Summer School on Modular Functions
ANTWERP 1972

Formes modulaires et fonctions zêta p-adiques

par Jean-Pierre SERRE

à Carl Ludwig Siegel
à l'occasion de son 76-ième anniversaire

Table des Matières

Introduction

Soient K un corps de nombres algébriques totalement réel, et ζ_K sa fonction zêta. D'après un théorème de Siegel [24], $\zeta_K(1-k)$ est un nombre rationnel si k est entier ≥ 1; il est $\neq 0$ si k est pair. Lorsque K est abélien sur $\mathbf{Q}$, on peut écrire ce nombre comme produit de "nombres de Bernoulli généralisés" :

$$\zeta_K(1-k) = \prod_\chi L(\chi, 1-k) = \prod_\chi (- b_k(\chi)/k), \qquad \text{cf. [18]},$$

où χ parcourt l'ensemble des caractères de $\mathbf{Q}$ attachés à K. Cela permet de démontrer des propriétés de congruence reliant les $\zeta_K(1-k)$ pour diverses valeurs de k, et d'en déduire par interpolation une fonction zêta p-adique pour le corps K, au sens de Kubota-Leopoldt (cf. [7], [10], [11], [16]).

Dans ce qui suit, je me propose d'étendre une partie de ces résultats au cas d'un corps totalement réel quelconque (non nécessairement abélien sur $\mathbf{Q}$). La méthode suivie est celle de Klingen [13] et Siegel [25], [26]. Elle consiste à utiliser le fait que $\zeta_K(1-k)$ est le terme constant d'une certaine forme modulaire sur $SL_2(\mathbf{Z})$ dont les autres termes se calculent par des formules simples (ce sont des combinaisons linéaires d'exponentielles en k). Tout revient donc à transférer les propriétés de ces termes au terme constant lui-même. On est amené, pour ce faire, à définir les "formes modulaires p-adiques", limites de formes modulaires au sens usuel (sur le groupe $SL_2(\mathbf{Z})$); de telles formes intervenaient déjà, au moins implicitement, dans les travaux d'Atkin sur les coefficients c(n) de l'invariant modulaire j, cf. [2]. L'étude de ces formes fait l'objet des §§ 1, 2 et 3; elle repose de façon essentielle sur le théorème

récent de Swinnerton-Dyer [27] donnant la structure de l'algèbre des formes modulaires (mod.p). Les principaux résultats sont les suivants :

a) Une forme modulaire p-adique a un poids qui est, non plus un entier, mais un élément d'un certain groupe p-adique $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, cf. n°1.4.

b) Si

$$f = \sum_{n=0}^{\infty} a_n(f)\, q^n$$

est une forme modulaire p-adique de poids $\neq 0$, il existe des formules donnant $a_0(f)$ en termes des $a_n(f)$, $n \geq 1$, cf. n°2.3.

c) Toute forme modulaire (au sens usuel) sur le groupe $\Gamma_0(p)$ est une forme modulaire p-adique, cf. §3.

Dans l'application aux fonctions zêta, on rencontre des familles (f_s) de formes modulaires p-adiques dépendant (ainsi que leur poids) d'un paramètre p-adique s. L'étude de ces familles fait l'objet du §4. Le cas le plus important est celui où les fonctions $s \longmapsto a_n(f_s)$, $n \geq 1$, appartiennent à l'algèbre d'Iwasawa Λ du n°4.1; on en déduit alors des propriétés analogues pour la fonction $s \longmapsto a_0(f_s)$, cf. n°s 4.6 et 4.7.

Une fois ces résultats établis, leur application à l'interpolation p-adique de ζ_K ne présente pas de difficultés; c'est l'objet du §5. La fonction zêta p-adique de K est définie au n° 5.3; ses principales propriétés sont données par les ths. 20, 21, et 22. De nombreuses questions restent ouvertes; on en trouvera une brève discussion au n°5.6.

§1. Formes modulaires p-adiques

1.1. Notations

a) Congruences

La lettre p désigne un nombre premier; on note v_p la valuation du corps p-adique $\mathbf{Q}_p$, normée de telle sorte que $v_p(p) = 1$; un élément x de $\mathbf{Q}_p$ est dit p-entier s'il appartient à $\mathbf{Z}_p$, i.e. si $v_p(x) \geq 0$.

Si $f = \sum a_n q^n \in \mathbf{Q}_p[[q]]$ est une série formelle en une indéterminée q, on pose

$$v_p(f) = \inf . v_p(a_n).$$

Ainsi, $v_p(f) \geq 0$ signifie que $f \in \mathbf{Z}_p[[q]]$. Lorsque $v_p(f) \geq m$, on écrit aussi $f \equiv 0 \pmod{p^m}$.

Soit (f_i) une suite d'éléments de $\mathbf{Q}_p[[q]]$. On dit que f_i tend vers f si les coefficients de f_i tendent uniformément vers ceux de f, i.e. si $v_p(f - f_i) \to +\infty$.

b) Séries d'Eisenstein

Si k est un entier pair ≥ 2, nous poserons

$$G_k = -b_k/2k + \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n \qquad (q = e^{2\pi i z}),$$

$$E_k = -\frac{2k}{b_k} G_k = 1 - \frac{2k}{b_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n,$$

où b_k désigne le k-ième nombre de Bernoulli et $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. Si $k \geq 4$, G_k et E_k sont des formes modulaires de poids k (relativement au groupe $SL_2(\mathbf{Z})$).

c) Les séries P,Q,R

On pose, avec Ramanujan,

$$P = E_2 = 1 - 24 \sum \sigma_1(n)\, q^n$$

$$Q = E_4 = 1 + 240 \sum \sigma_3(n)\, q^n$$

$$R = E_6 = 1 - 504 \sum \sigma_5(n)\, q^n.$$

Les séries Q et R engendrent l'algèbre graduée des formes modulaires : toute forme modulaire de poids k s'écrit de façon unique comme polynôme isobare de poids k en Q et R. Par exemple :

$$E_8 = Q^2, \quad E_{10} = QR, \quad E_{12} = \frac{441\, Q^3 + 250\, R^2}{691}, \quad E_{14} = Q^2R,$$

$$\Delta = 2^{-6}3^{-3}(Q^3 - R^2) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

La série P n'est pas une forme modulaire au sens habituel. Toutefois nous démontrerons plus loin (cf. n° 2.1) que c'est une "forme modulaire p-adique" de poids 2.

d) Exemples de congruences

D'après Kummer, $b_k/2k$ est p-entier si et seulement si k n'est pas divisible par p - 1; on a alors $v_p(G_k) = 0$. De plus, si $k' \equiv k \pmod{(p-1)}$, on a $b_k/2k \equiv b_{k'}/2k' \pmod{p}$; comme la congruence analogue pour $\sigma_{k-1}(n)$ est évidente, on en conclut que :

$$G_k \equiv G_{k'} \pmod{p} \quad \text{si } k' \equiv k \not\equiv 0 \pmod{(p-1)}.$$

(Plus généralement, il semble que toute congruence sur les nombres de Bernoulli puisse être étendue en une congruence sur les G_k.)

Lorsque k, par contre, est divisible par p - 1, le théorème de Clausen-von Staudt montre que $v_p(b_k/k) = -1 - v_p(k)$. On a donc $v_p(k/b_k) \geq 1$, d'où :

$$E_k \equiv 1 \pmod{p} \qquad \text{si } k \equiv 0 \pmod{(p-1)}.$$

Plus précisément :

$$E_k \equiv 1 \pmod{p^m} \iff k \equiv 0 \pmod{(p-1)p^{m-1}} \quad \text{si } p \neq 2$$

$$E_k \equiv 1 \pmod{2^m} \iff k \equiv 0 \pmod{2^{m-2}}.$$

1.2. L'algèbre des formes modulaires (mod.p)

Si $k \in \mathbf{Z}$, notons M_k l'ensemble des formes modulaires

$$f = \sum_{n=0}^{\infty} a_n q^n,$$

de poids k, dont les coefficients a_n sont rationnels et p-entiers. Si $f \in M_k$, la réduction $\tilde{f}$ de f modulo p appartient à l'algèbre $\mathbf{F}_p[[q]]$ des séries formelles à coefficients dans $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. L'ensemble des séries ainsi obtenues sera noté $\tilde{M}_k$. On pose

$$\tilde{M} = \sum_{k \in \mathbf{Z}} \tilde{M}_k ;$$

c'est une sous-algèbre de $\mathbf{F}_p[[q]]$, appelée algèbre des formes modulaires (mod.p). La structure de $\tilde{M}$ a été déterminée par Swinnerton-Dyer [27]. Rappelons brièvement le résultat (pour plus de détails, voir [20] ou [27]) :

(i) Le cas $p \geq 5$

On a vu (n° 1.1) que $E_{p-1} \equiv 1 \pmod{p}$, autrement dit $\tilde{E}_{p-1} = 1$. La multiplication par E_{p-1} applique M_k dans M_{k+p-1}, et l'on en déduit des inclusions :

$$\tilde{M}_k \subset \tilde{M}_{k+p-1} \subset \ldots \subset \tilde{M}_{k+n(p-1)} \subset \ldots$$

Si $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$, notons $\tilde{M}^{\alpha}$ la réunion des $\tilde{M}_k$, pour k parcourant α. L'un des résultats de Swinnerton-Dyer est que $\tilde{M}$ est somme directe des $\tilde{M}^{\alpha}$,

pour $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$; en d'autres termes, $\tilde{M}$ est une algèbre graduée, de groupe des degrés $\mathbf{Z}/(p-1)\mathbf{Z}$; on a $\tilde{M}^{\alpha} = 0$ si α est impair, i.e. non divisible par 2 dans $\mathbf{Z}/(p-1)\mathbf{Z}$. De plus, $\tilde{M}$ s'identifie au quotient de l'algèbre de polynômes $F_p[Q,R]$ par l'idéal principal engendré par $\tilde{A} - 1$, où $\tilde{A}(Q,R)$ est le polynôme isobare de poids $p - 1$ obtenu par réduction (mod.p) à partir du polynôme A tel que $E_{p-1} = A(Q,R)$. (En termes imagés, la relation $\tilde{E}_{p-1} = 1$ est "la seule relation" entre formes modulaires (mod.p).)

Cette description de $\tilde{M}$ montre que $\tilde{M}$ (resp. sa sous-algèbre $\tilde{M}^{\circ}$) est l'algèbre affine d'une courbe algébrique Y (resp. Y°) qui est lisse sur F_p; on trouvera une interprétation "géométrique" de Y et de Y° dans [20], p.416-05; notons seulement ici que $\tilde{M}$ et $\tilde{M}^{\circ}$ sont des anneaux de Dedekind, puisque Y et Y° sont lisses.

Exemples

- Pour $p = 11$, on a $E_{p-1} = QR$, d'où :

$$\tilde{M} = F_{11}[Q,R]/(QR - 1) \quad \text{et} \quad \tilde{M}^{\circ} = F_{11}[Q^5,R^5]/(Q^5R^5 - 1).$$

Les courbes $Y = \mathrm{Spec}(\tilde{M})$ et $Y^{\circ} = \mathrm{Spec}(\tilde{M}^{\circ})$ sont des courbes de genre 0, ayant chacune deux points à l'infini, rationnels sur F_{11}.

- Pour $p = 13$, on a $E_{p-1} = \frac{441\,Q^3 + 250\,R^2}{691}$, d'où :

$$\tilde{M} = F_{13}[Q,R]/(Q^3 + 10R^2 - 11) \quad \text{et} \quad \tilde{M}^{\circ} = F_{13}[Q^3].$$

La courbe Y (resp. Y°) est une courbe de genre 1 (resp. de genre 0), ayant un seul point à l'infini, rationnel sur F_{13}.

(ii) Le cas $p = 2,3$

On a alors $\tilde{Q} = \tilde{R} = 1$. On en déduit facilement que $\tilde{M}$ s'identifie à l'algèbre de polynômes $F_p[\tilde{\Delta}]$, engendrée par la réduction (mod.p) de Δ. On a $\tilde{M}_{k-2} \subset \tilde{M}_k$ et même $\tilde{M}_{k-2} = \tilde{M}_k$ si k n'est pas divisible par 12. On convient que $\tilde{M}^{\circ} = \tilde{M}$.

1.3. Congruences (mod p^m) entre formes modulaires

THÉORÈME 1. Soit m un entier ≥ 1. Soient f et f' deux formes modulaires à coefficients rationnels, de poids k et k' respectivement. On suppose que $f \neq 0$ et que

$$v_p(f - f') \geq v_p(f) + m.$$

On a alors :

$$k' \equiv k \pmod{(p-1)p^{m-1}} \quad \text{si} \quad p \geq 3$$

$$k' \equiv k \pmod{2^{m-2}} \quad \text{si} \quad p = 2.$$

Quitte à multiplier f par un scalaire, on peut supposer que $v_p(f) = 0$, auquel cas l'hypothèse équivaut à :

$$f' \equiv f \pmod{p^m}.$$

En particulier, les coefficients de f et de f' sont p-entiers, et l'on a $\tilde{f} = \tilde{f}' \neq 0$. Si $p \geq 5$, on voit que $\tilde{f}$ et $\tilde{f}'$ appartiennent à la même composante $\tilde{M}^\alpha$ de l'algèbre $\tilde{M}$ (cf. n° 1.2), autrement dit, on a $k' \equiv k \pmod{(p-1)}$; la même congruence subsiste si $p = 2$ ou 3, puisque k' et k sont pairs. Le th.1 est donc démontré pour $m = 1$.

Supposons maintenant $m \geq 2$. Soit $h = k' - k$. Quitte à remplacer f' par

$$f'E_{(p-1)p^n}$$

avec n assez grand, on peut supposer que $h \geq 4$. La série d'Eisenstein E_h est alors une forme modulaire de poids h; comme h est divisible par p-1, on a $E_h \equiv 1 \pmod{p}$. Posons $r = v_p(h) + 1$ si $p \geq 3$ et $r = v_p(h) + 2$ si $p = 2$. Il nous faut montrer que $r \geq m$. Supposons que $r < m$. On a $f.E_h - f' = f - f' + f(E_h - 1)$.

Or $f - f' \equiv 0 \pmod{p^m}$ et $E_h - 1 \equiv 0 \pmod{p^r}$, cf. n° 1.1. On en conclut que $f.E_h - f' \equiv 0 \pmod{p^r}$ et que

$$p^{-r}(f.E_h - f') \equiv p^{-r}f(E_h - 1) \pmod{p}.$$

Or, d'après le théorème de Clausen-von Staudt, on a

$$p^{-r}(E_h - 1) = \lambda\phi, \quad \text{où} \quad \phi = \sum_{n=1}^{\infty} \sigma_{h-1}(n)q^n, \quad \text{et} \quad v_p(\lambda) = 0.$$

La congruence ci-dessus équivaut donc à

$$f\phi \equiv g \pmod{p},$$

où g est la forme modulaire $\lambda^{-1}p^{-r}(f.E_h - f')$, qui est de poids k'. Comme $\tilde{f} \neq 0$, ceci peut s'écrire $\tilde{\phi} = \tilde{g}/\tilde{f}$ et montre que $\tilde{\phi}$ appartient au corps des fractions de $\tilde{M}$; de plus, $\tilde{g}$ et $\tilde{f}$ ont même poids (mod.(p-1)); on en déduit que $\tilde{\phi}$ appartient au corps des fractions de $\tilde{M}^\circ$. Or, on a

$$\tilde{\phi} - \tilde{\phi}^p = \tilde{\psi}, \quad \text{avec} \quad \psi = \sum_{(p,n)=1} \sigma_{h-1}(n)q^n,$$

et on vérifie facilement que

$$\psi \equiv \theta^{h-1}\left(\sum_{n=1}^{\infty} \sigma_1(n)q^n\right), \quad \text{où} \quad \theta = q\, d/dq \quad \text{(cf. [27])}.$$

Pour tirer de là une contradiction, distinguons deux cas :

(i) $p \geq 5$.

On a alors

$$\tilde{\psi} = -\frac{1}{24}\,\theta^{h-1}(\tilde{P}) = -\frac{1}{24}\,\theta^{p-2}(\tilde{E}_{p+1}),$$

d'où $\tilde{\psi} \in \tilde{M}^\circ$, vu les propriétés de l'opérateur θ (cf. [20], [27]). L'équation $\tilde{\phi} - \tilde{\phi}^p = \tilde{\psi}$ montre que $\tilde{\phi}$ est entier sur $\tilde{M}^\circ$, donc appartient à $\tilde{M}^\circ$, puisque $\tilde{M}^\circ$ est intégralement clos; cela contredit le lemme de [20], p.416-11.

(ii) $p = 2$ ou 3.

On a alors $\tilde{\psi} = \tilde{\Delta}$, comme le montrent les congruences donnant $\tau(n)$ modulo 6. Or $\tilde{M} = \mathbf{F}_p[\tilde{\Delta}]$, et l'équation $X - X^p = \tilde{\Delta}$ est évidemment irréductible sur le corps $\mathbf{F}_p(\tilde{\Delta})$. On obtient encore une contradiction.

Remarques

1) Le fait que $\tilde{\phi}$ ne puisse pas appartenir au corps des fractions de $\tilde{M}^\circ$ peut aussi se démontrer par un argument de filtration, généralisant celui de [20], loc.cit.

2) Il serait intéressant de décrire géométriquement le revêtement cyclique de degré p de la courbe Y° (ou de la courbe Y) défini par l'équation $X - X^p = \tilde{\psi}$.

1.4. Formes modulaires p-adiques

a) Le groupe X

Soit m un entier ≥ 1 (resp. ≥ 2 si $p = 2$). Posons

$$X_m = \mathbf{Z}/(p-1)p^{m-1}\mathbf{Z} = \mathbf{Z}/p^{m-1}\mathbf{Z} \times \mathbf{Z}/(p-1)\mathbf{Z} \quad \text{si} \quad p \neq 2$$

et $$X_m = \mathbf{Z}/2^{m-2}\mathbf{Z} \quad \text{si} \quad p = 2.$$

Lorsque $m \to \infty$, les X_m forment de façon naturelle un système projectif; nous désignerons par X la limite projective de ce système. On a

$$X = \varprojlim X_m = \begin{cases} \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z} & \text{si} \quad p \neq 2 \\ \mathbf{Z}_2 & \text{si} \quad p = 2, \end{cases}$$

où $\mathbf{Z}_p$ est l'anneau des entiers p-adiques. Le groupe X est un groupe de Lie p-adique compact de dimension 1. L'homomorphisme canonique $\mathbf{Z} \to X$

est injectif; nous l'utiliserons pour identifier $\mathbf{Z}$ à un sous-groupe dense de X.

Il y a souvent intérêt à considérer les éléments de X comme des caractères (p-adiques) du groupe $\mathbf{Z}_p^*$ des unités p-adiques. De façon plus précise, soit V_p le groupe des endomorphismes continus de $\mathbf{Z}_p^*$, muni de la topologie de la convergence uniforme. On vérifie facilement que l'application naturelle de $\mathbf{Z}$ dans V_p se prolonge en un homomorphisme continu $\varepsilon : X \to V_p$. Cet homomorphisme est injectif si $p = 2$, et bijectif si $p \neq 2$. Si $k \in X$, et $v \in \mathbf{Z}_p$, on note v^k le transformé de v par l'endomorphisme $\varepsilon(k)$ de $\mathbf{Z}_p$. Si l'on écrit $k = (s,u)$, avec $s \in \mathbf{Z}_p$, $u \in \mathbf{Z}/(p-1)\mathbf{Z}$, et si l'on décompose v en $v_1 v_2$, avec $v_1^{p-1} = 1$ et $v_2 \equiv 1$ (mod.p), on a $v^k = v_1^k v_2^k = v_1^u v_2^s$.

Un élément $k \in X$ est dit pair s'il appartient au sous-groupe 2X, i.e. si $(-1)^k = 1$. Lorsque $p \neq 2$, cela signifie que la seconde composante u de k est un élément pair de $\mathbf{Z}/(p-1)\mathbf{Z}$; lorsque $p = 2$, cela signifie que k appartient à $2\mathbf{Z}_2$.

b) Définition des formes modulaires p-adiques

Une forme modulaire p-adique est une série formelle

$$f = \sum_{n=0}^{\infty} a_n q^n,$$

à coefficients $a_n \in \mathbf{Q}_p$, possédant la propriété suivante :

(*) Il existe une suite f_i de formes modulaires à coefficients rationnels, de poids k_i, telle que $\lim.f_i = f$.

(Rappelons, cf. n° 1.1, que $\lim.f_i = f$ signifie que $v_p(f_i - f)$ tend vers $+\infty$, i.e. que les coefficients des f_i tendent uniformément vers ceux de f.)

Remarque. La définition ci-dessus est la définition originale donnée dans [21]. On en trouvera une interprétation "géométrique" (ainsi qu'une généralisation) dans le texte de Katz [12].

c) Poids d'une forme modulaire p-adique

THÉORÈME 2. Soit f une forme modulaire p-adique $\neq 0$, et soit (f_i) une suite de formes modulaires de poids (k_i), à coefficients rationnels, ayant pour limite f. Les k_i ont alors une limite dans le groupe $X = \varprojlim X_m$; cette limite dépend de f, mais pas de la suite (f_i) choisie.

Par hypothèse, on a $v_p(f_i - f_j) \to +\infty$; d'autre part, les $v_p(f_i)$ sont égaux à $v_p(f)$ pour i assez grand. En appliquant le th.1, on en déduit que, pour tout $m \geq 1$, l'image de la suite k_i dans X_m est stationnaire; cela signifie que les k_i ont une limite k dans X. Le fait que cette limite ne dépende pas de la suite choisie est immédiat.

La limite k des k_i est appelée le poids de f; c'est un élément pair de X. On convient que 0 est de poids k, quel que soit $k \in 2X$. Avec cette convention, les formes modulaires p-adiques de poids donné forment un $\mathbb{Q}_p$-espace vectoriel (et même un espace de Banach p-adique pour la norme définie par v_p).

Si des formes modulaires p-adiques f_i, de poids $k_i \in 2X$, tendent vers une série formelle f, celle-ci est une forme modulaire p-adique. De plus, si $f \neq 0$, les k_i ont une limite k dans X, et f est de poids k; cela se déduit du th.2, en approchant les f_i par des formes modulaires au sens usuel.

Exemple. Si $p = 2,3,5$, on a $Q \equiv 1 \pmod{p}$, d'où

$$\frac{1}{Q} = \lim_{m \to \infty} Q^{p^m - 1},$$

ce qui montre que 1/Q est modulaire p-adique, de même que la série $1/j = \Delta/Q^3$, qui est de poids 0. Il n'est d'ailleurs pas difficile de démontrer que (pour $p = 2,3,5$) une série f est modulaire p-adique de poids 0 si et seulement si elle s'écrit sous la forme

$$f = \sum_{n=0}^{\infty} b_n/j^n = \sum_{n=0}^{\infty} b_n \Delta^n Q^{-3n},$$

avec $b_n \in \mathbf{Q}_p$ et $v_p(b_n) \to +\infty$, et l'on a alors $v_p(f) = \inf. v_p(b_n)$.

Plus généralement, on aurait pu définir l'algèbre des formes modulaires p-adiques de poids 0 comme l'algèbre "de Tate" de la droite projective privée des disques ouverts de rayon 1 centrés aux valeurs "supersingulières" de j; c'est le point de vue adopté par Katz [12].

1.5. Premières propriétés des formes modulaires p-adiques

Si f est une forme modulaire p-adique, on a $v_p(f) \neq -\infty$, i.e. il existe une puissance p^N de p telle que $p^N f \in \mathbf{Z}_p[[q]]$; cela résulte de la définition, et du fait analogue pour les formes modulaires usuelles. De plus, le th.1 reste valable :

THÉORÈME 1'. *Soit* m *un entier* ≥ 1. *Soient* f *et* f' *deux formes modulaires p-adiques, non nulles, de poids* k, $k' \in X$ *respectivement. Si*

$$v_p(f - f') \geq v_p(f) + m,$$

k *et* k' *ont même image dans* X_m.

On écrit f (resp. f') comme limite de formes modulaires usuelles f_i (resp. f_i') de poids k_i (resp. k_i'). Pour i assez grand, on a

$$v_p(f_i) = v_p(f) = v_p(f') = v_p(f_i')$$

et
$$v_p(f_i - f_i') \geq v_p(f) + m,$$

ce qui, d'après le th.1, montre que k_i et k_i' ont même image dans X_m; le théorème en résulte.

COROLLAIRE 1. *Soit* $f = a_o + a_1 q + \ldots + a_n q^n + \ldots$ *une forme modulaire p-adique de poids* $k \in X$. *Soit* m *un entier* ≥ 0 *tel que l'image de* k *dans* X_{m+1} *soit* $\neq 0$. *On a alors*

$$v_p(a_o) + m \geq \inf_{n \geq 1}. \; v_p(a_n).$$

(En d'autres termes, si les a_n sont p-entiers pour $n \geq 1$, il en est de même de $p^m a_o$.)

Si $a_o = 0$, il n'y a rien à démontrer. Sinon, la fonction constante $f' = a_o$ est de poids 0, et l'on a

$$v_p(f - f') = \inf_{n \geq 1} v_p(a_n).$$

Comme les poids de f et f' ont des images différentes dans X_{m+1}, le th.1' montre que $v_p(f) + m + 1 > v_p(f - f')$, d'où le résultat cherché puisque $v_p(a_o) \geq v_p(f)$.

Remarque. Lorsque k n'est pas divisible par p-1, i.e. n'appartient pas au sous-groupe $\mathbf{Z}_p$ de X, on peut prendre $m = 0$ dans le corollaire précédent, et l'on en déduit que, si les a_n sont p-entiers pour $n \geq 1$, il en est de même de a_o.

COROLLAIRE 2. Soit

$$f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n$$

une suite de formes modulaires p-adiques, de poids $k^{(i)}$. Supposons que :

(a) les $a_n^{(i)}$, $n \geq 1$, tendent uniformément vers des $a_n \in \mathbf{Q}_p$;

(b) les $k^{(i)}$ tendent dans X vers une limite $k \neq 0$.

Alors les $a_o^{(i)}$ ont une limite $a_o \in \mathbf{Q}_p$, et la série

$$f = a_o + a_1 q + \ldots + a_n q^n + \ldots$$

est une forme modulaire p-adique de poids k.

Vu l'hypothèse $\lim k^{(i)} \neq 0$, on peut supposer qu'il existe un entier m tel que tous les $k^{(i)}$ aient une même image non nulle dans X_m. D'autre part, vu (a), il existe $t \in \mathbf{Z}$ tel que $v_p(a_n^{(i)}) \geq t$ pour tout $n \geq 1$, et tout i. D'après le cor.1, on a donc $v_p(a_o^{(i)}) > t - m$ pour tout i. Les $a_o^{(i)}$ forment donc une partie relativement compacte de $\mathbf{Q}_p$. Si (i_j) est

une suite extraite de (i) telle que $a_o^{(i_j)}$ converge vers un élément a_o de $\mathbf{Q}_p$, la série

$$f = \lim.f^{(i_j)} = a_o + a_1 q + \ldots + a_n q^n + \ldots$$

est évidemment modulaire p-adique de poids k. De plus, si (i'_j) est une autre suite extraite de (i) telle que $a_o^{(i'_j)}$ converge vers a'_o, la série $f' = a'_o + a_1 q + \ldots + a_n q^n + \ldots$ est également modulaire p-adique de poids k, et il en est de même de $f - f' = a_o - a'_o$. Comme $a_o - a'_o$ est aussi de poids 0, ce n'est possible que si $a_o = a'_o$. Ainsi, a_o ne dépend pas du choix de la suite (i_j), ce qui montre bien que $a_o^{(i)}$ est une suite convergente.

1.6. Exemple : séries d'Eisenstein p-adiques

Soit $k \in X$. Si n est un entier ≥ 1, nous noterons $\sigma^*_{k-1}(n)$ l'entier p-adique défini par

$$\sigma^*_{k-1}(n) = \sum d^{k-1},$$

la somme étant étendue aux diviseurs positifs d de n qui sont premiers à p. Cela a un sens, puisqu'un tel élément d est une unité p-adique, ainsi que d^{k-1}, cf. n° 1.4, a).

Supposons maintenant que k soit pair. Choisissons une suite d'entiers pairs $k_i \geq 4$ qui tende vers l'infini au sens usuel (ce que nous écrirons $|k_i| \to \infty$), et qui tende vers k dans X; c'est évidemment possible. On a alors

$$\lim.\sigma_{k_i-1}(n) = \sigma^*_{k-1}(n) \quad \text{dans } \mathbf{Z}_p;$$

en effet d^{k_i-1} tend vers 0 si d est divisible par p (puisque $|k_i| \to \infty$) et tend vers d^{k-1} sinon (puisque $k_i \to k$ dans X). De plus, la convergence

est uniforme en n. Or les $\sigma_{k_i-1}(n)$ sont les coefficients d'indice ≥ 1 de la série d'Eisenstein

$$G_{k_i} = -b_{k_i}/2k_i + \sum_{n=1}^{\infty} \sigma_{k_i-1}(n)q^n,$$

et le terme constant de cette série est $-b_{k_i}/2k_i$, qui est égal, comme on sait, à $\frac{1}{2}\zeta(1-k_i)$. Appliquant alors le cor.2 au th.1', on en déduit que, si $k \neq 0$, les G_{k_i} ont une limite G_k^* qui est une forme modulaire p-adique de poids k :

$$G_k^* = a_o + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)q^n, \quad \text{où} \quad a_o = \frac{1}{2} \lim_{i \to \infty} \zeta(1-k_i).$$

Il est clair que cette limite ne dépend pas du choix de la suite k_i; nous l'appellerons la série d'Eisenstein p-adique de poids k; son terme constant a_o sera noté $\frac{1}{2}\zeta^*(1-k)$, de sorte que l'on a

$$G_k^* = \tfrac{1}{2}\zeta^*(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)q^n \qquad (k \in X,\ k \text{ pair} \neq 0).$$

Cela définit une fonction ζ^* sur les éléments impairs de $X - \{1\}$; le cor.2 au th.1' montre que cette fonction est continue (en fait, la série G_k^* elle-même dépend continûment de k). Nous allons voir que ζ^* est essentiellement la fonction zêta p-adique de Kubota-Leopoldt [16]. De façon plus précise:

THÉORÈME 3. (i) Si $p \neq 2$, et si (s,u) est un élément impair $\neq 1$ de $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ on a

$$\zeta^*(s,u) = L_p(s;\ \omega^{1-u}),$$

où $L_p(s;\chi)$ désigne la fonction L p-adique d'un caractère χ (Iwasawa [11], p.29-30) et ω désigne le caractère défini dans [11], p.18.

(ii) Si $p = 2$, et si s est un élément impair $\neq 1$ de $X = \mathbf{Z}_2$,

on a $\zeta^*(s) = L_2(s; \chi^0)$, cf. [11], p.29-30.

Notons ζ' la fonction

$$(s,u) \longmapsto L_p(s; \omega^{1-u}) \quad \text{si} \quad p \neq 2$$

$$s \longmapsto L_p(s; \chi^0) \quad \text{si} \quad p = 2.$$

Il résulte de [11], loc.cit., que ζ' est continue, et que

$$\zeta'(1-k) = (1 - p^{k-1})\,\zeta(1-k) \quad \text{si} \quad k \in 2\mathbf{Z},\ k \geqslant 2.$$

Si $k \in 2X$, $k \neq 0$, et si (k_i) est une suite convergeant vers k comme ci-dessus, on a

$$\zeta'(1-k) = \lim_{i \to \infty} \zeta'(1-k_i) = \lim_{i \to \infty} (1 - p^{k_i - 1})\,\zeta(1-k_i).$$

Mais, comme $|k_i|$ tend vers $+\infty$, on a $\lim_{i \to \infty} (1 - p^{k_i-1}) = 1$, d'où

$$\zeta'(1-k) = \lim_{i \to \infty} \zeta(1-k_i) = \zeta^*(1-k),$$

ce qui démontre bien que $\zeta' = \zeta^*$.

Exemple

Supposons que $p \equiv 3 \pmod 4$ et $p \neq 3$. Prenons pour k l'élément $(1, \frac{p+1}{2})$ de $\mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$. On peut montrer que

$$G_k^* = \tfrac{1}{2}h(-p) + \sum_{n=1}^{\infty} \sum_{d|n} \left(\frac{d}{p}\right) q^n,$$

où $h(-p)$ est le nombre de classes du corps $\mathbf{Q}(\sqrt{-p})$.

Remarques

1) Lorsque k est un entier pair $\geqslant 2$, on vient de voir que

$$\zeta^*(1-k) = (1-p^{k-1})\,\zeta(1-k);$$

c'est la valeur en $1-k$ de la fonction zêta "débarrassée de son p-ième facteur". On a en outre

$$G_k^* = G_k - p^{k-1}\,G_k|V, \qquad \text{cf. n° 2.1.}$$

2) La fonction ζ^* n'est pas définie au point $s = 1$: elle a un <u>pôle simple</u> en ce point [7], [11], [16].

3) Lorsque k est divisible par $p-1$, on a $v_p(\zeta^*(1-k)) < 0$, de sorte que la série

$$E_k^* = 2G_k^*/\zeta^*(1-k) = 1 + \frac{2}{\zeta^*(1-k)} \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)q^n$$

est à coefficients p-entiers, et $E_k^* \equiv 1 \pmod{p}$. Plus précisément, si l'image de k dans X_m est nulle, on a

$$E_k^* \equiv 0 \pmod{p^m}.$$

En particulier, E_k^* tend vers 1 lorsque k tend vers 0; cela conduit à poser $E_0^* = 1$.

4) Lorsque k n'est pas divisible par $p-1$, il est congru mod.$(p-1)$ à un entier a compris entre 2 et $p-3$, et l'on a

$$\zeta^*(1-k) \equiv -b_a/a \pmod{p},$$

en vertu des congruences de Kummer. En particulier, si p est <u>régulier</u>, on a $\zeta^*(1-k) \not\equiv 0 \pmod{p}$, et la fonction ζ^* ne s'annule nulle part.

Par contre, si p est irrégulier, il peut se faire que $\zeta^*(1-k) = 0$ pour certaines valeurs de k; la série G_k^* correspondante est alors "parabolique" : son terme constant est nul.

§2. Opérateurs de Hecke

2.1. Action de T_ℓ, U, V, θ sur les formes modulaires p-adiques

Si

$$f = \sum_{n=0}^{\infty} a_n q^n$$

est une série formelle à coefficients dans $\mathbf{Q}_p$, on pose :

$$f|U = \sum_{n=0}^{\infty} a_{pn} q^n \quad \text{et} \quad f|V = \sum_{n=0}^{\infty} a_n q^{pn}.$$

Si ℓ est un nombre premier $\neq p$, et si $k \in X$, on pose :

$$f|_k T_\ell = \sum_{n=0}^{\infty} a_{\ell n} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{\ell n}.$$

Lorsque k est sous-entendu, on écrit $f|T_\ell$ au lieu de $f|_k T_\ell$.

THÉORÈME 4. *Si f est une forme modulaire p-adique de poids k, il en est de même de f|U, f|V et des $f|_k T_\ell$ (ℓ premier $\neq p$).*

Choisissons une suite $f_i = \sum a_{n,i} q^n$ de formes modulaires (au sens usuel), à coefficients rationnels, telle que

$$\lim_{i \to \infty} f_i = f.$$

Quitte à remplacer f_i par $f_i E_{(p-1)p^i}$, on peut supposer que les poids k_i des f_i sont tels que $|k_i| \to \infty$. Pour tout nombre premier ℓ, on sait (cf. par exemple [3], [22]) que le transformé $f_i|T_\ell$ de f_i par l'opérateur de Hecke T_ℓ est une forme modulaire de poids k_i, donnée par la formule :

$$f_i|T_\ell = \sum a_{\ell n,i}\, q^n + \ell^{k_i-1} \sum a_{n,i}\, q^{\ell n}.$$

On a $\lim_{i\to\infty} \ell^{k_i-1} = \ell^{k-1}$ si $\ell \neq p$ (car alors ℓ est une unité p-adique), et $\lim_{i\to\infty} \ell^{k_i-1} = 0$ si $\ell = p$ (puisque $|k_i| \to \infty$). On en conclut que les $f_i|T_\ell$ tendent vers $f|T_\ell$ si $\ell \neq p$, et vers $f|U$ si $\ell = p$; cela montre bien que les séries $f|T_\ell$ et $f|U$ sont des formes modulaires p-adiques, de poids $\lim_{i\to\infty} k_i = k$. Appliquant ce résultat à f_i, on voit que $f_i|U$ est modulaire p-adique de poids k_i; comme $f_i|T_p$ est aussi modulaire de poids k_i, on en conclut que $f_i|V = p^{1-k_i}(f_i|T_p - f_i|U)$ est modulaire p-adique de poids k_i; comme $f|V = \lim_{i\to\infty} f_i|V$, il en résulte bien que $f|V$ est modulaire p-adique de poids k.

Remarque. On peut également définir les opérateurs de Hecke T_m pour tout entier m premier à p, au moyen des formules usuelles. Ces opérateurs commutent entre eux, commutent à U et V, et l'on a

$$T_m T_n = T_n T_m = T_{mn} \quad \text{si} \quad (m,n) = 1,$$

$$T_\ell\, T_{\ell^n} = T_{\ell^{n+1}} + \ell^{k-1}\, T_{\ell^{n-1}} \quad \text{si} \quad \ell \text{ est premier et } n \geq 1.$$

Exemples

On a $G_k^*|T_\ell = (1 + \ell^{k-1})G_k^*$ et $G_k^*|U = G_k^*$.

Si k est un entier pair ≥ 2, un calcul immédiat montre que

$$G_k^* = G_k - p^{k-1}G_k|V = G_k|(1 - p^{k-1}V).$$

On en déduit

$$G_k = G_k^*|(1 - p^{k-1}V)^{-1} = G_k^* + p^{k-1}G_k^*|V + \ldots + p^{m(k-1)}G_k^*|V^m + \ldots$$

Pour $k = 2$, cette formule montre que $G_2 = -P/24$ est somme d'une série convergente de formes modulaires p-adiques de poids 2. On en conclut que P est une forme modulaire p-adique de poids 2.

THÉORÈME 5. *Soit* $f = \sum a_n q^n$ *une forme modulaire p-adique de poids* k.

(a) *La série*

$$\theta f = q\, df/dq = \sum n\, a_n\, q^n$$

est une forme modulaire p-adique de poids $k + 2$.

(b) *Pour tout* $h \in X$, *la série*

$$f|R_h = \sum_{(n,p)=1} n^h\, a_n\, q^n$$

est une forme modulaire p-adique de poids $k + 2h$.

Soit (f_i) une suite de formes modulaires, à coefficients rationnels, telle que $\lim f_i = f$, et soit k_i le poids de f_i. On sait (cf. [20], [27]) que $\theta f_i = k_i P f_i/12 + g_i$, où g_i est une forme modulaire de poids $k_i + 2$. Puisque P est modulaire p-adique de poids 2, il en résulte que θf_i est modulaire p-adique de poids $k_i + 2$, et en passant à la limite cela montre bien que θf est modulaire p-adique de poids $k + 2$.

Choisissons maintenant une suite d'entiers positifs h_i telle que

$$h_i \to h \text{ dans } X \quad \text{et} \quad |h_i| \to \infty.$$

Vu ce qui précède, $\theta^{h_i} f$ est modulaire p-adique de poids $k + 2h_i$. Comme $\theta^{h_i} f$ tend vers $f|R_h$ lorsque $i \to \infty$, on voit bien que $f|R_h$ est modulaire p-adique de poids $k + 2h$.

Remarque

On a les formules : $(\theta f)|U = p\theta(f|U)$, $f|R_h|U = 0$,

$$\theta(f|V) = p(\theta f)|V, \quad (\theta f)|_{k+2} T_\ell = \ell\, \theta(f|_k T_\ell), \quad f|V|R_h = 0,$$

et $$(f|R_h)|_{k+2h}\, T_\ell = \ell^h\, (f|_k\, T_\ell)|R_h$$

pour tout ℓ premier $\neq p$.

Exemples

Pour $h = 0$, on a

$$f|R_o = \lim_{m \to \infty} \theta^{(p-1)p^m} f = f|(1 - UV) = \sum_{(n,p)=1} a_n q^n.$$

Pour $h = (0, \frac{p-1}{2}) \in \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, $p \geq 3$, on a :

$$f|R_h = \lim_{m \to \infty} \theta^{(p-1)p^m/2} f = \sum \left(\frac{n}{p}\right) a_n\, q^n.$$

2.2. Une propriété de contraction

Les opérateurs de Hecke T_ℓ et T_p laissent stable l'espace M_k des formes modulaires de poids k à coefficients p-entiers. Par réduction (mod.p) ils opèrent donc sur $\tilde{M}_k$; comme $T_p \equiv U \pmod{p}$, on en conclut que U opère sur $\tilde{M}_k$, donc aussi sur les espaces

$$\tilde{M}^\alpha = \bigcup_{k \in \alpha} \tilde{M}_k \qquad (\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}, \quad \text{cf. n° 1.2}).$$

En fait, U "contracte" les $\tilde{M}_k$. De façon plus précise, nous allons démontrer le théorème suivant, en rapport étroit avec des résultats d'Atkin [2], Koike [15] et Dwork :

THÉORÈME 6.

(i) *Si* $k > p + 1$, *U applique* $\tilde{M}_k$ *dans* $\tilde{M}_{k'}$, *avec* $k' < k$.

(ii) *La restriction de* U *à* $\tilde{M}_{p-1}$ *est bijective*.

Lorsque $p = 2$ ou 3, on a $\tilde{M} = \mathbf{F}_p[\tilde{\Delta}]$, et $\tilde{M}_k$ est l'espace des polynômes en $\tilde{\Delta}$ de degré $\leq k/12$. Utilisant la formule $(g^p f)|U \equiv g.(f|U) \pmod{p}$,

on vérifie que $\tilde{\Delta}^i|U = 0$ si $i \not\equiv 0 \pmod{p}$ et $\tilde{\Delta}^i|U = \tilde{\Delta}^{i/p}$ sinon. On en conclut que U applique $\tilde{M}_k$ dans $\tilde{M}_{k'}$, avec $k' = [k/p]$, d'où le théorème dans ce cas.

Supposons maintenant $p \geq 5$. Si f est un élément d'un $\tilde{M}^\alpha$, notons w(f) la filtration de f (cf. [20], [27]), i.e. la borne inférieure des k tels que $f \in \tilde{M}_k$.

LEMME 1.

(a) On a $w(\theta f) \leq w(f) + p+1$, et il y a égalité si et seulement si $w(f) \not\equiv 0 \pmod{p}$.

(b) On a $w(f^i) = i\, w(f)$ pour tout $i \geq 1$.

L'assertion (a) est démontrée dans [27], Lemme 5 et dans [20], cor.3 au th.5.

Pour prouver (b), on peut supposer $f \neq 0$, i.e. $w(f) \neq -\infty$. Ecrivons alors f comme polynôme isobare $F(\tilde{Q},\tilde{R})$ en $\tilde{Q},\tilde{R}$, de poids $k = w(f)$. Le polynôme F n'est pas divisible par le polynôme $\tilde{A}$ du n° 1.2 ([27], loc. cit.). Comme $\tilde{A}$ est sans facteur multiple, il en résulte que F^i n'est pas non plus divisible par $\tilde{A}$, d'où le fait que $f^i = F^i(\tilde{Q},\tilde{R})$ est de filtration ik.

LEMME 2.

(i) On a $w(f|U) \leq p + (w(f) - 1)/p$.

(ii) Si $w(f) = p-1$, on a $w(f|U) = p-1$.

On a l'identité

$$(f|U)^p = f - \theta^{p-1}f \quad \text{pour tout} \quad f \in \mathbf{F}_p[[q]].$$

Si l'on pose $k = w(f)$ et $k' = w(f|U)$, le lemme 1 montre que

$$w((f|U)^p) = pk' \quad \text{et} \quad w(\theta^{p-1}f) \leq k + p^2 - 1.$$

On en conclut que $pk' \leqslant \mathrm{Sup}(k, k + p^2 - 1) = k + p^2 - 1$, ce qui démontre (i).

Supposons maintenant que $k = p-1$. Si l'on calcule $\theta^2 f$ au moyen de la formule $12\theta = kP + \partial$ (cf. [27] pour la définition de la dérivation ∂), on trouve que $12^2\theta^2 f = Qf + \partial^2 f$, d'où $\theta^2 f \in \tilde{M}_{p+3}$. La filtration h de $\theta^2 f$ est donc $-\infty$, 4 ou p+3. Dans le premier cas, on aurait $\theta^2 f = 0$, d'où $\theta^{p-1} f = 0$ et f serait égal à $(f|U)^p$, ce qui est absurde, puisque la filtration de f n'est pas divisible par p. Dans le cas $h = 4$, $\theta^2 f$ serait multiple non nul de Q, ce qui est également absurde puisque son terme constant est nul. On a donc nécessairement $w(\theta^2 f) = p+3$. Appliquant le Lemme 1, on en conclut que

$$w(\theta^i \theta^2 f) = p + 3 + i(p+1) \quad \text{pour} \quad 0 \leqslant i \leqslant p-3.$$

(Observer que $p + 3 + i(p + 1)$ n'est pas divisible par p si $i \leqslant p-4$.)

En particulier, on a $w(\theta^{p-1} f) = p + 3 + (p - 3)(p+1) = p(p - 1)$, d'où $w((f|U)^p) = p(p-1)$, et $w(f|U) = p-1$.

Le théorème 6 est maintenant immédiat. L'assertion (i) résulte du Lemme 2 (i), compte tenu de ce que $p + (k - 1)/p$ est $< k$ si $k > p + 1$. D'autre part, si f est un élément non nul de $\tilde{M}_{p-1}$, on a, soit $w(f) = 0$, et f est une constante, d'où $f|U = f \neq 0$, soit $w(f) = p-1$ et le Lemme 2 (ii) montre que $w(f|U) = p-1$, d'où $f|U \neq 0$; ainsi, la restriction de U à $\tilde{M}_{p-1}$ est injective, donc bijective, puisque $\tilde{M}_{p-1}$ est de dimension finie.

Le th.6 entraîne aussitôt le résultat suivant :

COROLLAIRE. *Soit* α *un élément pair de* $\mathbf{Z}/(p-1)\mathbf{Z}$, $p \geqslant 5$.

(i) *On peut décomposer* $\tilde{M}^\alpha$ *de façon unique en* $\tilde{M}^\alpha = \tilde{S}^\alpha \oplus \tilde{N}^\alpha$, *de telle sorte que* U *soit bijectif sur* $\tilde{S}^\alpha$ *et localement nilpotent sur* $\tilde{N}^\alpha$. *On a* $\tilde{S}^\alpha \subset \tilde{M}_j$, *où* $j \in \alpha$ *est tel que* $4 \leqslant j \leqslant p+1$; *en particulier,* $\tilde{S}^\alpha$ *est de dimension finie.*

(ii) *Pour* $\alpha = 0$, *on a* $j = p - 1$ *et* $\tilde{S}^0 = \tilde{M}_{p-1}$.

Lorsque $p = 2$ ou 3, on a une décomposition analogue de $\tilde{M} = \mathbf{F}_p[\tilde{\Delta}]$ en $\tilde{M} = \tilde{S} \oplus \tilde{N}$, avec $\tilde{S} = \tilde{M}_0 = \mathbf{F}_p$ et $\tilde{N} = \tilde{\Delta}.\tilde{M}$; l'endomorphisme U est l'identité sur $\tilde{S}$, et est localement nilpotent sur $\tilde{N}$.

Remarque

Lorsque $\alpha \neq 0$, il peut se faire que $\tilde{S}^\alpha$ soit distinct de $\tilde{M}_j$, i.e. que la restriction de U à $\tilde{M}_j$ admette 0 pour valeur propre; c'est le cas pour $\alpha = j = 16$ et $p = 59$. On a toutefois $\tilde{S}^\alpha = \tilde{M}_j$ dans chacun des cas suivants :

$\alpha = 2$, $j = p+1$; les seules valeurs propres de U sur $\tilde{M}_{p+1}$ sont en effet ± 1, cf. n° 3.3, cor. au th.11.

$\alpha = j = 4, 6, 8, 10, 14$; $\tilde{M}_j$ est alors réduit aux multiples de la série d'Eisenstein $\tilde{G}_j$, et celle-ci est invariante par U.

Pour $\alpha = j = 12$ (et $p \geqslant 11$), les valeurs propres de U sur $\tilde{M}_j$ sont 1 et $\tau(p)$. On a donc $\tilde{S}^\alpha \neq \tilde{M}_j$ si et seulement si $\tau(p) \equiv 0 \pmod{p}$; d'après M.Newman, c'est le cas pour $p = 2411$.

2.3. Application au calcul du terme constant d'une forme modulaire p-adique

Si f est une série formelle en q, nous conviendrons de noter $a_n(f)$ son n-ième coefficient; nous dirons que f est parabolique si son terme constant $a_0(f)$ est nul.

Soit f une forme modulaire p-adique de poids $k \in X$. Nous allons voir que, si $k \neq 0$, $a_0(f)$ peut se "calculer" en fonction des $a_n(f)$, $n \geqslant 1$. Commençons par un cas particulier simple :

THÉORÈME 7. Si f est une forme modulaire p-adique de poids $k \neq 0$, et si $p = 2, 3, 5$ ou 7, on a

$$(*) \qquad a_0(f) = \frac{1}{2}\zeta^*(1-k) \lim_{n \to \infty} a_{p^n}(f).$$

Comme p est régulier, on a $\zeta^*(1-k) \neq 0$, cf. n° 1.6, et la série d'Eisenstein p-adique G_k^* a un terme constant $\neq 0$. On peut donc écrire f

comme somme d'une forme parabolique et d'un multiple de G_k^*. On est ainsi ramené à démontrer le th.7 dans les deux cas suivants :

a) $f = G_k^*$.

On a alors $a_o(f) = \frac{1}{2}\zeta^*(1-k)$ et $a_{p^n}(f) = \sigma^*_{k-1}(p^n) = 1$; la formule est évidente.

b) f est parabolique.

On doit prouver que $a_{p^n}(f)$ tend vers 0. Comme $a_{p^n}(f) = a_1(f|U^n)$, il suffit de prouver :

LEMME 3. Si f est parabolique, et $p \leqslant 7$, on a

$$\lim_{n \to \infty} f|U^n = 0.$$

Quitte à faire une homothétie sur f, on peut supposer que $v_p(f) = 0$. Soit $\tilde{f}$ la réduction (mod.p) de f, et soit α l'image de k dans $\mathbf{Z}/(p-1)\mathbf{Z}$; on a $f \in \tilde{M}^\alpha$. Utilisons la décomposition $\tilde{M}^\alpha = \tilde{S}^\alpha \oplus \tilde{N}^\alpha$ fournie par le corollaire au th.6. Du fait que $p \leqslant 7$, l'entier j correspondant est $\leqslant 8$, et $\tilde{S}^\alpha$ est simplement l'ensemble des multiples de $\tilde{E}_k$; il en résulte que $\tilde{N}^\alpha$ est l'ensemble des éléments paraboliques de M. On a donc $\tilde{f} \in \tilde{N}^\alpha$, et il existe un entier $m \geqslant 1$ tel que $\tilde{f}|U^m = 0$, i.e.

$$v_p(f|U^m) \geqslant 1.$$

Appliquons ce résultat à la forme parabolique $\frac{1}{p} f|U^m$. On en déduit qu'il existe un entier $m' \geqslant 1$ tel que

$$v_p(f|U^{m+m'}) \geqslant 2.$$

D'où, par une récurrence évidente, le fait que $v_p(f|U^n)$ tend vers l'infini avec n, ce qui démontre le lemme (et le th.7).

Remarque

Lorsque $p \geqslant 11$, la formule (*) reste valable pourvu que l'on ait

$k \equiv 4, 6, 8, 10, 14 \pmod{(p-1)}$; la démonstration est la même. Le cas $p = 11$, $f = \Delta$ montre qu'une hypothèse sur k est nécessaire.

Nous allons maintenant établir une formule analogue à (*), valable pour tout k divisible par p-1.

THÉORÈME 8. *Il existe un polynôme* H *en* U *et les* T_ℓ, *à coefficients entiers, tel que, pour tout* $k \in X$ *divisible par* p-1, *on ait* :

(i) $E_k^* | H = c(k)\, E_k^*$, *avec* $c(k)$ *inversible dans* $\mathbf{Z}_p$,

(ii) $\lim_{n \to \infty} f | H^n = 0$

pour toute forme modulaire p-*adique* f *de poids* k *qui est parabolique*.

(Noter que H ne dépend pas de k, mais que son action sur f en dépend; lorsque l'on désire mettre ce fait en évidence, on écrit $f|_k H$ au lieu de $f|H$.)

COROLLAIRE. *Pour toute forme modulaire* p-*adique* f, *de poids* $k \neq 0$, *avec* $k \equiv 0 \pmod{(p-1)}$, *on a*

$$(**) \qquad a_0(f) = \tfrac{1}{2}\zeta^*(1-k) \lim_{n \to \infty} c(k)^{-n}\, a_1(f|H^n).$$

En effet, il suffit de vérifier la formule (**) lorsque $f = E_k^*$ et lorsque f est parabolique; dans le premier cas elle résulte de (i), et dans le second de (ii).

(On notera que, pour k fixé, $a_1(f|H^n)$ est combinaison $\mathbf{Z}_p$-linéaire des $a_m(f)$, $m \geq 1$; la formule (**) donne donc bien un procédé de calcul de $a_0(f)$ en fonction des $a_m(f)$.)

Démonstration du théorème 8

Si $p = 2, 3, 5, 7$ on prend $H = U$, cf. th.7. On peut donc supposer que $p \geq 11$. Tout revient à construire un polynôme $\tilde{H}$ en U et les T_ℓ, à coefficients dans $\mathbf{F}_p$, tel que :

(i)' $1|\tilde{H} = c$, *avec* $c \neq 0$ *dans* $\mathbf{F}_p$.

(ii)' $f \mapsto f|\tilde{H}$ *est localement nilpotent sur l'ensemble* $\tilde{P}^o$ *des éléments*

paraboliques de $\tilde{M}^o$.

En effet, si l'on dispose d'un tel $\tilde{H}$, on prend pour H un polynôme à coefficients entiers dont la réduction (mod.p) est égale à $\tilde{H}$. Comme $E_k^*|U = E_k^*$ et $E_k^*|T_\ell = (1 + \ell^{k-1})E_k^*$, on a

$$E_k^*|H = c(k)\, E_k^*, \quad \text{avec} \quad c(k) \in \mathbf{Z}_p;$$

de plus, l'image de c(k) dans $\mathbf{F}_p$ est égale à c, ce qui montre que c(k) est inversible dans $\mathbf{Z}_p$, d'où (i). Le fait que (ii)' entraîne (ii) se démontre par l'argument utilisé pour le th.7.

Construction de $\tilde{H}$

Faisons opérer U et les T_ℓ sur l'espace vectoriel $\tilde{S}^o = \tilde{M}_{p-1}$, cf. cor. au th.6. Ces opérateurs commutent entre eux et respectent la décomposition de $\tilde{M}_{p-1}$ en $\mathbf{F}_p \oplus \tilde{P}_{p-1}$, où $\tilde{P}_{p-1}$ désigne le sous-espace des formes paraboliques. Les valeurs propres de U et T_ℓ sur le sous-espace $\tilde{M}_o = \mathbf{F}_p$ sont respectivement 1 et $1 + \ell^{-1}$.

Par contre :

LEMME 4. *Il n'existe pas d'élément* $f \neq 0$ *de* $\tilde{P}_{p-1}$ *tel que*

$$f|U = f \quad \text{et} \quad f|T_\ell = (1 + \ell^{-1})f$$

pour tout ℓ *premier* $\neq p$.

En effet, supposons qu'un tel f existe, et écrivons-le $f = \sum_{n=1}^{\infty} a_n q^n$. On a par hypothèse

$$a_{pn} = a_n, \quad a_{\ell n} = (1 + \ell^{-1})a_n \quad \text{si} \quad n \not\equiv 0 \pmod{\ell},$$

$$a_{\ell n} = (1 + \ell^{-1})a_n - \ell^{-1}a_{n/\ell} \quad \text{si} \quad n \equiv 0 \pmod{\ell}.$$

Ces formules permettent de calculer par récurrence a_n à partir de a_1. On trouve $a_n = a_1\sigma^*_{-1}(n) = a_1\, \sigma_{p-2}(n)$, i.e. $f = a_1\, \tilde{\phi}$, où

$$\phi = \sum_{n=1}^{\infty} \sigma_{p-2}(n) q^n.$$

Mais, d'après le lemme de [20], p.416-11, la série $\tilde{\phi}$ n'appartient pas à $\tilde{M}^o$; on obtient donc une contradiction.

Le lemme suivant est élémentaire :

LEMME 5. *Soient* k *un corps commutatif*, Y *un* k*-espace vectoriel de dimension finie*, $(U_i)_{i \in I}$ *une famille d'endomorphismes de* Y, *et* $(\lambda_i)_{i \in I}$ *une famille d'éléments de* k. *On suppose que les* U_i *commutent entre eux, et qu'il n'existe aucun élément* $y \neq 0$ *de* Y *tel que* $U_i y = \lambda_i y$ *pour tout* $i \in I$. *Il existe alors un polynôme* $F \in k[(X_i)_{i \in I}]$ *tel que* $F((U_i)_{i \in I}) = 0$ *et* $F((\lambda_i)_{i \in I}) \neq 0$.

Appliquons ce lemme aux endomorphismes U et T_ℓ de l'espace $Y = \tilde{P}_{p-1}$, et aux scalaires 1 et $1 + \ell^{-1}$, cf. lemme 4. On en déduit l'existence d'un polynôme F en U et les T_ℓ dont la restriction à $\tilde{P}_{p-1}$ est nulle, et qui ne s'annule pas sur $\mathbf{F}_p$. Le polynôme $\tilde{H} = U.F$ répond alors à la question. En effet, il vérifie évidemment (i)'. D'autre part, on a $\tilde{P}^o = \tilde{P}_{p-1} \oplus \tilde{N}^o$, et F est nul sur $\tilde{P}_{p-1}$, tandis que U est localement nilpotent sur $\tilde{N}^o$, cf. cor.au. th.6; comme U et F commutent, il en résulte que U.F est localement nilpotent sur $\tilde{P}^o$, ce qui achève la démonstration.

Exemples

$p \leqslant 11$: $H = U$ et $c(k) = 1$;

$p = 13$: $H = U(U + 5)$ et $c(k) = 6$; $H = U(T_2 - 2)$ et $c(k) = 2^{k-1} - 1$;

$p = 17$: $H = U(T_2 + 5)$ et $c(k) = 2^{k-1} + 6$.

Passons maintenant au cas d'un poids non divisible par p-1. Faute de mieux, je me bornerai à un théorème d'existence :

THÉORÈME 9. *Soit* k *un élément pair de* X, *non divisible par* p-1. *Il existe une suite* $(\lambda_{m,n})_{m,n \geqslant 1}$ *d'éléments de* $\mathbf{Z}_p$ *telle que* :

a) *pour tout* n, *on a* $\lambda_{m,n} = 0$ *pour* m *assez grand*;

b) *si l'on pose*

$$u_n(f) = \sum_{m=1}^{\infty} \lambda_{m,n}\, a_m(f),$$

on a

$$(***) \qquad a_o(f) = \lim_{n \to \infty} u_n(f)$$

pour toute forme modulaire p-adique f de poids k.

(Précisons que les coefficients $\lambda_{m,n}$ dépendent du poids k choisi.)

Notons M(k) le $\mathbf{Q}_p$-espace vectoriel des formes modulaires p-adiques de poids k.

LEMME 6. Soit Y un sous-espace de dimension finie de M(k). Il existe des éléments $(\lambda_m)_{m \geq 1}$ de $\mathbf{Z}_p$, nuls sauf un nombre fini d'entre eux, tels que

$$a_o(f) = \sum_{m=1}^{\infty} \lambda_m\, a_m(f) \quad \text{pour tout} \quad f \in Y.$$

Soit Y_o le sous-$\mathbf{Z}_p$-module de Y formé des éléments f tels que $v_p(f) \geq 0$. Il est facile de voir que Y_o est un $\mathbf{Z}_p$-module libre de rang $r = \dim.V$. Soit $f_1,\ldots,f_r$ une base de Y_o. On peut trouver r indices $m_1, \ldots, m_r \geq 1$ tels que

$$\det(a_{m_i}(f_j)) \not\equiv 0 \pmod{p}.$$

Sinon en effet il existerait des $c_j \in \mathbf{Z}_p$, non tous divisibles par p, tels que

$$a_m\Big(\sum_{j=1}^{r} c_j f_j\Big) \equiv 0 \pmod{p} \quad \text{pour tout} \quad m \geq 1;$$

si l'on pose

$$f = \sum_{j=1}^{r} c_j f_j,$$

le cor.1 au th.1' du n° 1.5 montrerait que $v_p(f) \geq 1$, contrairement au

fait que les c_j ne sont pas tous divisibles par p. Ceci étant, il est clair que les formes linéaires $a_{m_1}, \ldots a_{m_r}$ forment une base du dual du $\mathbf{Z}_p$-module Y_o, et comme a_o est une forme linéaire sur Y_o, on peut écrire a_o sous la forme

$$a_o = \sum_{i=1}^{r} \lambda_i a_{m_i}, \quad \text{avec} \quad \lambda_i \in \mathbf{Z}_p,$$

d'où le lemme.

Soit maintenant $M(k)_o$ l'ensemble des $f \in M(k)$ tels que $v_p(f) \geq 0$. Si α est l'image de k dans $\mathbf{Z}/(p-1)\mathbf{Z}$, on a $M(k)_o/pM(k)_o \subset \tilde{M}^{\alpha}$ (il y a même égalité), et par suite l'ensemble $M(k)_o/pM(k)_o$ est <u>dénombrable</u>. Il en résulte que l'on peut trouver dans M(k) une suite croissante

$$V_1 \subset V_2 \subset \ldots \subset V_n \subset \ldots$$

de $\mathbf{Q}_p$-sous-espaces vectoriels de dimensions finies dont la réunion est dense dans M(k). Pour chacun des V_n, le lemme 6 montre qu'il existe une combinaison $\mathbf{Z}_p$-linéaire u_n des $a_m (m \geq 1)$ telle que $a_o(f) = u_n(f)$ pour tout $f \in V_n$. Comme la famille des u_n est équicontinue, le fait qu'elle converge vers a_o sur une partie dense de M(k) entraîne qu'elle converge partout, et l'on a donc bien

$$a_o(f) = \lim_{n \to \infty} u_n(f) \quad \text{pour tout} \quad f \in M(k).$$

<u>Remarques</u>

1) La démonstration ci-dessus peut aussi s'exprimer en disant que le $\mathbf{Z}_p$-module engendré par les $a_m (m \geq 1)$ est <u>faiblement dense</u> dans la boule unité du dual de l'espace de Banach p-adique M(k).

2) Dans le cas archimédien (i.e. pour les formes modulaires usuelles de poids $k > 0$), le problème consistant à exprimer $a_o(f)$ à partir des $a_n(f)$, $n \geq 1$, a une solution très simple, due à Hecke : on forme la

série de Dirichlet

$$\phi_f(s) = \sum_{n=1} a_n(f)\, n^{-s},$$

on la prolonge en une fonction méromorphe dans $\mathbf{C}$, et l'on prend sa valeur $\phi_f(0)$ au point $s = 0$: c'est $- a_0(f)$.

§3. Formes modulaires sur $\Gamma_0(p)$

Le but de ce § est de justifier le principe suivant, bien connu expérimentalement : toute forme modulaire sur $\Gamma_0(p)$ est p-adiquement sur $SL_2(\mathbf{Z})$. La méthode suivie est due à Atkin; elle repose sur les propriétés des coefficients des séries d'Eisenstein. Une autre méthode, basée sur un théorème de Deligne ([6], §7), est exposée dans Katz [12] et Koike [15].

3.1. Rappels

a) Notation

Soit f une fonction sur le demi-plan de Poincaré $H = \{z \mid \mathrm{Im}(z) > 0\}$; soient $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ une matrice réelle de déterminant > 0, et k un entier; on définit une fonction $f|_k\gamma$ sur H par la formule

$$(f|_k\gamma)(z) = \det(\gamma)^{k/2}\, (cz + d)^{-k}\, f\left(\frac{az + b}{cz + d}\right).$$

On a $(f|_k\gamma)|_k\gamma' = f|_k\gamma\gamma'$ et $f|_k\gamma = f$ si γ est une homothétie > 0. Lorsque k est sous-entendu, on écrit $f|\gamma$ au lieu de $f|_k\gamma$.

b) Formes modulaires sur $\Gamma_0(p)$

Le groupe $\Gamma_0(p)$ est défini comme le sous-groupe de $SL_2(\mathbf{Z})$ formé des

matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ telles que $c \equiv 0 \pmod{p}$; il est d'indice $p+1$ dans $SL_2(\mathbf{Z})$; il est normalisé dans $GL_2(\mathbf{Q})$ par la matrice $W = \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$.

Soit k un entier. Une <u>forme modulaire de poids</u> k sur $\Gamma_o(p)$ est une fonction holomorphe f sur H telle que :

(i) $f|_k\gamma = f$ <u>pour tout</u> $\gamma \in \Gamma_o(p)$;

(ii) f <u>est holomorphe aux pointes de</u> $\Gamma_o(p)$.

En fait, $\Gamma_o(p)$ n'a que deux pointes, ∞ et 0, qui sont permutées par W. La condition (ii) équivaut donc à la suivante :

(ii') <u>Les fonctions</u> f <u>et</u> $f|_kW$ <u>ont des développements en série</u>

$$f = \sum_{n=0}^{\infty} a_n q^n, \qquad f|_kW = \sum_{n=0}^{\infty} b_n q^n$$

$$(q = e^{2\pi iz}, \quad a_n \in \mathbf{C}, \quad b_n \in \mathbf{C})$$

<u>qui convergent pour tout</u> $z \in H$ (i.e. pour tout q tel que $|q| < 1$).

Si f est modulaire, il en est de même de $f|W$, et $f|W^2 = f$.

Lorsque k est < 0, ou impair, toute forme modulaire de poids k est nulle. Dans ce qui suit, nous supposerons donc k pair ≥ 0.

c) <u>Trace d'une forme modulaire sur</u> $\Gamma_o(p)$

Soit f une forme modulaire de poids k sur $\Gamma_o(p)$. Choisissons des représentants $\gamma_1, \ldots, \gamma_{p+1}$ de l'espace homogène $\Gamma_o(p)\backslash SL_2(\mathbf{Z})$, et posons

$$Tr(f) = \sum_{j=1}^{p+1} f|_k\gamma_j.$$

On vérifie immédiatement que Tr(f) ne dépend pas du choix des γ_j, et que c'est une forme modulaire de poids k sur $SL_2(\mathbf{Z})$; on l'appelle la <u>trace</u> de f. Nous aurons besoin de son développement en série :

LEMME 7. <u>Si</u> $f = \sum a_n q^n$ <u>et</u> $f|_kW = \sum b_n q^n$, <u>on a</u>

$$Tr(f) = \sum a_n q^n + p^{1-k/2} \sum b_{pn} q^n = f + p^{1-k/2}(f|_kW)|U.$$

On choisit pour représentants $\gamma_j = \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix}$, $1 \leq j \leq p$, et $\gamma_{p+1} = 1$. Le terme $f|_k\gamma_{p+1}$ donne f. Pour calculer les autres termes, posons $g = f|_k W$, et écrivons $\gamma_j (1 \leq j \leq p)$ sous la forme $W\beta_j$, où $\beta_j = \begin{pmatrix} 1/p & j/p \\ 0 & 1 \end{pmatrix}$. On a

$$\sum_{j=1}^{p} f|_k \gamma_j = \sum_{j=1}^{p} g|_k \beta_j ;$$

c'est la fonction

$$z \longmapsto p^{-k/2} \sum_{j=1}^{p} g\left(\frac{z+j}{p}\right).$$

Or un calcul simple montre que

$$\sum_{j=1}^{p} g\left(\frac{z+j}{p}\right) = p(g|U)(z).$$

D'où le lemme.

Remarques

1) Le calcul ci-dessus s'applique plus généralement aux fonctions modulaires de poids k, non nécessairement holomorphes; la seule différence est que les séries considérées peuvent avoir des exposants négatifs.

2) Le lemme 7, appliqué à $f|_k W$ donne

$$\mathrm{Tr}(f|_k W) = f|_k W + p^{1-k/2} f|U,$$

ce qui montre que f|U est une forme modulaire de poids k sur $\Gamma_0(p)$.

Si de plus f est modulaire sur $SL_2(\mathbb{Z})$, on a $f|_k W = p^{k/2} f|V$ comme on le voit en écrivant $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ et en remarquant que f est invariant par $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. D'où :

$$\mathrm{Tr}(f|_k W) = p^{k/2} f|V + p^{1-k/2} f|U = p^{1-k/2} f|_k T_p$$

On a ainsi ramené l'opérateur de Hecke T_p à l'opérateur Tr.

3) Supposons $k \geq 4$. Les formes modulaires f de poids k sur $\Gamma_o(p)$ telles que $Tr(f) = Tr(f|_k W) = 0$ ne sont autres que les combinaisons linéaires des "new forms" d'Atkin-Lehner [3].

d) Propriétés de rationalité et d'intégralité

Soit $j_p = j|V$ la fonction $z \longmapsto j(pz)$. On sait que le corps des fonctions modulaires (de poids 0) sur $\Gamma_0(p)$ est le corps $\mathbf{C}(j, j_p)$ et que j et j_p sont liés par une équation absolument irréductible à coefficients dans $\mathbf{Q}$. En d'autres termes, la courbe complexe $Y_{\mathbf{C}}$ compactifiée de $H/\Gamma_o(p)$ provient par extension des scalaires d'une courbe Y définie sur $\mathbf{Q}$, caractérisée par le fait que son corps des fonctions rationnelles est $\mathbf{Q}(j, j_p)$. Si F est un sous-corps de $\mathbf{C}$, on peut donc parler d'une fonction (ou d'une forme différentielle) sur $Y_{\mathbf{C}}$ qui est rationnelle sur F. Ceci s'applique en particulier aux formes modulaires de poids k, identifiables à des formes différentielles de poids k/2 par $f \longmapsto f(dq/q)^{k/2}$. Comme j et j_p ont des développements en série à coefficients rationnels, on vérifie facilement qu'une forme modulaire $f = \sum a_n q^n$ est rationnelle sur F si et seulement si ses coefficients a_n appartiennent à F. De plus, le corps de rationalité de $f|W$ est le même que celui de f; cela résulte de ce que l'automorphisme W de $Y_{\mathbf{C}}$ est rationnel sur $\mathbf{Q}$.

Il résulte de ceci que les formes modulaires de poids k sur $\Gamma_o(p)$ ont une base formée de fonctions rationnelles sur $\mathbf{Q}$. En fait, il existe même une base formée de fonctions dont les coefficients a_n sont entiers; ce résultat, nettement moins évident, peut se démontrer, soit en utilisant l'existence d'un modèle de Y sur $\mathbf{Z}$ pour lequel q est une uniformisante à l'infini (Igusa, Deligne), soit en se ramenant au fait que les valeurs propres des opérateurs de Hecke sont des entiers algébriques (Shimura [22], p.85, th.3.52). Une conséquence de ceci est que, si $f = \sum a_n q^n$ est une forme modulaire à coefficients rationnels, les dénominateurs des a_n sont bornés. (On notera que, si les coefficients a_n de f sont entiers, il n'en est pas nécessairement de même des coefficients b_n de

$f|_k W$: les b_n sont rationnels, mais peuvent avoir pour dénominateurs des puissances de p.)

3.2. Passage de $\Gamma_0(p)$ à $SL_2(\mathbf{Z})$

THÉORÈME 10. *Soit $f = \sum a_n q^n$ une forme modulaire de poids k sur $\Gamma_0(p)$. Supposons que les coefficients a_n soient rationnels. Alors f est une forme modulaire p-adique de poids k (au sens du n° 1.4).*

(En d'autres termes, f est limite de formes modulaires f_m sur $SL_2(\mathbf{Z})$ dont les poids k_m tendent vers k dans l'espace X du n° 1.4.)

Choisissons un entier pair $a \geq 4$, divisible par p-1. Posons

$$g = E_a - p^{a/2} E_a|_a W = E_a - p^a E_a|V,$$

où E_a est la série d'Eisenstein de poids a, cf. n° 1.1. Il est clair que g est une forme modulaire de poids a sur $\Gamma_0(p)$, cf. n° 3.1. De plus :

LEMME 8. *On a $g \equiv 1 \pmod{p}$ et $g|_a W \equiv 0 \pmod{p^{1+a/2}}$.*

(Précisons que, dans ces congruences, on considère g et $g|_a W$ comme des séries en q, à coefficients rationnels.)

Le fait que $g \equiv 1 \pmod{p}$ provient de ce que $E_a \equiv 1 \pmod{p}$. D'autre part, on a

$$g|_a W = E_a|_a W - p^{a/2} E_a = p^{a/2}(E_a|V - E_a).$$

Comme $E_a \equiv 1 \equiv E_a|V \pmod{p}$, on en déduit bien que $g|_a W$ est congru à $0 \pmod{p^{1+a/2}}$.

Passons maintenant à la démonstration du th.10. L'hypothèse faite sur f signifie que f est rationnelle sur $\mathbf{Q}$, et il en est de même de $f|_k W$, cf. n° 3.1. Si m est un entier ≥ 0, la fonction fg^{p^m} est une forme modulaire sur $\Gamma_0(p)$, de poids $k_m = k + ap^m$, et rationnelle sur $\mathbf{Q}$.

Sa trace $f_m = \mathrm{Tr}(fg^{p^m})$ est donc une forme modulaire sur $SL_2(\mathbf{Z})$, à coefficients rationnels, et de poids k_m. Comme les k_m tendent vers k dans X, le théorème sera démontré si l'on prouve que $\lim.f_m = f$, i.e. que $v_p(f_m - f)$ tend vers l'infini avec m. Or cela résulte du lemme plus précis suivant :

LEMME 9. On a $v_p(f_m - f) \geq \mathrm{Inf}(m + 1 + v_p(f),\ p^m + 1 + v_p(f|_k W) - \frac{k}{2})$.

(Noter que, si $f \neq 0$, $v_p(f)$ et $v_p(f|_k W)$ sont finis, puisque les séries f et $f|_k W$ ont des coefficients à dénominateurs bornés, cf. n° 3.1.)

Ecrivons $f_m - f$ sous la forme $(f_m - fg^{p^m}) + f(g^{p^m} - 1)$. D'après le lemme 8, on a $g \equiv 1 \pmod{p}$ d'où $g^{p^m} \equiv 1 \pmod{p^{m+1}}$, et

$$v_p(f(g^{p^m} - 1)) \geq m + 1 + v_p(f).$$

D'autre part, le lemme 7 montre que

$$f_m - fg^{p^m} = p^{1-k_m/2}(fg^{p^m}|_{k_m} W)|U,$$

d'où $\quad v_p(f_m - fg^{p^m}) \geq 1 - k_m/2 + v_p(f|_k W) + p^m v_p(g|_a W)$;

en appliquant le lemme 8, on en déduit :

$$v_p(f_m - fg^{p^m}) \geq 1 - (k + ap^m)/2 + v_p(f|_k W) + p^m(1 + a/2)$$

$$\geq p^m + 1 + v_p(f|_k W) - k/2.$$

Le lemme 9 résulte de ces formules et de l'inégalité évidente :

$$v_p(f_m - f) \geq \mathrm{Inf}(v_p(f_m - fg^{p^m}),\quad v_p(f(g^{p^m} - 1))).$$

Remarque

Nous avons supposé f holomorphe aux deux pointes ∞ et 0. Il suffirait en fait que f soit holomorphe en ∞ et méromorphe en 0. La démonstration est la même que ci-dessus; on remarque que la forme g s'annule en 0, donc que fg^{p^m} est une forme modulaire pour m assez grand, et l'on a ici encore $f = \lim.\mathrm{Tr}(fg^{p^m})$.

Ainsi, si l'on pose

$$j = Q^3/\Delta = q^{-1} + \sum_{n=0}^{\infty} c(n)\, q^n,$$

on peut appliquer le th.10 à la fonction $f = j|U = \sum c(pn)\, q^n$, qui a un pôle d'ordre p à la pointe 0. On en conclut que $j|U$ est une forme modulaire p-adique de poids 0; on retrouve - sous une forme plus faible - un théorème de Deligne ([6], §7).

3.3. Réduction (mod.p) des formes de poids 2 sur $\Gamma_0(p)$

Le th.10 montre que la réduction (mod.p) d'une forme modulaire sur $\Gamma_0(p)$, à coefficients p-entiers, est une forme modulaire (mod.p) sur $SL_2(\mathbf{Z})$, au sens du n° 1.2. Dans le cas du poids 2, on peut donner un résultat plus précis :

THÉORÈME 11. On suppose $p \geqslant 3$. Soit f une forme modulaire de poids 2 sur $\Gamma_0(p)$, à coefficients rationnels p-entiers.

(a) On a $f|_2 W = -f|U$; c'est une forme à coefficients p-entiers.

(b) La réduction $\tilde{f}$ de f (mod.p) appartient à l'espace $\tilde{M}_{p+1}$ du n° 1.2.

(c) Inversement, tout élément de $\tilde{M}_{p+1}$ est réduction (mod.p) d'une forme modulaire de poids 2 sur $\Gamma_0(p)$, à coefficients p-entiers.

(En d'autres termes, il y a identité entre :

réduction (mod.p) des formes modulaires de poids 2 sur $\Gamma_0(p)$

et

réduction (mod.p) des formes modulaires de poids p+1 sur $SL_2(\mathbf{Z})$.)

L'assertion (a) est bien connue (Hecke [8], p.777). On la démontre en remarquant que toute forme de poids 2 sur $SL_2(\mathbf{Z})$ est nulle, et que l'on a donc $\mathrm{Tr}(f|_2 W) = 0$; or d'après le lemme 7, $\mathrm{Tr}(f|_2 W)$ est égal à $f|_2 W + f|U$.

Démontrons (b) et (c) en supposant d'abord $p \geq 5$. Posons

$$g = E_{p-1} - p^{(p-1)/2} E_{p-1}|W = E_{p-1} - p^{p-1} E_{p-1}|V,$$

cf. démonstration du th.10. La fonction fg est une forme modulaire de poids p+1 sur $\Gamma_0(p)$, à coefficients p-entiers; sa trace $\mathrm{Tr}(fg)$ appartient à M_{p+1}. De plus, le lemme 9 du n° 3.2, appliqué à $m = 0$ et $k = 2$, montre que $v_p(\mathrm{Tr}(fg) - f) \geq 1$, i.e. que

$$f \equiv \mathrm{Tr}(fg) \pmod{p},$$

d'où $\tilde{f} \in \tilde{M}_{p+1}$, ce qui démontre (b) pour $p \geq 5$. Soit maintenant N le sous-espace vectoriel de $\tilde{M}_{p+1}$ formé des fonctions telles que $\tilde{f}$. La dimension de N est égale à la dimension de l'espace des formes modulaires de poids 2 sur $\Gamma_0(p)$, i.e. 1 + g(Y) où g(Y) désigne le genre de la courbe Y définie par $\Gamma_0(p)$. La valeur de g(Y) est bien connue (cf. par exemple Hecke [8], p.810) : si l'on écrit $p = 12a + b$, avec $b = 1,5,7,11$, on a $g(Y) = a - 1, a, a, a + 1$ respectivement. D'autre part, on sait que

$$\dim.M_k = \begin{cases} [k/12] & \text{si } k \equiv 2 \pmod{12} \\ 1 + [k/12] & \text{si } k \not\equiv 2 \pmod{12}. \end{cases} \qquad (k \text{ pair} \geq 0)$$

On en déduit que $\dim.\tilde{M}_{p+1} = 1 + g(Y) = \dim.N$, d'où le fait que $N = \tilde{M}_{p+1}$, ce qui démontre (c) dans le cas $p \geq 5$.

Reste le cas $p = 3$. L'espace $\tilde{M}_4$ a pour base $\tilde{Q} = 1$. D'autre part, on a $g(Y) = 0$, et les formes de poids 2 sur $\Gamma_0(3)$ sont simplement les multiples de la série d'Eisenstein $E_2^* = P - 3P|V$, cf. Hecke [8], p.817.

Comme $\tilde{E}_2^* = \tilde{P} = 1$, les assertions (b) et (c) sont évidentes.

COROLLAIRE. Les valeurs propres de U sur $\tilde{M}_{p+1}$ sont égales à ± 1.

En effet, le th.11 montre que $\tilde{f}|U^2 = \tilde{f}|W^2 = \tilde{f}$ pour tout $\tilde{f} \in \tilde{M}_{p+1}$.

Remarque. Cette démonstration a également été obtenue par Atkin.

Exemples

1) Pour p = 11, 17, 19, le genre de Y est 1. Il existe une unique forme parabolique de poids 2 sur $\Gamma_0(p)$:

$$f_p = a_1 q + a_2 q^2 + \ldots, \quad \text{avec} \quad a_1 = 1.$$

La série de Dirichlet correspondante $\sum a_n/n^s$ est essentiellement la fonction zêta de Y ([22], p.182). D'après le th.11, f_p est congru (mod.p) à une forme parabolique de poids 12, 18, 20 sur $SL_2(\mathbf{Z})$; on en déduit les congruences :

$$f_{11} \equiv \Delta \pmod{11}; \quad f_{17} \equiv R\Delta \pmod{17}; \quad f_{19} \equiv Q^2\Delta \pmod{19}.$$

La première de ces congruences peut aussi se déduire de l'identité :

$$f_{11} = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, \qquad \text{cf. [22], p.49.}$$

2) Pour p = 23, 31, le genre de Y est 2. Le nombre de classes du corps $\mathbf{Q}(\sqrt{-p})$ est 3. Soit χ un caractère d'ordre 3 du groupe des classes d'idéaux de ce corps, et posons

$$g_p = \sum \chi(a)\, q^{Na} = \begin{cases} q - q^2 - q^3 + q^6 + \ldots & (p = 23) \\ q - q^2 - q^5 - q^7 + \ldots & (p = 31) \end{cases},$$

la sommation étant étendue à tous les idéaux entiers a. Il n'est pas difficile de voir que $g_p = \frac{1}{2}(\theta_1 - \theta_2)$, où θ_1 (resp. θ_2) est la série

thêta associée à la forme binaire $m^2 + mn + \frac{p+1}{4} n^2$ (resp. à la forme $2m^2 + mn + \frac{p+1}{8} n^2$). Il en résulte (cf. [8], p.478-479) que g_p est une forme modulaire de poids 1 sur $\Gamma_o(p)$, de "Nebentypus" au sens de Hecke (cf. n° 3.4 ci-après). Son carré est une forme de poids 2, commençant par le terme q^2. Appliquant le th.11, on en déduit les congruences

$$g_{23}^2 \equiv \Delta^2 \pmod{23} \quad \text{et} \quad g_{31}^2 \equiv Q^2\Delta^2 \pmod{31},$$

d'où, en extrayant les racines carrées,

$$g_{23} \equiv \Delta \pmod{23} \quad \text{et} \quad g_{31} \equiv Q\Delta \pmod{31}.$$

La première de ces congruences peut aussi se déduire de l'identité

$$g_{23} = q \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{23n});$$

elle est due à Wilton; voir là-dessus [27], p.34.

3.4. Formes de "Nebentypus" sur $\Gamma_o(p)$

On suppose $p \geq 3$. Soit ε un caractère (mod.p), i.e. un homomorphisme du groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ dans $\mathbf{C}^*$. Si n est un entier de réduction mod.p égale à $\tilde{n}$, on pose

$$\varepsilon(n) = 0 \quad \text{si} \quad \tilde{n} = 0 \quad \text{et} \quad \varepsilon(n) = \varepsilon(\tilde{n}) \quad \text{sinon.}$$

On étend ε à $\Gamma_o(p)$ par :

$$\varepsilon(\gamma) = \varepsilon(a)^{-1} = \varepsilon(d) \quad \text{si} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Cela a un sens puisque $ad \equiv 1 \pmod{p}$.

Soit $k \in \mathbf{Z}$. Une fonction f sur H est appelée une forme modulaire de

type (k, ε) sur $\Gamma_0(p)$ si elle est holomorphe sur H et vérifie les deux conditions :

(i) $f|_k\gamma = \varepsilon(\gamma)f$ pour tout $\gamma \in \Gamma_0(p)$;

(ii) f est holomorphe aux pointes de $\Gamma_0(p)$.

Lorsque $\varepsilon' = 1$ ("Haupttypus" de Hecke [8], p.809), on retrouve la notion de forme modulaire de poids k, au sens du n° 3.1; le cas $\varepsilon \neq 1$ est celui appelé "Nebentypus" par Hecke.

Si $f \neq 0$, on a $k \geq 0$, et $\varepsilon(-1) = (-1)^k$; autrement dit, k est pair si $\varepsilon(-1) = 1$ et impair si $\varepsilon(-1) = -1$.

Une telle forme f a un développement en série

$$\sum_{n=0}^{\infty} a_n q^n,$$

avec $a_n \in \mathbf{C}$. Notons μ_{p-1} le groupe des racines (p-1)-ièmes de 1. Nous allons voir que, si les a_n appartiennent au corps $\mathbf{Q}(\mu_{p-1})$, la série f "est" une forme modulaire p-adique (ce qui généralisera le th.10). De façon plus précise, on sait que p se décompose complètement dans $\mathbf{Q}(\mu_{p-1})$ en idéaux premiers de degré 1 :

$$p_1, \ldots, p_r \quad \text{avec} \quad r = \phi(p-1) = [\mathbf{Q}(\mu_{p-1}) : \mathbf{Q}].$$

Choisissons un de ces idéaux premiers, ce qui définit un plongement σ de $\mathbf{Q}(\mu_{p-1})$ dans le corps p-adique $\mathbf{Q}_p$; comme le groupe des racines (p-1)-ièmes de l'unité de $\mathbf{Q}_p$ s'identifie canoniquement à $(\mathbf{Z}/p\mathbf{Z})^*$ ("représentants multiplicatifs"), on voit que σ définit un isomorphisme de μ_{p-1} sur $(\mathbf{Z}/p\mathbf{Z})^*$, et tout isomorphisme est obtenu ainsi (en choisissant convenablement p_i). En composant $\varepsilon : (\mathbf{Z}/p\mathbf{Z})^* \to \mu_{p-1}$ et $\sigma : \mu_{p-1} \to (\mathbf{Z}/p\mathbf{Z})^*$ on obtient un endomorphisme de $(\mathbf{Z}/p\mathbf{Z})^*$, qui est nécessairement de la forme $x \mapsto x^\alpha$, avec $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$. Avec ces notations, on a :

THÉORÈME 12. Soit $f = \sum a_n q^n$ une forme modulaire de type (k, ε) sur $\Gamma_0(p)$, telle que $a_n \in \mathbf{Q}(\mu_{p-1})$ pour tout n. Alors la série

$$f^\sigma = \sum a_n^\sigma q^n, \quad \underline{\text{à coefficients}} \quad a_n^\sigma \in \mathbf{Q}_p,$$

<u>est une forme modulaire</u> p-<u>adique de poids</u> $k + \alpha$.

(Précisons que α est identifié à l'élément $(0, \alpha)$ du groupe des poids $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, et $k + \alpha$ à $(k, k+\alpha)$. On peut supposer $f \neq 0$, d'où $\varepsilon(-1) = (-1)^k$, et il en résulte que $k + \alpha$ est un élément <u>pair</u> de X.)

Lorsque $\varepsilon = 1$, f est combinaison $\mathbf{Q}(\mu_{p-1})$-linéaire de formes modulaires de poids k (au sens du n° 3.1) à coefficients rationnels, et le th.12 résulte du th.10; nous pouvons donc supposer $\varepsilon \neq 1$.

Commençons par un cas particulier :

LEMME 10. <u>Si</u> $k \geq 1$, <u>et</u> $\varepsilon(-1) = (-1)^k$, <u>la série</u>

$$G_k(\varepsilon) = \frac{1}{2} L(1-k, \varepsilon) + \sum_{n=1}^{\infty} \Big(\sum_{d|n} \varepsilon(d)\, d^{k-1} \Big) q^n$$

<u>est une forme modulaire de type</u> (k, ε) <u>sur</u> $\Gamma_o(p)$. <u>Ses coefficients appartiennent à</u> $\mathbf{Q}(\mu_{p-1})$, <u>et l'on a</u>

$$G_k(\varepsilon)^\sigma = G_h^*,$$

<u>où</u> G_h^* <u>est la série d'Eisenstein</u> p-<u>adique de poids</u> $h = k + \alpha$, <u>au sens du</u> n° 1.6.

Le fait que $G_k(\varepsilon)$ soit de type (k, ε) résulte de la détermination par Hecke des séries d'Eisenstein de niveau p (cf. [8], p.461-486, ainsi que l'<u>Appendice</u> du §5). De façon plus précise, avec les notations de [8], <u>loc.cit.</u>, on vérifie que $G_k(\varepsilon)$ est égale, à un facteur scalaire près, à la fonction

$$\sum_{\lambda \in (\mathbf{Z}/p\mathbf{Z})^*} \varepsilon(\lambda)^{-1}\, G_k(z; 0, \lambda, p);$$

comme $G_k(z;0,\lambda,p)|_k \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = G_k(z;0,d\lambda,p)$ si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_o(p)$, on en

déduit, par un calcul immédiat, que $G_k(\varepsilon)|_k \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \varepsilon(d)\, G_k(\varepsilon)$, ce qui montre bien que $G_k(\varepsilon)$ est de type (k, ε). Ses coefficients appartiennent au corps engendré par les valeurs de ε, qui est contenu dans $\mathbf{Q}(\mu_{p-1})$. Montrons maintenant que $G_k(\varepsilon)^\sigma$ est égale à G_h^*. Si $n \geq 1$, le n-ième coefficient a_n^σ de $G_k(\varepsilon)^\sigma$ est égal à $\sum \varepsilon(d)^\sigma\, d^{k-1}$, la sommation portant sur les diviseurs d de n qui sont premiers à p. Ecrivons d dans $\mathbf{Q}_p$ sous la forme $\omega(d)\,\langle d\rangle$, avec $\omega(d)^{p-1} = 1$, et $\langle d\rangle \equiv 1 \pmod{p}$, cf. Iwasawa [11], p.18. On a alors $\varepsilon(d)^\sigma = \omega(d)^\alpha = d^\alpha$, vu la définition de α. D'où

$$a_n^\sigma = \sum d^{k+\alpha-1} = \sigma_{h-1}^*(n),$$

ce qui est bien le n-ième coefficient de G_h^*. D'autre part, $L(1-k, \varepsilon)^\sigma$ est égal à $-b_k(\omega^\alpha)/k = L_p(1-k, \omega^{k+\alpha})$, avec les notations de [11], §3. Vu le th.3 du n° 1.6, on a donc

$$L(1-k, \varepsilon)^\sigma = \zeta^*(1-k, 1-k-\alpha) = \zeta^*(1-h);$$

le terme constant de $G_k(\varepsilon)^\sigma$ est égal à celui de G_h^*, ce qui achève la démonstration du lemme.

Revenons maintenant au th.12. Choisissons une suite d'entiers $k_n \geq 1$ tendant vers α dans X, et tels que $k_n - \alpha \in (p-1)X$ pour tout n. Posons

$$g_n = \lambda_n^{-1} G_{k_n}(\varepsilon^{-1}),$$

où λ_n est le terme constant de la série $G_{k_n}(\varepsilon^{-1})$, cf. lemme 10. Le produit fg_n est une forme modulaire sur $\Gamma_o(p)$ de type $(k + k_n, 1)$; il en résulte, comme on l'a dit plus haut, que $f^\sigma g_n^\sigma$ est une forme modulaire p-adique de poids $k + k_n$. D'autre part, d'après le lemme 10 appliqué à k_n et ε^{-1}, on a $g_n^\sigma = E_{h_n}^*$, où $h_n = k_n - \alpha$. Comme h_n tend vers 0 dans X, il en résulte que g_n^σ tend vers $E_o^* = 1$, d'où $\lim. f^\sigma g_n^\sigma = f^\sigma$, ce qui

montre que f^σ est modulaire p-adique de poids $k + \alpha = \lim.(k + k_n)$ et achève la démonstration.

Remarque

Sous les hypothèses du th.12, on peut démontrer que $f|_k W$ est de type (k, ε^{-1}); on a $f|_k W^2 = \varepsilon(-1)f$.

§4. Familles analytiques de formes modulaires p-adiques

4.1. L'algèbre d'Iwasawa ($p \neq 2$)

a) Notations

Si $n \geq 1$, on note U_n le sous-groupe de $\mathbf{Z}_p^*$ formé des entiers p-adiques u tels que $u \equiv 1 \pmod{p^n}$. On sait que

$$U_1 \simeq \varprojlim (U_1/U_n)$$

est isomorphe à $\mathbf{Z}_p$. Si $s \in \mathbf{Z}_p$ et $u \in U_1$, on définit de façon évidente $u^s \in U_1$, cf. n° 1.4, a).

On note F l'algèbre des fonctions sur $\mathbf{Z}_p$, à valeurs dans $\mathbf{Z}_p$. Si $u \in U_1$, on note f_u la fonction $s \longmapsto u^s$. Les $f_u (u \in U_1)$ engendrent un sous-$\mathbf{Z}_p$-module L de F, qui est une sous-algèbre. D'après le théorème d'indépendance des caractères (Dedekind), les f_u forment une base de L, et l'on peut identifier L à l'algèbre $\mathbf{Z}_p[U_1]$ du groupe U_1. Un élément de L s'écrit donc, de façon unique, sous la forme

$$s \longmapsto f(s) = \sum_{u \in U_1} \lambda_u u^s, \quad \text{avec} \quad \lambda_u \in \mathbf{Z}_p,$$

les λ_u étant presque tous nuls.

b) L'algèbre $\overline{L}$

On définit $\overline{L}$ comme l'adhérence de L dans F, pour la topologie de la convergence uniforme. Notons d'ailleurs que les éléments de L sont équicontinus : si $f \in L$ et $n > 0$, on a

$$s \equiv s' \pmod{p^n} \Rightarrow f(s) \equiv f(s') \pmod{p^{n+1}}.$$

La même propriété est donc vraie pour $\overline{L}$; de plus, sur $\overline{L}$, la topologie de la convergence uniforme coïncide avec celle de la convergence simple sur un sous-espace dense, et cette topologie fait de $\overline{L}$ un espace compact.

c) L'algèbre Λ

C'est l'algèbre $\mathbf{Z}_p[[U_1]] = \varprojlim \mathbf{Z}_p[U_1/U_n]$, cf. [10], [11]. On sait qu'elle est isomorphe à l'algèbre $\mathbf{Z}_p[[T]]$ des séries formelles en une indéterminée T. L'isomorphisme s'obtient en choisissant un générateur topologique $u = 1 + \pi$ de U_1, avec $v_p(\pi) = 1$, et en associant à l'élément f_u de $\mathbf{Z}_p[U_1]$ l'élément $1 + T$ de $\mathbf{Z}_p[[T]]$.

L'anneau Λ est un anneau local régulier de dimension 2; il joue un rôle essentiel dans les travaux d'Iwasawa sur les classes d'idéaux des extensions cyclotomiques (le groupe U_1 intervenant alors comme un groupe de Galois). On notera que Λ est compact pour la topologie définie par les puissances de son idéal maximal; lorsqu'on identifie Λ à $\mathbf{Z}_p[[T]]$, cette topologie devient celle de la convergence simple des coefficients; le groupe topologique Λ est donc isomorphe à un produit infini de groupes $\mathbf{Z}_p$.

d) Identification de $\overline{L}$ à Λ.

Les algèbres $\overline{L}$ et Λ contiennent toutes deux $L = \mathbf{Z}_p[U_1]$ comme sous-algèbre dense. Il s'impose de les comparer :

LEMME 11. Il existe un unique isomorphisme d'algèbres topologiques

$$\varepsilon : \Lambda \to \overline{L}$$

dont la restriction à $\mathbf{Z}_p[U_1]$ soit l'identité.

L'unicité de ε résulte de ce que $\mathbf{Z}_p[U_1]$ est dense dans Λ. Pour en montrer l'existence, identifions comme ci-dessus Λ à $\mathbf{Z}_p[[T]]$ au moyen du choix d'un générateur topologique u de U_1. Si $f = \sum a_n T^n$ est un élément de Λ, on définit $\varepsilon(f)$ comme la fonction

$$s \longmapsto f(u^s - 1) = \sum a_n (u^s - 1)^n,$$

ce qui a un sens car $u^s - 1 \equiv 0 \pmod{p}$. Il est clair que ε est un homomorphisme continu de Λ dans F, et que $\varepsilon(f_u) = f_u$; il en résulte que ε est l'identité sur L; par continuité, on a donc $\varepsilon(\Lambda) = \overline{L}$. Le fait que ε soit injectif est immédiat; comme Λ est compact, c'est un homéomorphisme.

Remarques

1) Dans ce qui suit, nous identifierons Λ à $\overline{L}$ au moyen de ε. Comme on vient de le voir, cela revient à passer d'une série en T à une fonction de s par le "changement de variables"

$$T = u^s - 1 = vs + \ldots + v^n s^n/n! + \ldots, \quad \text{où} \quad v = \log(u).$$

2) Il y a une troisième interprétation de Λ, due à B.Mazur, qui est souvent utile : c'est l'algèbre des "distributions" (ou "mesures") à valeurs dans $\mathbf{Z}_p$ sur l'espace U_1. On appelle ainsi toute fonction $U \longmapsto \mu(U)$, définie sur les ouverts compacts de U_1, simplement additive, et à valeurs dans $\mathbf{Z}_p$; une telle mesure se prolonge par continuité en une forme linéaire

$$f \longmapsto \int_{U_1} f(u)\mu(u)$$

sur l'espace des fonctions continues sur U_1 à valeurs dans $\mathbf{Z}_p$. Si l'on associe à μ la fonction $s \longmapsto \int_{U_1} u^s \, \mu(u)$,

on obtient un élément de Λ; tout élément de Λ s'obtient ainsi, de manière unique; les éléments de L correspondent aux mesures discrètes.

e) Zéros d'un élément de Λ

Tout élément $f \neq 0$ de $\Lambda = \mathbf{Z}_p[[T]]$ a une "décomposition de Weierstrass" canonique :

$$f = p^{\mu}(T^{\lambda} + a_1 T^{\lambda-1} + \ldots + a_{\lambda})\, u(T),$$

avec λ, $\mu \geq 0$, $v_p(a_i) \geq 1$, et u inversible dans Λ. En particulier, le nombre de zéros de f(s) est fini et $\leq \lambda$.

Comme application, signalons :

LEMME 12. Soit $f_1, \ldots, f_n, \ldots$ une suite d'éléments de Λ. On suppose que $\lim. f_n(s)$ existe pour tout élément s d'une partie infinie S de $\mathbf{Z}_p$. Alors les f_n convergent uniformément sur $\mathbf{Z}_p$ vers une fonction f appartenant à Λ.

Sinon, vu la compacité de Λ, on pourrait extraire de la suite (f_n) deux suites convergeant vers des éléments distincts f' et f" de Λ. La fonction f' - f" s'annulerait sur S, donc aurait une infinité de zéros, contrairement à ce que l'on vient de voir.

(La famille Λ se comporte comme une "famille normale" au sens de Montel.)

4.2. L'algèbre d'Iwasawa ($p = 2$)

On définit encore U_n comme le sous-groupe de $\mathbf{Z}_p^*$ formé des entiers 2-adiques u tels que $u \equiv 1 \pmod{2^n}$. On a

$$\mathbf{Z}_p^* = U_1 = \{\pm 1\} \times U_2$$

et U_2 est isomorphe à $\mathbf{Z}_2$; si $u \in U_1$, on note $\omega(u)$ sa composante dans $\{\pm 1\}$ et $\langle u \rangle$ sa composante dans U_2, cf. [11], p.18.

On définit les algèbres L et Λ au moyen du groupe U_2 (et non plus du groupe U_1). De façon plus précise, L est l'algèbre engendrée par les fonctions $f_u : s \longmapsto u^s$, avec $u \in U_2$. On montre, comme au n° 4.1, que l'adhérence $\overline{L}$ de L s'identifie à l'algèbre d'Iwasawa

$$\Lambda = \mathbf{Z}_2[[U_2]] = \varprojlim \mathbf{Z}_2[U_2/U_n].$$

Ici encore, cette algèbre est isomorphe à $\mathbf{Z}_2[[T]]$, l'isomorphisme s'obtenant en choisissant un générateur topologique u de U_2 et en associant à l'élément f_u de $\mathbf{Z}_2[U_2]$ l'élément $1 + T$ de $\mathbf{Z}_2[[T]]$, cf. [11], p.69.

Les autres résultats du n° 4.1 se transposent de manière évidente au cas $p = 2$.

4.3. Caractérisation des éléments de Λ par leurs développements en série

Nous allons voir que les fonctions f appartenant à Λ peuvent être caractérisées comme des séries de Taylor convergentes

$$f(s) = \sum_{n=0}^{\infty} a_n s^n,$$

dont les coefficients a_n vérifient certaines congruences. Pour écrire commodément ces congruences, définissons des entiers c_{in} $(1 \leq i \leq n)$ par l'identité

$$\sum_{i=1}^{n} c_{in} Y^i = Y(Y-1)(Y-2)\ldots(Y-n+1) = n!\binom{Y}{n}.$$

On a alors :

THÉORÈME 13. Pour qu'une fonction $f \in F$ appartienne à Λ, il faut et il suffit qu'il existe des entiers p-adiques b_n $(n = 0,1,\ldots)$ tels que

a) $f(s) = \sum_{n=0}^{\infty} b_n p^n s^n/n!$ pour tout $s \in \mathbf{Z}_p$,

b) $v_p(\sum_{i=1}^{n} c_{in} b_i) \geq v_p(n!)$ pour tout $n \geq 1$.

(Si p = 2, on doit modifier a) en remplaçant p^n par 4^n.)

Remarques

1) Comme $c_{nn} = 1$, la condition b) équivaut à dire que chacun des b_n est congru (mod.$n!\mathbf{Z}_p$) à une certaine combinaison $\mathbf{Z}$-linéaire des b_j, $j < n$.

2) On a

$$v_p(b_n p^n/n!) \geq n - v_p(n!) \geq n\frac{p-2}{p-1} \quad \text{si} \quad p \neq 2$$

$$v_2(b_n 4^n/n!) \geq 2n - v_2(n!) \geq n \quad \text{si} \quad p = 2.$$

Il en résulte que la série entière donnant f converge dans un disque p-adique strictement plus grand que le disque unité; a fortiori, elle converge sur $\mathbf{Z}_p$, ce qui donne un sens à a).

Démonstration du th.13

Je me borne au cas $p \neq 2$; le cas $p = 2$ est analogue.

(i) Le développement

$$T = vs + \ldots + v^n s^n/n! + \ldots, \quad \text{avec} \quad v_p(v) = 1,$$

donné au n° 4.1 montre que T, ainsi que ses puissances, a un développement en série du type a). Par linéarité et passage à la limite, on voit qu'il en est de même de toute fonction f de Λ. De plus les coefficients $b_n = b_n(f)$ de f dépendent continûment de f. On en conclut que l'application $f \longmapsto (b_n(f))$ est un isomorphisme du groupe compact Λ sur un certain sous-module fermé S_Λ du $\mathbf{Z}_p$-module produit $S = (\mathbf{Z}_p)^{\mathbf{N}}$ des suites

$(b_n)_{n \geq 0}$. Tout revient donc à montrer que S_Λ coïncide avec le sous-module S_b de S défini par les congruences b).

(ii) Tout élément u de U_1 s'écrit exp(py), avec $y \in \mathbf{Z}_p$. On en conclut que

$$u^s = \exp(pys) = \sum_{n=0}^{\infty} y^n p^n s^n / n!,$$

i.e. que $b_n(f_u) = y^n$. Or la suite (y^n) appartient à S_b. On a en effet

$$\sum c_{in} y^n = y(y-1)\ldots(y-n+1) = n! \binom{y}{n},$$

et l'on sait que $\binom{y}{n}$ est un entier p-adique; cela montre bien que $\sum c_{in} y^n$ est divisible par n! dans $\mathbf{Z}_p$.

Par linéarité et passage à la limite on conclut de là que S_Λ est contenu dans S_b. Il reste à voir que S_Λ est égal à S_b; vu ce qui précède, cela équivaut à dire que les suites de la forme (y^n), avec $y \in \mathbf{Z}_p$, engendrent un sous-$\mathbf{Z}_p$-module dense de S_b.

(iii) Soit $m \geq 1$ et soient $b_0, \ldots, b_m \in \mathbf{Z}_p$ satisfaisant aux congruences b) pour $n \leq m$. Nous allons montrer qu'il existe $f \in \Lambda$ tel que $b_i(f) = b_i$ pour $0 \leq i \leq m$, ce qui achèvera la démonstration.

On procède par récurrence sur m, le cas m = 0 étant évident. Vu l'hypothèse de récurrence, il existe $g \in \Lambda$ tel que $b_i(g) = b_i$ pour $i \leq m-1$; tout revient à trouver $h \in \Lambda$ tel que $b_i(h) = 0$ pour $i \leq m-1$ et $b_m(h) = b_m - b_m(g)$. On est donc ramené au cas où les b_i sont nuls pour $i \leq m-1$; vu la congruence b) il en résulte que b_m est de la forme $m!\, z$, avec $z \in \mathbf{Z}_p$. On prend alors pour f le monôme $z(p/v)^m T^m$, avec les notations de (i); il est clair qu'il répond à la question.

COROLLAIRE. Soit $f \in \Lambda$, et soient b_n les coefficients correspondants. On a $b_n \equiv b_{n+p-1} \pmod{p}$ pour tout $n \geq 1$.

En effet, cette congruence est évidente lorsque la suite (b_n) est de la forme (y^n), avec $y \in \mathbf{Z}_p$, et le cas général s'en déduit par linéarité

et passage à la limite. (Bien entendu, on peut aussi utiliser b).)

Remarque

Signalons une autre propriété de stabilité de l'algèbre Λ :

$$\underline{\text{si}} \quad f \in \Lambda, \quad \underline{\text{on a}} \quad \frac{df}{ds} \in p\Lambda \quad \underline{\text{si}} \quad p \neq 2 \quad \underline{\text{et}} \quad \frac{df}{ds} \in 4\Lambda \quad \underline{\text{si}} \quad p = 2.$$

Cela résulte de la formule $\frac{df}{ds} = v(1 + T)\frac{df}{dT}$.

4.4. Caractérisation des éléments de Λ par des propriétés d'interpolation

Soient $s_o, s_1 \in \mathbf{Z}_p$ et $f \in F$. Posons $a_n = a_n(f) = f(s_o + ns_1)$ pour $n = 0, 1, \ldots$ et désignons par $\delta_o, \delta_1, \ldots, \delta_n, \ldots$ les différences successives de la suite (a_n) :

$$\delta_o = a_o, \quad \delta_1 = a_1 - a_o, \quad \delta_2 = a_2 - 2a_1 + a_o, \ldots,$$

$$\delta_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_{n-i}.$$

THÉORÈME 14. Posons

$$h = 1 + v_p(s_1) \quad \underline{\text{si}} \quad p \neq 2 \quad \underline{\text{et}} \quad h = 2 + v_2(s_1) \quad \underline{\text{si}} \quad p = 2.$$

Si $f \in \Lambda$, on a

a) $\delta_n \equiv 0 \pmod{p^{nh}}$ pour tout $n \geq 0$,

b) $v_p\left(\sum_{i=1}^{n} c_{in}\delta_i p^{-ih}\right) \geq v_p(n!)$ pour tout $n \geq 1$.

(On rappelle que c_{in} est le coefficient de Y^i dans le polynôme $Y(Y - 1)\ldots(Y - n + 1)$, cf. n° 4.3.)

Il suffit de considérer le cas où $f(s) = u^s$ avec $u \in U_1$ (resp. avec $u \in U_2$ si $p = 2$); le cas général s'en déduira par linéarité et passage

à la limite. On a alors

$$a_n = u^{s_o u^{ns_1}} \quad \text{et} \quad \delta_n = u^{s_o}(u^{s_1} - 1)^n.$$

Or $u^{s_1} - 1$ est de la forme $p^h y$, avec $y \in \mathbf{Z}_p$. On a donc $v_p(\delta_n) \geq nh$, ce qui prouve a). L'assertion b) provient de ce que

$$\sum_{i=1}^{n} c_{in}\delta_i p^{-ih} = u^{s_o}(\sum c_{in} y^i) = u^{s_o} y(y-1)\ldots(y-n+1)$$

$$= n!\, u^{s_o}\binom{y}{n} \equiv 0 \pmod{n!\mathbf{Z}_p}.$$

COROLLAIRE. *Posons* $e_n = \delta_n p^{-nh}$. *On a* $e_n \equiv e_{n+p-1} \pmod{p}$ *pour tout* $n \geq 1$.

La démonstration est la même que celle du corollaire au th.13.

En fait, les congruences de th.14 *caractérisent* les éléments de l'algèbre d'Iwasawa Λ. De façon plus précise, prenons $s_o = 0$ et $s_1 = 1$, de sorte que $a_n = f(n)$, et que les δ_n sont les coefficients d'interpolation usuels; on sait (critère de Mahler, cf. [1]) que, si f est continue, les δ_n tendent vers 0, et que l'on a

$$f(s) = \sum_{n=0}^{\infty} \delta_n \binom{s}{n} \quad \text{pour tout} \quad s \in \mathbf{Z}_p.$$

THÉORÈME 15. *Soit* f *une fonction continue sur* $\mathbf{Z}_p$, *à valeurs dans* $\mathbf{Q}_p$, *et soient* $\delta_n = \sum (-1)^i \binom{n}{i} f(n-i)$ *ses coefficients d'interpolation. Pour que* f *appartienne à* Λ, *il faut et il suffit que* :

a) $\delta_n \equiv 0 \pmod{p^n}$ *pour tout* $n \geq 0$,

b) $v_p(\sum_{i=1}^{n} c_{in}\delta_i p^{-i}) \geq v_p(n!)$ *pour tout* $n \geq 1$.

(Si $p = 2$, on doit remplacer p^n par 4^n dans a), et p^{-i} par 4^{-i} dans b).)

La nécessité résulte du th.14. Prouvons la suffisance, en nous bornant au cas $p \neq 2$ (le cas $p = 2$ est analogue). Soit S_b l'ensemble des suites (b_n) d'entiers p-adiques tels que

$$v_p(\sum c_{in} b_i) \geq v_p(n!) \quad \text{pour tout} \quad n \geq 1.$$

On a vu au n° 4.2 que les suites de la forme (y^n), avec $y \in \mathbf{Z}_p$, engendrent un sous-module dense de S_b pour la topologie produit. Par hypothèse, la suite $(\delta_n p^{-n})$ appartient à S_b. Pour tout entier m on peut donc choisir des éléments λ_i, y_i de $\mathbf{Z}_p$, en nombre fini, tels que

$$\delta_n p^{-n} = \sum \lambda_i y_i^n \quad \text{pour tout} \quad n \leq m.$$

Posons $$f_m(s) = \sum \lambda_i (1 + py_i)^s.$$

On a $f_m \in \Lambda$ (et même $f_m \in L$); de plus les formules ci-dessus montrent que les coefficients d'interpolation de f_m sont les mêmes que ceux de f jusqu'à l'indice m; on a donc $f_m(n) = f(n)$ pour $n \leq m$, et la suite (f_m) tend vers f pour la topologie de la convergence simple sur l'ensembel $\mathbf{N}$ des entiers ≥ 0. Comme $\mathbf{N}$ est dense dans $\mathbf{Z}_p$, cela entraîne que $f = \lim.f_m$, cf. n° 4.1 b), et par suite on a bien $f \in \Lambda$.

4.5. Exemple : coefficients des séries d'Eisenstein p-adiques

Considérons la série

$$G_k^* = \frac{1}{2}\zeta^*(1 - k) + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n)\, q^n \quad (k \in X, \ k \text{ pair} \neq 0)$$

définie au n° 1.6. Ecrivons k sous la forme $k = (s,u)$, avec :

$$s \in \mathbf{Z}_p, \quad u \in \mathbf{Z}/(p-1)\mathbf{Z}, \quad u \text{ pair (si } p \neq 2), \quad s \text{ pair (si } p = 2).$$

Les coefficients de $G_k^* = G_{s,u}^*$ sont :

$$a_o(G_{s,u}^*) = \tfrac{1}{2}\zeta^*(1 - s, 1 - u)$$

$$a_n(G_{s,u}^*) = \sigma_{k-1}^*(n) = \sum_{\substack{d|n \\ (d,p)=1}} d^{k-1} \quad \text{si} \quad n \geq 1.$$

Décomposons l'unité p-adique d en $\omega(d)\,\langle d\rangle$, avec

$$\omega(d)^{p-1} = 1, \quad \langle d\rangle \in U_1 \quad \text{si} \quad p \neq 2,$$

$$\omega(d) = \pm 1, \quad \langle d\rangle \in U_2 \quad \text{si} \quad p = 2.$$

On a alors :

$$a_n(G_{s,u}^*) = \sum d^{-1}\, \omega(d)^k\, \langle d\rangle^k = \sum d^{-1}\, \omega(d)^u\, \langle d\rangle^s \quad (n \geq 1).$$

On en conclut que, pour u et n fixés (avec $n \geq 1$) la fonction

$$s \longmapsto a_n(G_{s,u}^*)$$

appartient à l'algèbre L du n° 4.1, et a fortiori à son adhérence Λ. (Noter que, si $u = 0$, cette fonction n'est définie que pour $s \neq 0$; si $p = 2$, elle n'est même définie que pour $s \in 2\mathbf{Z}_2$, $s \neq 0$.)

On a un résultat analogue, mais beaucoup moins évident, pour le terme constant $a_o(G_{s,u}^*)$:

THÉORÈME 16 (Iwasawa).

a) Si u est un élément pair $\neq 0$ de $\mathbf{Z}/(p-1)\mathbf{Z}$, la fonction

$$s \longmapsto a_o(G_{s,u}^*) = \tfrac{1}{2}\zeta^*(1-s, 1-u)$$

appartient à l'algèbre Λ.

b) Si $u = 0$, la fonction

$$s \longmapsto a_0(G^*_{s,u}) = \tfrac{1}{2}\zeta^*(1-s, 1)$$

est de la forme $T^{-1}g(T)$, où g est un élément inversible de Λ.

(Dans b), on a identifié Λ à $\mathbf{Z}_p[[T]]$, cf. n^{os} 4.1 et 4.2.)

Cet énoncé est simplement une reformulation des principaux résultats de [10], compte tenu de ce que $\zeta^*(1-s, 1-u) = L_p(1-s; \omega^u)$, cf. n° 1.6, th.3 (i). Voir aussi [11], §6.

Remarques

1) Dans le cas $u \neq 0$, le th.16, combiné avec le th.14 a) redonne les classiques congruences de Kummer (cf. Fresnel [7] et Shiratani [23]); le th.14 b) donne des congruences supplémentaires, peut-être nouvelles.

2) Dans le cas $u = 0$, le th.16 montre que la fonction

$$s \longmapsto 2\zeta^*(1-s, 1)^{-1}$$

appartient à Λ et est divisible par T (elle a un "zéro simple" en $T = 0$). Il en résulte que les coefficients $a_n(E^*_{s,0})$ de la série

$$E^*_{s,0} = \frac{2}{\zeta^*(1-s, 1)}\, G^*_{s,0}$$

appartiennent à Λ et sont divisibles par T si $n \geqslant 1$.

4.6. Familles de formes modulaires p-adiques (poids non divisible par $p - 1$)

Considérons une forme modulaire p-adique f_s dépendant d'un paramètre $s \in \mathbf{Z}_p$ et de poids $k(s) \in 2X$. On suppose que $k(s)$ est de la forme (rs, u), avec $r \in \mathbf{Z}$ et $u \in \mathbf{Z}/(p-1)\mathbf{Z}$ indépendants de s. On suppose en outre que u est $\neq 0$ (ce qui entraîne $p \neq 2, 3$); le cas $u = 0$ sera traité au n° suivant.

THÉORÈME 17. Supposons que, pour tout $n \geqslant 1$, la fonction $s \longmapsto a_n(f_s)$ appartienne à l'algèbre d'Iwasawa Λ. Il en est alors de même de la fonction $s \longmapsto a_o(f_s)$.

Nous allons utiliser la série d'Eisenstein p-adique E^*_{-rs} de poids -rs, normalisée de telle sorte que son terme constant soit 1, cf. n° 1.6. Ecrivons-la sous la forme

$$E^*_{-rs} = \sum_{n=0}^{\infty} e_n(s)q^n, \quad \text{avec} \quad e_o(s) = 1.$$

On a vu au n° précédent que les coefficients de E^*_s appartiennent à Λ; il en est donc de même des $e_n(s)$; on a de plus $e_n(0) = 0$ si $n \geqslant 1$ puisque $E^*_o = 1$.

La fonction $f'_s = f_s E^*_{-rs}$ est une forme modulaire p-adique de poids (0,u) indépendant de s. Ses coefficients sont donnés par :

$$a_m(f'_s) = e_m(s)a_o(f_s) + \sum_{i=1}^{m} e_{m-i}(s)a_i(f_s).$$

D'après le th.9 du n° 2.3, appliqué à k = (0,u), il existe une suite $(\lambda_{m,n})_{m,n \geqslant 1}$ d'éléments de $\mathbb{Z}_p$, avec $\lambda_{m,n} = 0$ pour m assez grand (dépendant de n), telle que

$$a_o(f'_s) = \lim_{n \to \infty} \sum_m \lambda_{m,n}\, a_m(f'_s).$$

Comme f_s et f'_s ont même terme constant, ceci peut se récrire :

$$a_o(f_s) = \lim_{n \to \infty} \left(\sum_m \lambda_{m,n} e_m(s) a_o(f_s) + \sum_{m,i \geq 1} \lambda_{m,n} e_{m-i}(s) a_i(f_s) \right).$$

Posons $g_n(s) = \sum_m \lambda_{m,n}\, e_m(s)$. Les fonctions g_n appartiennent à Λ, qui est compact. Quitte à remplacer la suite (n) par une sous-suite, on peut donc supposer que les $g_n(s)$ convergent dans Λ vers un élément g; comme $g_n(0) = 0$ pour tout n, on a $g(0) = 0$. La formule ci-dessus peut alors se récrire :

$$(1 - g(s))a_o(f_s) = \lim_{n \to \infty} b_n(s),$$

$$\text{avec} \quad b_n(s) = \sum_{m,i \geq 1} \lambda_{m,n}\, e_{m-i}(s) a_i(f_s).$$

Vu l'hypothèse faite sur les $a_i(f_s)$, les fonctions b_n appartiennent à Λ pour tout n. Comme ces fonctions convergent simplement vers la fonction

$$s \longmapsto (1 - g(s))a_o(f_s),$$

on en déduit que cette dernière fonction appartient à Λ, cf. n° 4.1, lemme 12. Mais le fait que $g(0) = 0$ entraîne que g appartient à l'idéal maximal de Λ, et $1 - g$ est inversible dans Λ. On en conclut bien que $s \longmapsto a_o(f_s)$ appartient à Λ.

4.7. Familles de formes modulaires p-adiques (poids divisible par p-1)

Considérons, comme au n° précédent, une forme modulaire p-adique f_s dépendant d'un paramètre s. Nous supposons maintenant que f_s est définie pour tout $s \neq 0$ de $\mathbf{Z}_p$ (resp. pour tout $s \neq 0$ de $2\mathbf{Z}_2$ si $p = 2$), et que son poids $k(s)$ est de la forme $rs = (rs,0)$ où r est un entier non nul.

Convenons de dire qu'une fonction sur $\mathbf{Z}_p - \{0\}$ (resp. sur $2\mathbf{Z}_2 - \{0\}$) appartient à Λ si elle est la restriction d'une fonction de Λ.

THÉORÈME 18. Supposons que, pour tout $n \geq 1$, la fonction $s \longmapsto a_n(f_s)$

appartienne à Λ. Il en est alors de même de la fonction

$$s \longmapsto 2\zeta^*(1 - rs, 1)^{-1}\, a_o(f_s).$$

Identifions Λ à $\mathbf{Z}_p[[T]]$ comme d'habitude. D'après le th.16, la fonction $s \longmapsto 2\zeta^*(1 - s, 1)^{-1}$ est de la forme $T.h(T)$, où h est un élément inversible de Λ. Comme $s \longmapsto rs$ correspond à $1 + T \longmapsto (1 + T)^r$, on en conclut que la fonction $s \longmapsto 2\zeta^*(1 - rs, 1)^{-1}$ est de la forme $((1 + T)^r - 1)g(T)$, avec g inversible dans Λ. D'où :

COROLLAIRE. La fonction $s \longmapsto a_o(f_s)$ appartient au corps des fractions de Λ; on peut l'écrire $c(T)/((1 + T)^r - 1)$, avec $c \in \Lambda$.

Remarque

Si q est la plus grande puissance de p qui divise r, on peut mettre $(1 + T)^r - 1$ sous la forme $u(T)((1 + T)^q - 1)$, où u est un élément inversible de Λ. On peut donc récrire la fonction $s \longmapsto a_o(f_s)$ comme une fraction $d(T)/((1 + T)^q - 1)$, avec $d \in \Lambda$.

Démonstration du th.18

Choisissons un polynôme H en U et les T_ℓ, à coefficients entiers, qui satisfasse aux conditions du th.8 du n° 2.3 : pour tout $k \in \mathbf{Z}_p$, on a

(i) $E_k^*|_k H = c(k)\, E_k^*$ avec $c(k)$ inversible dans $\mathbf{Z}_p$,

(ii) $\lim_{n \to \infty} f|_k H^n = 0$ pour toute forme modulaire p-adique f de poids k qui est parabolique.

D'après le cor. au th.8, on a

$$2\zeta^*(1 - rs, 1)^{-1}\, a_o(f_s) = \lim_{n \to \infty} c(rs)^{-n}\, a_1(f_s|_{rs}\, H^n),$$

et tout revient à montrer que les fonctions

$$s \longmapsto c(rs)^{-n} \quad \text{et} \quad s \longmapsto a_1(f_s|_{rs}\ H^n)$$

appartiennent à Λ (en effet, on sait qu'une suite de fonctions de Λ qui converge en tout point d'une partie infinie de $\mathbf{Z}_p$ converge uniformément vers une fonction de Λ, cf. n° 4.1, lemme 12). Or on a le résultat suivant :

LEMME 13. *Soit* R *un polynôme en* U *et les* T_ℓ, *à coefficients dans* $\mathbf{Z}_p$. *Il existe une famille de fonctions* $k \longmapsto c_{ij}(R,k)_{i,j \geq 0}$, *appartenant à sous-algèbre* L *de* Λ (cf. n° 4.1) *et telles que, pour tout* $i \geq 0$, *on ait* :

a) $c_{ij}(R,k) = 0$ *pour* j *assez grand, pour* $j = 0$ *si* $i \geq 1$, *et pour* $j \geq 1$ *si* $i = 0$;

b) $a_i(f|_k\ R) = \sum_j c_{ij}(R,k)\ a_j(f)$ *pour toute série formelle p-adique* f, *et tout* $k \in 2\mathbf{Z}_p$.

Lorsque R est égal à U, ou à l'un des T_ℓ, le lemme résulte des formules donnant $f|U$ et $f|_k\ T_\ell$, cf. n° 2.1. Le cas général s'en déduit en remarquant que, si l'énoncé est vrai pour deux polynômes R_1 et R_2, il l'est aussi pour R_1R_2 et $R_1 + R_2$.

Revenons à la démonstration du th.18. On a

$$a_1(f_s|_{rs}\ H^n) = \sum_{j \geq 1} c_{1j}(H^n, rs)\ a_j(f_s),$$

et cette formule montre bien que $s \longmapsto a_1(f_s|_{rs}\ H^n)$ appartient à Λ.

On a d'autre part $c(k) = a_o(E_k^*|_k\ H) = c_{oo}(H,k)$, ce qui montre que $k \longmapsto c(k)$ appartient à L, et il en est de même de $s \longmapsto c(rs)$. De plus, d'après (i), les valeurs prises par c(rs) sont des unités p-adiques. Si l'on écrit $s \longmapsto c(rs)$ comme une série en T, le terme constant de cette série est inversible dans $\mathbf{Z}_p$; la série elle-même est donc inversible dans $\Lambda = \mathbf{Z}_p[[T]]$, et l'on en conclut que $s \longmapsto c(rs)^{-n}$ appartient à Λ quel que soit n, ce qui achève le démonstration du théorème.

Remarque

Dans les ths.17 et 18, il n'est pas nécessaire de supposer f_s définie pour tout $s \in \mathbf{Z}_p$ (ou tout $s \neq 0$); il suffit de se donner les f_s pour s appartenant à une partie infinie S de $\mathbf{Z}_p$, et de faire l'hypothèse suivante : pour tout $n \geqslant 1$, la fonction $s \longmapsto a_n(f_s)$ est la restriction à S d'une fonction appartenant à Λ.

§5. Fonctions zêta p-adiques

5.1. Notations

La lettre K désigne un corps de nombres algébriques totalement réel de degré r sur $\mathbf{Q}$: $K \otimes_{\mathbf{Q}} \mathbf{R}$ est isomorphe à $\mathbf{R}^r$. L'anneau des entiers de K est noté 0_K, sa différente (par rapport à $\mathbf{Z}$) est notée d et son discriminant d.

Si x (resp. a) est un élément (resp. un idéal) de K, on note Nx (resp. Na) sa norme, qui est un élément (resp. un élément positif) de $\mathbf{Q}$; par exemple $d = Nd$. On note Tr(x) la trace de x.

Un élément x de K est dit totalement positif si $\sigma(x) > 0$ pour tout plongement $\sigma : K \to \mathbf{R}$. On écrit alors $x \gg 0$; on a $Tr(x) > 0$.

La fonction zêta de K est définie par la formule

$$\zeta_K(s) = \sum Na^{-s} = \prod (1 - Np^{-s})^{-1}$$

où a (resp. p) parcourt l'ensemble des idéaux $\neq 0$ (resp. des idéaux premiers $\neq 0$) de 0_K. Cette formule vaut pour $R(s) > 1$. On prolonge ζ_K en une fonction méromorphe sur $\mathbf{C}$, ayant pour seul pôle (simple) le point $s = 1$. La fonction

$$d^{s/2}\,\pi^{-rs/2}\,\Gamma\left(\frac{s}{2}\right)^{r}\,\zeta_K(s)$$

est invariante par $s \longmapsto 1 - s$ ("équation fonctionnelle"). On en déduit que, si n est un entier ≥ 1, on a

$\zeta_K(1 - n) = 0$ si n est impair (le cas $r = 1$, $n = 1$ excepté)

$\zeta_K(1 - n) \neq 0$ si n est pair.

De plus, d'après un théorème énoncé par Hecke ([8], p.387) et démontré par Siegel [24], les $\zeta_K(1 - n)$, $n \geq 1$, sont des nombres rationnels.

5.2. Formes modulaires attachées à K

Soit k un entier pair ≥ 2. Définissons une série formelle g_k

$$g_k = \sum_{n=0}^{\infty} a_n(g_k)\, q^n$$

par les formules :

$$a_o(g_k) = 2^{-r}\zeta_K(1 - k),$$

$$a_n(g_k) = \sum_{\substack{\mathrm{Tr}(x)=n \\ x \in d^{-1} \\ x \gg 0}} \sum_{a \mid xd} (N\mathfrak{a})^{k-1} \qquad (n \geq 1),$$

où x parcourt les éléments totalement positifs de d^{-1} de trace n, et $\mathfrak{a}$ les idéaux de 0_K contenant $x\mathfrak{d}$. (Il revient au même de dire que l'on somme sur les couples $(x,\mathfrak{a})$ tels que $\mathfrak{a}$ soit entier, $x \in d^{-1}\mathfrak{a}$, $x \gg 0$ et $\mathrm{Tr}(x) = n$; c'est une somme finie.)

THÉORÈME 19 (Hecke-Siegel). Mis à part le cas $r = 1$, $k = 2$, la série g_k est une forme modulaire sur $SL_2(\mathbb{Z})$ de poids rk.

(Pour r = 1, i.e. $K \simeq \mathbf{Q}$, on a $g_k = G_k$, d'où la nécessité d'exclure $k = 2$, cf. n° 1.1.)

Si u est un idéal fractionnaire de K, on trouve dans Siegel [25], p.93, la définition d'une certaine fonction

$$F_k(u, z_1, \ldots, z_r), \qquad \mathrm{Im}(z_i) > 0,$$

qui est une <u>série d'Eisenstein</u> du corps K, au sens de Hecke [8], p.381-404; c'est une forme modulaire de poids k par rapport au groupe $SL_2(O_K)$ opérant sur le produit H^r de r demi-plans de Poincaré. Si l'on restreint $F_k(u, z_1, \ldots, z_r)$ à la diagonale H de H^r, on obtient une fonction

$$\Phi_k(u,z) = F_k(u, z, \ldots, z),$$

qui est une forme modulaire de poids rk, au sens usuel. Les coefficients de $\Phi_k(u,z)$ sont donnés dans [25], p.94, formule (19). Les fonctions $F_k(u, z_1, \ldots, z_r)$ et $\Phi_k(u,z)$ ne changent pas lorsqu'on multiplie u par un idéal principal. Posons alors

$$\Phi_k(z) = \sum_u \Phi_k(u,z),$$

où u parcourt un ensemble de représentants des classes d'idéaux de K. Les formules (18) et (19) de [25] donnent :

$$a_n(\Phi_k) = e_k a_n(g_k) \quad \text{pour} \quad n \geq 1, \quad \text{où} \quad e_k = d^{\frac{1}{2}-k} \left(\frac{(2\pi i)^k}{(k-1)!}\right)^r,$$

ainsi que

$$a_o(\Phi_k) = \zeta_K(k),$$

et l'équation fonctionnelle de ζ_K permet de récrire cette dernière formule sous la forme :

$$a_o(\Phi_k) = e_k\, 2^{-r}\zeta_K(1-k) = e_k a_o(g_k).$$

On a donc $g_k = e_k^{-1}\Phi_k$, ce qui montre bien que g_k est modulaire de poids rk.

COROLLAIRE.

(i) Si $rk \not\equiv 0 \pmod{p-1}$, $\zeta_K(1-k)$ est p-entier.

(ii) Si $rk \equiv 0 \pmod{p-1}$, on a

$$v_p(\zeta_K(1-k)) \geqslant -1 - v_p(rk) \qquad (p \neq 2)$$

$$v_p(\zeta_K(1-k)) \geqslant r - 2 - v_p(rk) \qquad (p = 2).$$

Cela résulte du cor.1 au th.1' du n° 1.5, compte tenu de ce que les coefficients $a_n(g_k)$ sont entiers pour $n \geqslant 1$. (Voir aussi [20], th.6 et th.6'.)

Remarques

1) Le corollaire ci-dessus fournit une estimation du dénominateur de $\zeta_K(1-k)$. Cette estimation est assez grossière : elle ne fait intervenir K que par l'intermédiaire de son degré r; pour k = 2, elle est moins bonne que celle donnée par la formule

$$\zeta_K(-1) = \text{caract.d'E-P. de } SL_2(O_K),$$

cf. [19], n° 3.7, prop.29-30.

2) Nous aurons besoin plus loin d'une variante du th.19, dans laquelle on modifie g_k en gardant uniquement les termes "premiers à p". De façon plus précise, soit S l'ensemble des idéaux premiers de O_K qui divisent p, et posons

$$\zeta_{K,S}(s) = \zeta_K(s) \prod_{p \in S}(1 - Np^{-s}) = \prod_{p \notin S}(1 - Np^{-s})^{-1}$$

$$= \sum_{(a,p)=1} Na^{-s}.$$

Définissons une série formelle g'_k par les formules

$$a_o(g'_k) = 2^{-r}\zeta_{K,S}(1-k) = 2^{-r}\zeta_K(1-k) \prod_{p \in S}(1 - Np^{k-1})$$

et $$a_n(g'_k) = \sum_{x,a} (Na)^{k-1} \qquad (n \geqslant 1),$$

où la sommation porte sur les couples (x,a), avec a entier premier à p, $x \in d^{-1}a$, $x \gg 0$ et $Tr(x) = n$.

On a alors :

THÉORÈME 19'. *La série g'_k est une forme modulaire sur $\Gamma_o(p)$ de poids rk (cf. n° 3.1).*

(Noter qu'ici le cas $r = 1$, $k = 2$ n'est plus exclu.)

La démonstration est analogue à celle du th.19, à cela près que l'on doit utiliser des séries d'Eisenstein de niveau p, cf. Kloosterman [14] et Siegel [26]. Pour plus de détails, voir l'exemple 2) de l'Appendice placé à fin de ce §.

5.3. La fonction zêta p-adique du corps K

Soit k un élément pair de X tel que $rk \neq 0$. Nous allons associer à k une forme modulaire p-adique g^*_k, de poids rk, par passage à la limite à partir des formes g_k du n° 5.2. Le procédé est le même que celui utilisé au n° 1.6 dans le cas de $\mathbf{Q}$. On choisit une suite d'entiers pairs $k_i \geqslant 4$ tels que $|k_i| \to \infty$ et $k_i \to k$ dans X. Si u est un entier p-adique, on a

$$\lim_{i \to \infty} u^{k_i} = 0 \quad \text{si} \quad u \equiv 0 \pmod{p}, \text{ et } \lim_{i \to \infty} u^{k_i} = u^k \quad \text{sinon,}$$

la convergence étant uniforme en u. On en conclut que

$$\lim_{i \to \infty} a_n(g_{k_i}) = \sum_{x,a} (Na)^{k-1}, \qquad (n \geqslant 1),$$

où la sommation porte sur les couples (x,a), avec a idéal de 0_K premier à p, $x \in d^{-1}a$, $x \gg 0$ et $\mathrm{Tr}(x) = n$; de plus, la convergence est uniforme en n. Appliquant alors le cor.2 au th.1' du n° 1.5, on en déduit que les g_{k_i} ont une limite g_k^* qui est une forme modulaire p-adique de poids rk, indépendante de la suite k_i choisie. Le terme constant de g_k^* sera noté $2^{-r}\zeta_K^*(1-k)$, de sorte que l'on a

$$a_o(g_k^*) = 2^{-r}\zeta_K^*(1-k) = 2^{-r} \lim_{i \to \infty} \zeta_K(1-k_i),$$

$$a_n(g_k^*) = \sum_{\substack{\mathrm{Tr}(x)=n \\ x \in d^{-1} \\ x \gg 0}} \sum_{\substack{a \mid xd \\ (a,p)=1}} (Na)^{k-1}, \qquad n \geq 1.$$

La fonction ζ_K^* ainsi définie sera appelée la fonction zêta p-adique du corps K; elle prend ses valeurs dans $\mathbf{Q}_p$.

THÉORÈME 20. Si k est un entier pair ≥ 2, on a

$$\zeta_K^*(1-k) = \zeta_{K,S}(1-k) = \zeta_K(1-k) \prod_{p \in S} (1 - Np^{k-1}).$$

(Rappelons que S est l'ensemble des idéaux premiers p qui divisent p.)

En effet, revenons à la série g_k' du n° précédent. D'après le th.19', cette série est une forme modulaire sur $\Gamma_o(p)$ de poids rk, donc aussi une forme modulaire p-adique de poids rk, cf. n° 3.2, th.10. Comme $a_n(g_k') = a_n(g_k^*)$ pour $n \geq 1$, on en déduit que $a_o(g_k') = a_o(g_k^*)$, d'où le théorème.

Remarque

Il est immédiat que ζ_K^* est continue sur l'ensemble des $1-k$, avec k pair et $rk \neq 0$. Le th.20 en fournit donc une caractérisation : c'est le prolongement par continuité de la fonction

$$m \longmapsto \zeta_{K,S}(m),$$

définie sur l'ensemble des entiers impairs < 0. (En particulier, lorsque K est abélien sur $\mathbf{Q}$, ζ_K^* coïncide avec la fonction zêta p-adique de K au sens de Kubota-Leopoldt, cf. [11], p.62, puisque cette dernière a la même propriété.)

En fait, ζ_K^* est même analytique. De façon plus précise, décomposons $k \in X$ en (s,u), avec $s \in \mathbf{Z}_p$, $u \in \mathbf{Z}/(p-1)\mathbf{Z}$, de sorte que la condition $rk \neq 0$ signifie simplement que $s \neq 0$ ou $ru \neq 0$. Ecrivons $\zeta_K^*(1-k)$ sous la forme $\zeta_K^*(1-s, 1-u)$. On a alors :

THÉORÈME 21. Soit u un élément pair de $\mathbf{Z}/(p-1)\mathbf{Z}$, $p \neq 2$.

(a) Si $ru \neq 0$, la fonction $s \longmapsto \zeta_K^*(1-s, 1-u)$ appartient à l'algèbre d'Iwasawa $\Lambda = \mathbf{Z}_p[[T]]$ du §4.

(b) Si $ru = 0$, la fonction $s \longmapsto \zeta_K^*(1-s, 1-u)$ est de la forme $h(T)/((1+T)^r - 1)$, avec $h \in \Lambda$.

THÉORÈME 21'. Si $p = 2$, la fonction $s \longmapsto \zeta_K^*(1-s)$ est de la forme $2^r h(T)/((1+T)^r - 1)$, avec $h \in \Lambda$.

(Noter que, pour $p = 2$, $\zeta_K^*(1-s)$ est défini pour $s \in 2\mathbf{Z}_2$, $s \neq 0$.)

Posons $k = (s,u)$. Si $n \geq 1$, la fonction $s \longmapsto a_n(g_k^*)$ est somme de fonctions de la forme $s \longmapsto (N\mathfrak{a})^{k-1}$, où $N\mathfrak{a}$ est une unité p-adique. En décomposant $N\mathfrak{a}$ à la façon habituelle (cf. n° 4.5) en $\omega(N\mathfrak{a})\langle N\mathfrak{a}\rangle$, on a

$$(N\mathfrak{a})^{k-1} = N\mathfrak{a}^{-1}\,\omega(N\mathfrak{a})^u\,\langle N\mathfrak{a}\rangle^s,$$

ce qui montre que $s \longmapsto a_n(g_k^*)$ appartient à l'algèbre L du n° 4.1. Les théorèmes 21 et 21' résultent alors des ths.17 et 18 du §4, appliqués à la famille (g_k^*).

COROLLAIRE 1. Si $ru \neq 0$ et $p \neq 2$, la fonction $s \longmapsto \zeta_K^*(1-s, 1-u)$ est holomorphe (au sens strict) dans un disque strictement plus grand que le disque unité.

En effet, le th.21 (a), combiné au th.13 du n° 4.3, montre que la fonction en question est donnée par une série de Taylor

$$\sum_{n=0}^{\infty} c_n s^n, \quad \text{avec} \quad v_p(c_n) \geq n\frac{p-2}{p-1}.$$

Une telle série converge dans un disque strictement plus grand que le disque unité.

COROLLAIRE 2. Si $ru = 0$, la fonction $s \mapsto \zeta_K^*(1 - s, 1 - u)$ est méromorphe (au sens strict) dans un disque strictement plus grand que le disque unité; si elle n'est pas holomorphe, elle a pour unique pôle le point $s = 0$, et c'est un pôle simple.

Cela se démontre de la même manière, en tenant compte du dénominateur $(1 + T)^r - 1 = u^{rs} - 1$, où u est un générateur topologique de U_1 (resp. de U_2 si $p = 2$); on vérifie en effet que $u^{rs} - 1$ peut s'écrire sous la forme $s/\phi(s)$, où ϕ est une série de Taylor convergeant dans un disque strictement plus grand que le disque unité.

COROLLAIRE 3. Soient a et b des entiers positifs. On suppose que a est pair ≥ 2, $ra \not\equiv 0 \pmod{p-1}$, et $b \equiv 0 \pmod{p-1}$. Les différences successives δ_n de la suite $a_n = \zeta_{K,S}(1 - a - nb)$ satisfont alors aux congruences

$$\delta_n \equiv 0 \pmod{p^n} \quad \text{et} \quad \sum_{i=1}^{n} c_{in}\delta_i p^{-i} \equiv 0 \pmod{n!\mathbf{Z}_p}, \quad \text{cf. n° 4.4.}$$

(Le fait que $\delta_n \equiv 0 \pmod{p^n}$ est une généralisation des congruences de Kummer.)

Vu le th.20, on a $a_n = \zeta_K^*(1 - a - nb, 1 - a)$. Le corollaire résulte de là, et des ths.21 et 14.

5.4. Complément : calcul de $\zeta_K^*(1 - k, 1 - u)$ pour k entier ≥ 1

On suppose u pair et $p \neq 2$. Le cas où $k \equiv u \pmod{p-1}$ est réglé par le th.20 : on a $\zeta_K^*(1 - k, 1 - u) = \zeta_{K,S}(1 - k)$. On va voir qu'il y a un résultat analogue dans le cas général, la fonction zêta étant remplacée par une fonction L.

De façon plus précise, soit ε un homomorphisme de $(\mathbf{Z}/p\mathbf{Z})^*$ dans $\mathbf{C}^*$ tel que $\varepsilon(-1) = (-1)^k$. Si a est un idéal premier à p, posons $\varepsilon_K(a) = \varepsilon(Na)$; la fonction ε_K définit un caractère du corps de nombres K; l'ensemble des idéaux premiers où ce caractère est ramifié est un sous-ensemble S_ε de S. Nous aurons besoin de la fonction $L(s,\varepsilon_K)$ de ε_K, ainsi que de la fonction $L_S(s, \varepsilon_K)$ déduite de $L(s, \varepsilon_K)$ par suppression des facteurs non premiers à p; on a :

$$L_S(s, \varepsilon_K) = \prod_{p \notin S} (1 - \varepsilon_K(p)Np^{-s})^{-1}$$

$$= L(s, \varepsilon_K) \prod_{p \in S-S_\varepsilon} (1 - \varepsilon_K(p)Np^{-s}).$$

Choisissons maintenant un plongement σ du corps $\mathbf{Q}(\mu_{p-1})$ dans $\mathbf{Q}_p$, cf. n° 3.4, de sorte que ε devient $x \longmapsto x^\alpha$, avec $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$.

THÉORÈME 22. On a $L_S(1 - k, \varepsilon_K)^\sigma = \zeta_K^*(1 - k, 1 - u)$, où $u = k + \alpha$.

(Pour u, k et σ donnés, il existe un ε et un seul tel que $u = k + \alpha$; le th.22 fournit donc bien un procédé de calcul de $\zeta_K^*(1 - k, 1 - u)$.)

Considérons la série $f_{k,\varepsilon}$ donnée par :

$$a_o(f_{k,\varepsilon}) = 2^{-r} L_S(1 - k, \varepsilon_K),$$

$$a_n(f_{k,\varepsilon}) = \sum_{x,a} \varepsilon_K(a)\, Na^{k-1}, \qquad n \geq 1,$$

où la sommation porte comme ci-dessus sur les (x, a), avec a premier à p, $x \in d^{-1}a$, $x \gg 0$ et $Tr(x) = n$. La série $f_{k,\varepsilon}$ est une forme modulaire sur $\Gamma_o(p)$ de type (rk, ε^r) au sens du n° 3.4, cf. Appendice, Exemple 3). D'après le th.12 du n° 3.4, il en résulte que la série p-adique $f_{k,\varepsilon}^\sigma$ est une forme modulaire p-adique de poids $rk + r\alpha$. Or, si $n \geq 1$, on a

$$a_n(f^{\sigma}_{k,\varepsilon}) = \sum_{x,a} \varepsilon_K(a)^{\sigma} (Na)^{k-1} = \sum_{x,a} \omega(Na)^{\alpha} (Na)^{k-1}$$

$$= \sum_{x,a} (Na)^{k+\alpha-1} = a_n(g^{*}_{k+\alpha}), \qquad \text{cf. n° 5.3.}$$

Comme $g_{k+\alpha}$ et $f^{\sigma}_{k,\varepsilon}$ ont même poids, et que ce poids est non nul, les formules ci-dessus entraînent $g^{*}_{k+\alpha} = f^{\sigma}_{k,\varepsilon}$. On a donc

$$2^{-r} L_S(1 - k, \varepsilon_K)^{\sigma} = a_o(f^{\sigma}_{k,\varepsilon}) = a_o(g^{*}_{k+\alpha}) = 2^{-r}\zeta^{*}_K(1 - k - \alpha),$$

d'où le théorème.

Remarque

Il résulte de l'équation fonctionnelle des séries L que l'on a $L(1 - k, \varepsilon_K) \neq 0$. Vu la formule liant L et L_S on en conclut que $\zeta^{*}_K(1 - k, 1 - u)$ est nul si et seulement si $k = 1$ et s'il existe $p \in S - S_\varepsilon$ tel que $\varepsilon_K(p) = 1$. (L'existence d'un tel zéro pour ζ^{*}_K m'a été suggérée par J.Coates - voir aussi [4], th.1.1.)

5.5. Complément : une propriété de périodicité de ζ^{*}_K

On suppose $p \neq 2$. Soit $K(\mu_p)$ le corps obtenu en adjoignant à K les racines p-ièmes de l'unité, et posons $b = [K(\mu_p) : K]$. Du fait que K est réel, b est pair, et divise p-1.

THÉORÈME 23. On a $\zeta^{*}_K(1 - s, 1 - u) = \zeta^{*}_K(1 - s, 1 - u')$ si $u' \equiv u \pmod{b}$.

Notons Y_b le sous-groupe de $\mathbf{Z}/(p-1)\mathbf{Z}$ engendré par b, et identifions Y_b à un sous-groupe de X. Il s'agit de prouver que $\zeta^{*}_K(1 - k) = \zeta^{*}_K(1-k')$ si $k' \equiv k \pmod{Y_b}$.

Si a est un idéal de K premier à p, on vérifie (soit directement, soit par la théorie du corps de classes) que $Na^b \equiv 1 \pmod{p}$, i.e. que $\omega(Na)$ appartient au noyau de $z \longmapsto z^b$ dans $(\mathbf{Z}/p\mathbf{Z})^{*}$. Il en résulte que, si $k' \equiv k \pmod{Y_b}$, on a $(Na)^{k'} = (Na)^{k}$, d'où $a_n(g^{*}_{k'}) = a_n(g^{*}_{k})$ pour $n \geq 1$. On a d'autre part $p - 1 = ab$, où a est le degré du corps $K \cap \mathbf{Q}(\mu_p)$; il

en résulte que a divise $r = [K:\mathbf{Q}]$, et, si $t \in Y_b$, on a $rt = 0$. Les séries g_k^* et $g_{k'}^*$ ont donc même poids rk. Vu les formules ci-dessus, on a donc $g_k^* = g_{k'}^*$, d'où le théorème.

Remarque

Notons $\mathbf{Q}(\mu)$ le corps engendré sur $\mathbf{Q}$ par toutes les racines p^n-ièmes de l'unité ($n = 1,2, \ldots$). Le degré de $K \cap \mathbf{Q}(\mu)$ est de la forme $a\,p^m$, avec $m \geq 0$. On peut montrer (par un argument analogue à celui du th.23) que, pour tout u, la fonction

$$s \longmapsto \zeta_K^*(1 - s, 1 - u)$$

appartient au corps des fractions de $\mathbf{Z}_p[[T_m]]$, où $T_m = (1 + T)^{p^m} - 1$. Si $ru \neq 0$, cette fonction appartient même à $\mathbf{Z}_p[[T_m]]$.

5.6. Questions

1) Comportement de $\zeta_K^*(1 - s, 1 - u)$ pour $s = 0$

Supposons d'abord $ru \neq 0$, de sorte que $\zeta_K^*(1 - s, 1 - u)$ est défini en $s = 0$. Peut-on calculer ce nombre (en termes de logarithmes p-adiques d'unités de $K(\mu_p)$, par exemple) ? C'est le cas lorsque K est abélien sur $\mathbf{Q}$, en vertu d'un résultat de Leopoldt ([11], §5).

Lorsque $ru = 0$, on aimerait savoir si $s = 0$ est effectivement un pôle. Il paraît probable que ce n'est le cas que si $au = 0$, où a est le degré de $K \cap \mathbf{Q}(\mu_p)$, cf. n° 5.5; cela résulterait en tout cas des conjectures faites dans [19], n° 3.7 et dans [4].

Lorsque $au = 0$ (ou $u = 0$, cela revient au même d'après le th.23), on peut espérer que le résidu de $\zeta_K^*(1 - s, 1 - u)$ en $s = 0$ est lié au régulateur p-adique de K par la même formule que dans le cas abélien ([11], loc.cit.); en outre, on devrait pouvoir remplacer le dénominateur $(1 + T)^r - 1$ du th.21 par $(1 + T)^{p^m} - 1$, où p^m est la plus grande puissance de p divisant le degré de $K \cap \mathbf{Q}(\mu)$, cf. n° 5.5.

2) Généralisations

Le cas traité ici est seulement celui des fonctions zêta. Il y a certainement des résultats analogues pour les fonctions L (abéliennes d'abord, puis non abéliennes). Il devrait être possible de les démontrer en utilisant des formes modulaires p-adiques sur d'autres groupes que $SL_2(\mathbf{Z})$, cf. Katz [12]. Pour obtenir des résultats vraiment satisfaisants (et en particulier pour se débarrasser des pôles parasites, cf. ci-dessus), il sera sans doute nécessaire de travailler sur le groupe modulaire du corps K (et non plus de $\mathbf{Q}$), i.e. d'utiliser les fonctions $F_k(u, z_1, \ldots, z_r)$ et non pas seulement les fonctions d'une variable obtenues en faisant $z_1 = \ldots = z_r$. Le groupe $\mathbf{Z}_p^*$ (ou son sous-groupe U_1) serait remplacé par le groupe de Galois G d'une certaine extension abélienne de K (non nécessairement cyclotomique); l'espace X serait remplacé par l'espace des caractères p-adiques de G, et l'algèbre Λ par $\mathbf{Z}_p[[G]]$.

3) Relations avec la théorie d'Iwasawa

Du point de vue développé dans [10], [11], les éléments de Λ apparaissent, non pas comme des fonctions, mais comme des relations entre éléments de certains modules galoisiens. Pour un corps K abélien sur $\mathbf{Q}$, on a des relations canoniques, les "relations de Stickelberger" qui conduisent aux fonctions zêta et L p-adiques (Iwasawa [10]). Dans le cas général, on ne dispose que de relations définies à multiplication par un élément inversible près (ce qui permet de parler de leurs zéros, cf. Coates-Lichtenbaum [4]). Il est probable que ces relations (ou fonctions) sont essentiellement les mêmes que celles considérées ici; il serait intéressant de le démontrer.

4) Corps non totalement réels

Si K n'est pas totalement réel, on a $\zeta_K(1 - n) = 0$ pour tout entier $n \geq 2$; ce fait pourrait laisser croire que K ne possède pas de fonction zêta p-adique "intéressante". Cependant, pour $K = \mathbf{Q}(i)$, Hurwitz [9] a défini des nombres rationnels qui jouissent de propriétés analogues à

celles des nombres de Bernoulli; les résultats de Hurwitz, ainsi que d'autres plus récents ([5], [17]), laissent penser que les nombres en question conduisent, eux aussi, à des fonctions analytiques p-adiques. Peut-être existe-t-il, plus généralement, une théorie p-adique des fonctions L à Grössencharaktere de type (A_0), au sens de Weil [28] ?

Appendice

Séries d'Eisenstein de niveau $\mathfrak{f}$

Notations

On se donne un idéal $\mathfrak{f} \neq 0$ de O_K, le conducteur. On note $S_{\mathfrak{f}}$ l'ensemble des diviseurs premiers de $\mathfrak{f}$, et l'on écrit

$$\mathfrak{f} = \prod_{p \in S_{\mathfrak{f}}} p^{f(p)}, \quad \text{avec} \quad f(p) \geq 1.$$

Si $\alpha \in K^*$, on dit que α est congru à 1 $(\mathrm{mod}.\mathfrak{f})$, et on écrit $\alpha \equiv 1$ $(\mathrm{mod}^{\times}.\mathfrak{f})$, si $v_p(\alpha - 1) \geq f(p)$ pour tout $p \in S_{\mathfrak{f}}$, où v_p désigne la valuation discrète attachée à p.

Soient a et b deux idéaux fractionnaires de K, premiers à $\mathfrak{f}$. On dit que a et b appartiennent à la même classe $(\mathrm{mod}.\mathfrak{f})$ s'il existe $\alpha \in K^*$, $\alpha \gg 0$, $\alpha \equiv 1$ $(\mathrm{mod}^{\times}.\mathfrak{f})$, tel que a soit le produit de b par l'idéal principal (α). Le groupe des classes d'idéaux $(\mathrm{mod}.\mathfrak{f})$ sera noté $C_{\mathfrak{f}}$; c'est un groupe fini.

Fonction zêta d'une classe

Soit $c \in C_{\mathfrak{f}}$. On lui associe la fonction zêta "partielle"

$$\zeta_{K,c}(s) = \sum_{a \in c} Na^{-s},$$

où la sommation porte sur tous les idéaux de 0_K appartenant à la classe c. Cette fonction se prolonge en une fonction méromorphe dans tout **C**, et ses valeurs aux entiers négatifs sont des nombres rationnels (Siegel [26], p.19).

Plus généralement, soit λ une fonction sur $C_{\mathfrak{f}}$ à valeurs complexes; on identifie λ de façon évidente à une fonction sur les idéaux fractionnaires premiers à $\mathfrak{f}$. On pose

$$\zeta_{K,\lambda}(s) = \sum_{c \in C_{\mathfrak{f}}} \lambda(c)\, \zeta_{K,c} = \sum_{(a,\mathfrak{f})=1} \lambda(a) Na^{-s}.$$

Ici encore, cette fonction se prolonge à tout **C**; ses valeurs aux entiers négatifs sont des combinaisons **Q**-linéaires des $\lambda(c)$. (Il y a parfois intérêt à considérer des fonctions λ à valeurs, non plus dans **C**, mais dans une **Q**-algèbre E - par exemple un corps p-adique - et à définir $\zeta_{K,\lambda}(1-k) \in E$ comme la somme des $\lambda(c)\, \zeta_{K,c}(1-k)$.)

Nous dirons que λ est paire si

$$\lambda((\alpha)a) = \lambda(a) \qquad \text{pour tout } a \text{ et tout } \alpha \equiv 1 \pmod{\overset{\times}{\mathfrak{f}}},$$

et que λ est impaire si

$$\lambda((\alpha)a) = \operatorname{sgn}(N\alpha)\lambda(a) \qquad \text{pour tout } a \text{ et tout } \alpha \equiv 1 \pmod{\overset{\times}{\mathfrak{f}}}.$$

Forme modulaire définie par une fonction λ

On se donne un entier $k \geq 1$, et une fonction λ sur $C_{\mathfrak{f}}$ comme ci-dessus. On suppose que λ et k ont même parité; on exclut les cas $(k = 1, \mathfrak{f} = 0_K)$ et $(k = 2, r = 1, \mathfrak{f} = 0_K)$, cf. [19], p.48.

On associe à k,λ la série formelle $G_{k,\lambda} = \sum_{n=0}^{\infty} a_n(G_{k,\lambda}) q^n$ définie par :

$$a_0(G_{k,\lambda}) = 2^{-r}\, \zeta_{K,\lambda}(1-k)$$

$$a_n(G_{k,\lambda}) = \sum_{x,a} \lambda(a)\, Na^{k-1}, \qquad n \geq 1,$$

où la sommation porte sur les couples (x,a) tels que a soit un idéal de 0_K premier à $\mathfrak{f}$, $x \in d^{-1}a$, $x \gg 0$ et $\operatorname{Tr}(x) = n$.

Soit d'autre part f le générateur > 0 de l'idéal $\mathfrak{f} \cap \mathbf{Z}$ de $\mathbf{Z}$. Notons $\Gamma_0(f)$ le sous-groupe de $SL_2(\mathbf{Z})$ formé des matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ telles que $\gamma \equiv 0$ (mod.f), et $\Gamma_1(f)$ le sous-groupe de $\Gamma_0(f)$ formé des matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ telles que $\alpha \equiv \delta \equiv 1 \pmod{f}$.

THÉORÈME 24 (Kloosterman-Siegel).

(i) La série $G_{k,\lambda}$ définie ci-dessus est une forme modulaire de poids rk sur $\Gamma_1(f)$.

(ii) Si $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ appartient à $\Gamma_0(f)$, on a

$$G_{k,\lambda}|_{rk} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = G_{k,\lambda_\delta},$$

où λ_δ est définie par la formule $\lambda_\delta(a) = \mathrm{sgn}(\delta)^{rk}\, \lambda((\delta)a)$.

Remarque

La définition de λ_δ peut aussi se présenter de la manière suivante : on a un homomorphisme naturel $\rho : (\mathbf{Z}/f\mathbf{Z})^* \to C_\mathfrak{f}$ obtenu en associant à un élément $\xi \in (\mathbf{Z}/f\mathbf{Z})^*$ l'idéal principal (x) engendré par un élément positif x de ξ. Comme δ est inversible mod.f, on peut donc parler de $\rho(\delta) \in C_\mathfrak{f}$, et la définition de λ_δ donnée ci-dessus équivaut simplement à

$$\lambda_\delta(c) = \lambda(\rho(\delta)c) \quad \text{pour tout} \quad c \in C_\mathfrak{f}.$$

Exemples

1) Prenons $\mathfrak{f} = (1)$, $\lambda = 1$, et k pair ≥ 2 (resp. ≥ 4 si $r = 2$). La série $G_{k,\lambda}$ n'est autre que la série g_k du n° 5.2; comme $f = 1$, on en déduit que g_k est une forme modulaire sur le groupe $SL_2(\mathbf{Z})$: on retrouve le th.19.

2) Prenons $\mathfrak{f} = (p)$, $\lambda = 1$ et k pair ≥ 2. On a $f = p$. La série $G_{k,\lambda}$ est égale à la série g'_k du n° 5.2. Comme $\lambda_\delta = \lambda$ pour tout δ premier à p, on en déduit que g'_k est une forme modulaire sur $\Gamma_0(p)$.

3) Les notations étant celles du n° 5.4, prenons $\mathfrak{f} = (p)$, et choisissons pour λ la fonction $a \to \varepsilon_K(a) = \varepsilon(Na)$; prenons $k \geq 1$ tel que

$\varepsilon(-1) = (-1)^k$, ce qui assure que k et λ ont même parité. La série $G_{k,\lambda}$ coïncide avec la série $f_{k,\varepsilon}$ introduite dans la démonstration du th.22 du n° 5.4. Comme on a $\lambda_\delta = \varepsilon(\delta)^r\lambda$, on en déduit que $f_{k,\varepsilon}$ est une forme modulaire de type (rk, ε^r) sur $\Gamma_o(p)$.

Démonstration du th.24

Je me bornerai à indiquer comment on le déduit des résultats de Siegel [26]. Choisissons des représentants $b_1,\ldots,b_h$ des éléments de C_δ, et posons $a_i = b_i d^{-1}\delta^{-1}$. A chaque a_i, Siegel attache une certaine forme modulaire $\phi_i = \phi_{a_i}$, cf. [26], p.48, formule (98). Posons :

$$\phi_\lambda = \sum_{i=1}^{h} \lambda(b_i)\,\phi_i.$$

D'après [26], p.49, ϕ_λ est une forme modulaire de poids rk sur un certain sous-groupe de congruence de $SL_2(\mathbf{Z})$. Son terme constant (avec les notations de [26], loc.cit.) est

$$a_o(\phi_\lambda) = \sum_i \lambda(b_i)Q_k(a_i) = \zeta_{K,\lambda}(1-k), \qquad \text{cf. [26], p.48 et 19.}$$

D'autre part, un calcul sans grande difficulté, basé sur les formules (101) de [26], p.48, montre que l'on a

$$a_n(\phi_\lambda) = 2^r\, a_n(G_{k,\lambda}) \quad \text{pour} \quad n \geq 1.$$

On en déduit que $G_{k,\lambda} = 2^{-r}\phi_\lambda$.

Si maintenant $M = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ est un élément de $\Gamma_o(f)$, on vérifie facilement que $\phi_{\delta a}|M = \mathrm{sgn}(\delta)^{rk}\,\phi_a$. Or, on peut écrire

$$\phi_\lambda = \sum_i \lambda(\delta b_i)\phi_{\delta a_i},$$

puisque les δb_i sont des représentants de C_δ. On en déduit :

$\phi_\lambda|M = \mathrm{sgn}(\delta)^{rk} \sum_i \lambda(\delta b_i)\,\phi_{a_i} = \phi_{\lambda_\delta}$, ce qui établit (i) et (ii).

BIBLIOGRAPHIE

[1] Y.AMICE - Interpolation p-adique, Bull.Soc.math.France, 92, 1964, p.117-160.

[2] A.O.L.ATKIN - Congruences for modular forms, Computers in math. research (R.F.Churchhouse et J-C.Herz ed.), p.8-19, North-Holland, Amsterdam, 1968.

[3] A.O.L.ATKIN et J.LEHNER - Hecke operators on $\Gamma_0(m)$, Math.Ann., 185, 1970, p.134-160.

[4] J.COATES et S.LICHTENBAUM - On ℓ-adic zeta functions, Ann. of Math., 98, 1973, p. 498-550

[5] R.M.DAMERELL - L-functions of elliptic curves with complex multiplication I, Acta Arith., 17, 1970, p.287-301.

[6] B.DWORK - p-adic cycles, Publ.Math.I.H.E.S., 37, 1969, p.27-115.

[7] J.FRESNEL - Nombres de Bernoulli et fonctions L p-adiques, Ann. Inst.Fourier, 17, 1967, p.281-333.

[8] E.HECKE - Mathematische Werke, Vandenhoeck und Ruprecht, Göttingen, 1959 (zw.Aufl. 1970).

[9] A.HURWITZ - Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, Math.Ann., 51, 1899, p.196-226 (Math.Werke, II, p.342-373).

[10] K.IWASAWA - On p-adic L functions, Ann.of Math., 89, 1969, p.198-205.

[11] K.IWASAWA - Lectures on p-adic L functions, Ann.Math.Studies 74, Princeton Univ.Press, 1972.

[12] N.KATZ - p-adic properties of modular schemes and modular forms, ce volume.

[13] H.KLINGEN - Über die Werte der Dedekindschen Zetafunktion, Math. Ann., 145, 1962, p.265-272.

[14] H.D.KLOOSTERMAN - Theorie der Eisensteinschen Reihen von mehreren Veränderlichen, Abh.Math.Sem. Hamb., 6, 1928, p.163-188.

[15] M.KOIKE - Congruences between modular forms and functions and applications to a conjecture of Atkin, J. Fac. Science Univ. Tokyo, 20, 1973, p.129-169

[16] T.KUBOTA et H.W.LEOPOLDT - Eine p-adische Theorie der Zetawerte, J.Crelle, 214-215, 1964, p.328-339.

[17] H.LANG - Kummersche Kongruenzen für die normierten Entwicklungskoeffizienten der Weierstrass'schen $\wp$ -Funktion, Abh.Math. Sem.Hamburg., 33, 1969, p.183-196.

[18] H.W.LEOPOLDT - Eine Verallgemeinerung der Bernoullischen Zahlen, Abh.Math.Sem.Hamburg., 22, 1958, p.131-140.

[19] J-P.SERRE - Cohomologie des groupes discrets, Ann.Math.Studies 70, p.77-169, Princeton Univ.Press, 1971.

[20] J-P.SERRE - Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer), Sém.Bourbaki, 1971/72, exposé 416.

[21] J-P.SERRE - Résumé des cours 1971/72, Annuaire du Collège de France, 1972/73, Paris, p.55-60.

[22] G.SHIMURA - Introduction to the arithmetic theory of automorphic functions, Princeton, 1971.

[23] K.SHIRATANI - Kummer's congruence for generalized Bernoulli numbers and its application, Mem.Kyushu Univ., 26, 1972, p.119-138.

[24] C.L.SIEGEL - Über die analytische Theorie der quadratischen Formen III, Ann.of Math., 38, 1937, p.212-291 (Gesam.Abh. I, p.469-548).

[25] C.L.SIEGEL - Berechnung von Zetafunktionen an ganzzahligen Stellen, Gött.Nach., 10, 1969, p.87-102.

[26] C.L.SIEGEL - Über die Fourierschen Koeffizienten von Modulformen, Gött.Nach., 3, 1970, p.15-56.

[27] H.P.F.SWINNERTON-DYER - On ℓ-adic representations and congruences for coefficients of modular forms, ce volume.

[28] A.WEIL - On a certain type of characters of the idèle-class group of an algebraic number field, Proc.Int.Symp. Tokyo-Nikko, 1955, p.1-7.