(x)Y$, on peut analyser chaque terme $x^{-b_i p^i}\phi_i(x)Y$ pour ses contributions au terme constant:

Cette contribution est $$Y_i = \begin{cases} 1 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times Y & \text{si } b_i = 0 \\ x^{-b_i p^i} \times \begin{pmatrix} 0 & 0 \\ 0 & x^{b_i p^i} \end{pmatrix} \times Y & \text{si } b_i \neq 0. \end{cases}$$ □

5 Généralisation au cas à plusieurs variables

On généralise le résultat principal au cas de k variables, généralisant [3, Section 4] où $k = 2$ et $a_p = 0$. Dans tout ce qui suit, on suppose que $k \geq 2$. Dans [5], Lei a étudié des matrices de logarithmes à deux variables ($k = 2$) en appliquant le produit tensoriel. Nous rappelons la convention pour les cas étudiés dans les dernières sections.

Exemple 5.1 Soit M une matrice. Deux exemples pour le produit tensoriel sont

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes M := \begin{pmatrix} a_{11}M & a_{12}M \\ a_{21}M & a_{22}M \end{pmatrix} \text{ et } \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} \otimes M := \begin{pmatrix} a_{11}M \\ a_{21}M \end{pmatrix}.$$

On dénote les vecteurs à k coordonnées par des lettres grasses, par exemple

$$\mathbf{x} = (x_1, \cdots, x_k) \text{ et } \mathbf{T} := (T_1, \cdots, T_k).$$

Définition 5.2 Pour une distribution μ sur $\mathbb{Z}_p^k$ à valeurs dans $\mathbb{C}_p$, on définit la transformée d'Amice–Mahler comme la série formelle

$$A_\mu(\mathbf{T}) := \int_{\mathbb{Z}_p^k} (1+T_1)^{x_1}(1+T_2)^{x_2}\cdots(1+T_k)^{x_k}\mu(\mathbf{x}).$$

Pour une matrice (μ_{ij}) de telles distributions on définit la transformée d'Amice–Mahler comme la matrice

$$\left(A_{\mu_{ij}}(\mathbf{T})\right).$$

Définition 5.3 Soit $\mu_{a_p}^{\otimes k}$ la matrice de distributions telle que la transformée d'Amice–Mahler est

$$\mathrm{Log}_{\mathrm{a_p}}(T_1) \otimes \mathrm{Log}_{\mathrm{a_p}}(T_2) \otimes \cdots \otimes \mathrm{Log}_{\mathrm{a_p}}(T_k).$$

Pour l'existence et l'unicité de $\mu_{a_p}^{\otimes k}$, voir [6, Theorem 3].

Pour $\mathbf{b} = (b_1, \cdots, b_k)$ et $\mathbf{n} = (n_1, \cdots, n_k)$, on écrit $\mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p$ pour l'ouvert

$$(b_1 + p^{n_1}\mathbb{Z}_p, \cdots, b_k + p^{n_k}\mathbb{Z}_p)$$

dans $\mathbb{Z}_p^k$.

Nous rappelons au lecteur que $\mu_{a_p}(b_i + p_i^n\mathbb{Z}_p)$ est une matrice de dimension 2×2.

Proposition 5.4 *Pour* $\mathbf{b} = (b_1, \cdots, b_k)$ *et* $\mathbf{n} = (n_1, \cdots, n_k)$ *comme ci-dessus, on a*

$$\mu_{a_p}^{\otimes k}(\mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p) = \mu_{a_p}(b_1 + p^{n_1}\mathbb{Z}_p) \otimes \mu_{a_p}(b_2 + p^{n_2}\mathbb{Z}_p) \otimes \cdots \otimes \mu_{a_p}(b_k + p^{n_k}\mathbb{Z}_p).$$

***Démonstration de la Proposition* 5.4** Par linéarité, cela suit de l'analogue de cette proposition pour le cas où les matrices sont de dimension 1×1. Cet analogue est la Proposition 6.1 (Multiplicativité) ci-dessous. □

Pour $b \in \mathbb{Z}_p$ et $n \in \mathbb{N}$, écrivons les longueurs des chaînes des chiffres dans le développement p-adique modulo p^n comme dans le Théorème 3, c.-à.-d. soient

$$\text{chiffres de } b \pmod{p^n} = (\underbrace{0, \cdots, 0}_{m_1}, \neq 0, \underbrace{0, \cdots, 0}_{m_2}, \neq 0, \cdots, \neq 0, \underbrace{0, \cdots, 0}_{m_l}).$$

Définition 5.5 Si $|a_p| > 0$ (cas supersingulier), la **représentation chromatique normalisée** de $b \pmod{p^n}$ est

$$M_{a_p}(b + p^n) := \begin{pmatrix} a_p & 1 \\ -\varepsilon & 0 \end{pmatrix}^{m_1} \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -\varepsilon & 0 \end{pmatrix}^{m_2} \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -\varepsilon & 0 \end{pmatrix}^{m_l} R_n.$$

Si $|a_p| = 0$, on définit la représentation normalisée chromatique $M_{a_p}(b+p^n)$ de $b \pmod{p^n}$ comme la première colonne du produit des matrices ci-dessus.

Corollaire 5.6 *Sous les hypothèses de la Proposition 5.4, les valeurs de $\mu_{a_p}^{\otimes k}$ sont données par des produits tensoriels des représentations chromatiques:*

$$\mu_{a_p}^{\otimes k}(\mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p) = M_{a_p}(b_1 + p^{n_1}) \otimes M_{a_p}(b_2 + p^{n_2}) \otimes \cdots \otimes M_{a_p}(b_k + p^{n_k}).$$

6 La Proposition 6.1 (Multiplicativité)

Nous introduisons une notation convenable pour discuter des vecteurs composés des $k - 1$ premières coordonnées des vecteurs comme $\mathbf{x}$ avec k coordonnées. On les dénote avec des lettres grasses avec une apostrophe, par exemple

$$\mathbf{x}' = (x_1, \cdots, x_{k-1}) \text{ et } \mathbf{T}' := (T_1, \cdots, T_{k-1}).$$

On pose aussi $\mathbf{b}' + p^{\mathbf{n}'}\mathbb{Z}_p$ pour l'ouvert

$$(b_1 + p^{n_1}\mathbb{Z}_p, \cdots, b_{k-1} + p^{n_{k-1}}\mathbb{Z}_p)$$

dans $\mathbb{Z}_p^{k-1}$.

Proposition 6.1 *(Multiplicativité) Soient $\mu(\mathbf{x})$, $\mu_1(\mathbf{x}')$, $\mu_2(x_k)$ des distributions sur $\mathbb{Z}_p^k$, $\mathbb{Z}_p^{k-1}$ et $\mathbb{Z}_p$. Si*

$$A_\mu(\mathbf{T}) = A_{\mu_1}(\mathbf{T}') \times A_{\mu_2}(T_k),$$

on a

$$\mu(\mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p) = \mu_1(\mathbf{b}' + p^{\mathbf{n}'}\mathbb{Z}_p) \times \mu_2(b_k + p^{n_k}\mathbb{Z}_p).$$

Étant donné deux vecteurs de même dimension, on définit leur puissance comme le vecteur des puissances des coordonnées. Par exemple pour $\mathbf{v} = (v_1, \cdots, v_k)$ et $\mathbf{w} = (w_1 \cdots, w_k)$,

$$\mathbf{v}^{\mathbf{w}} := (v_1^{w_1}, \cdots, v_k^{w_k}).$$

On définit aussi, pour $\mathbf{n} = (n_1, \cdots n_k)$,

$$p^{\mathbf{n}} := (p^{n_1}, \cdots, p^{n_k}).$$

Étant donné un vecteur, on définit sa pseudo-norme, dénotée $\|\cdot\|$, comme le produit de ses coordonnées, par exemple $\|p^{\mathbf{n}}\| = p^{n_1+n_2+\cdots+n_k}$.

On définit

$$\boldsymbol{\mu} := \mu_{p^{n_1}} \times \cdots \mu_{p^{n_k}}.$$

Lemme 6.2 *Soit* $\mathbf{m} \in \mathbb{Z}_p^k$. *On a* $\left\|\sum_{\zeta\in\boldsymbol{\mu}} \boldsymbol{\zeta}^{\mathbf{m}}\right\| = \sum_{\zeta\in\boldsymbol{\mu}} \|\boldsymbol{\zeta}^{\mathbf{m}}\|$.

Démonstration Pour des ensembles finis I et J, on a

$$\left(\sum_{i\in I} x_i\right)\left(\sum_{j\in J} y_j\right) = \sum_{(i,j)\in I\times J} x_i y_j.$$

□

On rappelle au lecteur que l'apostrophe signifie qu'on a tronqué la dernière coordonnée. Dans ce cas, on définit la puissance $\mathbf{v}'^{\mathbf{w}'}$, pseudo-norme, etc. d'une façon analogique. (Noter $k \geq 2$).

On dénote la fonction caractéristique de $\mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p$ sur $\mathbb{Z}_p^k$ par $\mathbb{1}_{\mathbf{b}+p^{\mathbf{n}}\mathbb{Z}_p}$:

$$\mathbb{1}_{\mathbf{b}+p^{\mathbf{n}}\mathbb{Z}_p}(x) = \begin{cases} 1 & \text{si } x \in \mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p \\ 0 & \text{si non.} \end{cases}$$

Lemme 6.3 *On a* $\int_{\mathbb{Z}_p^k} \mathbb{1}_{\mathbf{b}+p^{\mathbf{n}}\mathbb{Z}_p}\mu(\mathbf{x}) = \frac{1}{\|p^{\mathbf{n}}\|}\left\|\sum_{\zeta\in\boldsymbol{\mu}} \boldsymbol{\zeta}^{\mathbf{x}-\mathbf{b}}\right\|$.

Démonstration Cela suit du cas à une variable par induction:

On a

$$\begin{aligned} \mathbb{1}_{\mathbf{b}+p^{\mathbf{n}}\mathbb{Z}_p}\mu(\mathbf{x}) &= \mathbb{1}_{\mathbf{b}'+p^{\mathbf{n}'}\mathbb{Z}_p}\mu(\mathbf{x}') \times \mathbb{1}_{b_k+p^{n_k}\mathbb{Z}_p}\mu(x_k) \\ &= \frac{1}{\|p^{\mathbf{n}'}\|}\sum_{\boldsymbol{\zeta}'\in\boldsymbol{\mu}'}\left\|\boldsymbol{\zeta}'^{\mathbf{x}'-\mathbf{b}'}\right\| \frac{1}{p^{n_k}}\sum_{\zeta\in\mu_{p^k}}\left\|\zeta^{x_k-b_k}\right\| \\ &= \frac{1}{\|p^{\mathbf{n}}\|}\left\|\sum_{\zeta\in\boldsymbol{\mu}}\boldsymbol{\zeta}^{\mathbf{x}-\mathbf{b}}\right\| \text{ par la démonstration du Lemme 6.2.} \end{aligned}$$

□

***Démonstration de la Proposition* 6.1**

$$\begin{aligned} \mu(\mathbf{b} + p^{\mathbf{n}}\mathbb{Z}_p) &= \int_{\mathbb{Z}_p^k} \mathbb{1}_{\mathbf{b}+p^{\mathbf{n}}\mathbb{Z}_p}\mu(\mathbf{x}) \\ &= \frac{1}{\|p^{\mathbf{n}}\|}\int_{\mathbb{Z}_p^k}\left\|\sum_{\zeta\in\boldsymbol{\mu}}\boldsymbol{\zeta}^{\mathbf{x}-\mathbf{b}}\right\|\mu(\mathbf{x}) \quad \text{(par le Lemme 6.3)} \\ &= \frac{1}{\|p^{\mathbf{n}}\|}\sum_{\zeta\in\boldsymbol{\mu}}\int_{\mathbb{Z}_p^k}\left\|\boldsymbol{\zeta}^{\mathbf{x}-\mathbf{b}}\right\|\mu(\mathbf{x}) \quad \text{(par le Lemme 6.2)} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\|p^{\mathbf{n}}\|} \sum_{\boldsymbol{\zeta}\in\boldsymbol{\mu}} \left\| \boldsymbol{\zeta}^{-\mathbf{b}} \right\| \int_{\mathbb{Z}_p^k} \|\boldsymbol{\zeta}^{\mathbf{x}}\| \, \mu(\mathbf{x}) \\
&= \frac{1}{\|p^{\mathbf{n}}\|} \sum_{\boldsymbol{\zeta}\in\boldsymbol{\mu}} \left\| \boldsymbol{\zeta}^{-\mathbf{b}} \right\| A_\mu(\boldsymbol{\zeta}) \\
&= \frac{1}{\|p^{\mathbf{n}}\|} \sum_{\boldsymbol{\zeta}'\times\zeta\in\boldsymbol{\mu}'\times\mu_{p^{n_k}}} \left\| \boldsymbol{\zeta}'^{(-\mathbf{b}')} \right\| \zeta^{-b_k} A_{\mu'}(\boldsymbol{\zeta}') A_\mu(\zeta) \\
&= \frac{1}{\|p^{\mathbf{n}'}\|} \sum_{\boldsymbol{\zeta}'\in\boldsymbol{\mu}'} \left\| \boldsymbol{\zeta}'^{(-\mathbf{b}')} \right\| A_{\mu'}(\boldsymbol{\zeta}') \frac{1}{p^{n_k}} \sum_{\zeta\in\mu_{p^k}} \left\| \zeta^{-b_k} \right\| A_\mu(\zeta) \\
&= \mu_1(\mathbf{b}' + p^{\mathbf{n}'}\mathbb{Z}_p) \times \mu_2(b_k + p^{n_k}\mathbb{Z}_p).
\end{aligned}
$$

Pour l'avant-dernière égalité, on a appliqué l'analogue direct du Lemme 6.2 pour les dimensions $k-1$ et 1. □

Références

1. Yvette Amice et Jacques Vélu : Distributions p-adiques associées aux séries de Hecke. *Astérisque*, 24–25, 119–131, 1975.
2. Pierre Colmez: *Arithmétique de la fonction zêta, dans La fonction zêta*, pages 37–164. Ed. Éc. Polytech., Palaiseau, 2003.
3. Cédric Dion et Antonio Lei: Plus and minus logarithms and Amice transform. *C. R. Math. Acad. Sci. Paris*, 355(9), 942–948, 2017.
4. Shin-ichi Kobayashi: Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.*, 152(1), 1–36, 2003.
5. Antonio Lei: Factorisation of two-variable p-adic L-functions. *Canad. Math. Bull.*, 57(4), 845–852, 2014.
6. David Loeffler: p-adic integration on ray class groups and non-ordinary p-adic L-functions, dans *Iwasawa theory 2012*, volume 7 de *Contrib. Math. Comput. Sci.*, pages 357–378. Springer, Heidelberg, 2014.
7. Barry Mazur: Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18 183–266, 1972.
8. Bernadette Perrin-Riou: Arithmétique des courbes elliptiques à réduction supersingulière en p. *Experiment. Math.*, 12(2) 155–186, 2003.
9. Robert Pollack: On the p-adic L-function of a modular form at a supersingular prime. *Duke Math. J.*, 118(3) 523–558, 2003.
10. Gautier Ponsinet: On the structure of signed Selmer groups. *Math. Z.*, 294(3–4) 1635–1658, 2020.
11. Florian Sprung: The Šafarevič-Tate group in cyclotomic $\mathbb{Z}_p$-extensions at supersingular primes. *J. Reine Angew. Math.*, 681 199–218, 2013.
12. Florian Sprung: On pairs of p-adic L-functions for weight-two modular forms. *Algebra Number Theory*, 11(4) 885–928, 2017.
13. Florian E. Ito Sprung: Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures. *J. Number Theory*, 132(7) 1483–1506, 2012.
14. M. M. Višik: Nonarchimedean measures associated with Dirichlet series. *Mat. Sb. (N.S.)*, 99(141)(2) 248–260, 296, 1976.
15. Lawrence C. Washington: *Introduction to cyclotomic fields*, volume 83 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, deuxième édition, 1997.