RÉSUMÉ DES COURS
DE L'ANNÉE SCOLAIRE 1972 - 1973

I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, professeur

La théorie des formes modulaires p-adiques, esquissée dans le cours précédent, a été reprise et appliquée aux fonctions zêta des corps de nombres algébriques.

1. *Formes modulaires p-adiques*

1.1. *Définition.* Soit $f = \sum_{n=0}^{\infty} a_n q^n$ une série formelle dont les coefficients $a_n(f) = a_n$ appartiennent au corps $\mathbf{Q}_p$ des nombres p-adiques. On dit que f est une forme modulaire p-adique s'il existe une suite f_i de formes modulaires de poids k_i sur $\mathbf{SL}_2(\mathbf{Z})$ dont les coefficients $a_n(f_i)$ soient des nombres rationnels tendant uniformément vers les $a_n(f)$ dans $\mathbf{Q}_p$. On écrit alors

$$f = \lim . f_i.$$

Si $f \neq 0$, on démontre que les k_i ont une limite dans le groupe

$$X = \lim. \mathbf{Z}/(p-1)p^m\mathbf{Z} = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}.$$

Cette limite ne dépend pas du choix de la suite f_i ; on l'appelle le *poids* de f.

1.2. *Exemple.* Si $k \in 2X$, $k \neq 0$, on définit la *série d'Eisenstein* G_k^* de poids k comme limite de séries d'Eisenstein G_{k_i} usuelles. On a

$$G_k^* = \frac{1}{2}\,\zeta^*(1-k) + \sum_{(d,p)=1} d^{k-1}\,\frac{q^d}{1-q^d}.$$

Le terme constant $\zeta^*(1-k)$ de $2G_k^*$ est essentiellement la fonction zêta p-adique de $\mathbf{Q}$, au sens de Kubota-Leopoldt.

1.3. *Opérateurs.* Les formes modulaires p-adiques ont de meilleures propriétés de stabilité que les formes modulaires classiques.

Ainsi, si $f = \sum a_n q^n$ est modulaire p-adique de poids k, il en est de même des séries

$$f|T_l = \sum a_{ln}q^n + l^{k-1}\sum a_n q^{ln} \qquad (l \text{ premier} \neq p),$$

$$f|U = \sum a_{pn}q^n,$$

$$f|V = \sum a_n q^{pn}.$$

De plus, la série

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

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

Les *valeurs propres* de ces opérateurs ont des rapports, encore mal éclaircis, avec certaines représentations de degré 2 du groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

1.4. *Calcul de* $a_0(f)$. Il s'agit d'exprimer le terme constant $a_0(f)$ d'une forme modulaire p-adique f au moyen des $a_n(f)$, avec $n \geqslant 1$. Le cas $p = 2, 3, 5$ ou 7 est particulièrement simple : si f est de poids $k \neq 0$, on a

$$a_0(f) = \frac{1}{2}\,\zeta^*(1-k)\,\lim.a_1(f|U^m) \qquad \text{pour } m \to \infty.$$

Comme

$$a_1(f|U^m) = a_{p^m}(f),$$

cela exprime bien $a_0(f)$ au moyen des $a_n(f)$ pour $n \geqslant 1$.

Pour $p \geqslant 13$, il y a des formules analogues utilisant, non seulement U, mais aussi les T_l.

1.5. *Formes sur* $\Gamma_0(p)$. Le groupe $\Gamma_0(p)$ est le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ formé des matrices $\binom{a\ b}{c\ d}$ telles que $c \equiv 0$ (mod.p). On démontre que toute forme modulaire de poids k sur $\Gamma_0(p)$, à coefficients rationnels, est une forme modulaire p-adique au sens ci-dessus (i.e. peut être approchée par des formes modulaires sur $\mathbf{SL}_2(\mathbf{Z})$). Il y a un résultat analogue pour les formes « de Nebentypus » au sens de Hecke. Dans le même ordre d'idées, signalons qu'il y a identité (pour $p \neq 2$) 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 $\mathbf{SL}_2(\mathbf{Z})$.

2. *Fonctions zêta p-adiques*

Pour simplifier, on suppose $p \neq 2$ dans ce qui suit.

2.1. *L'algèbre d'Iwasawa* Λ. Les éléments de cette algèbre sont les fonctions $f : \mathbf{Z}_p \to \mathbf{Z}_p$ satisfaisant aux conditions équivalentes suivantes :

(i) f est limite uniforme (resp. limite simple) de fonctions de la forme

$$s \longmapsto \sum_{i=1}^{n} a_i u_i^s, \qquad \text{avec } a_i \in \mathbf{Z}_p,\ u_i \in U_1 = 1 + p\mathbf{Z}_p.$$

(ii) Il existe une mesure p-adique μ sur U_1 (au sens de B. Mazur), à valeurs dans $\mathbf{Z}_p$, telle que

$$f(s) = \int_{U_1} u^s \mu(u) \qquad \text{pour tout } s \in \mathbf{Z}_p.$$

(iii) Le changement de variables $1 + T = (1 + p)^s$ transforme f en un élément de l'algèbre de séries formelles $\mathbf{Z}_p[[T]]$.

(iv) f a un développement de Taylor de la forme

$$f(s) = \sum_{n=0}^{\infty} b_n p^n s^n / n!, \qquad \text{avec } b_n \in \mathbf{Z}_p$$

et

$$\sum_{i=1}^{n} c_{in} b_i \equiv 0 \pmod{n!\mathbf{Z}_p} \qquad \text{pour tout } n \geqslant 1,$$

où les c_{in} sont des entiers définis par l'identité

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

(v) f a un développement binomial de la forme

$$f(s) = \sum_{n=0}^{\infty} d_n p^n \binom{s}{n}, \text{ avec } d_n \in \mathbf{Z}_p,\ \binom{s}{n} = \frac{s(s-1)\ldots(s-n+1)}{n!},$$

et

$$\sum_{i=1}^{n} c_{in} d_i \equiv 0 \pmod{n!\mathbf{Z}_p} \qquad \text{pour tout } n \geqslant 1,$$

les c_{in} étant les mêmes que ci-dessus.

2.2. *Familles analytiques de formes modulaires p-adiques.* Soit f_s une forme modulaire p-adique dépendant d'un paramètre $s \in \mathbf{Z}_p$ et de poids $(rs,u) \in \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, où r et u sont indépendants de s. On écrit f_s sous la forme

$$f_s = a_0(f_s) + \sum_{n=1}^{\infty} a_n(f_s)\, q^n,$$

et l'on suppose que, pour tout $n \geqslant 1$, la fonction $s \mapsto a_n(f_s)$ appartient à l'algèbre d'Iwasawa Λ, cf. n° 2.1. Alors :

a) si $u \neq 0$, la fonction $s \mapsto a_0(f_s)$ appartient à Λ ;

b) si $u = 0$ et $r \neq 0$, la fonction $s \mapsto a_0(f_s)$ est de la forme $h(T)/((1+T)^r - 1)$, avec $h \in \Lambda = \mathbf{Z}_p[[T]]$.

2.3. *Définition de la fonction zêta p-adique d'un corps de nombres.* Soit K un corps de nombres algébriques totalement réel de degré r, et soit ζ_K sa fonction zêta (au sens usuel). Si k est un entier pair $\geqslant 2$, $\zeta_K(1-k)$ est un nombre *rationnel*. De plus, si $k \geqslant 4$ ou $r \geqslant 2$, il existe une forme modulaire g_k de poids rk sur $\mathbf{SL}_2(\mathbf{Z})$ dont les coefficients sont donnés par les formules suivantes :

$$a_0(g_k) = 2^{-r}\,\zeta_K(1-k)$$

et

$$a_n(g_k) = \sum_{x,\,\mathfrak{a}} (N\mathfrak{a})^{k-1} \qquad \text{pour } n \geqslant 1,$$

la sommation étant étendue aux couples formés d'un idéal entier $\mathfrak{a}$ de K et d'un élément x totalement positif de K tel que $\mathrm{Tr}(x) = n$ et $x \in \mathfrak{d}^{-1}\mathfrak{a}$ (où $\mathfrak{d}$ est la différente de K).

Ce résultat, dû à Hecke, Kloosterman et Siegel, permet d'effectuer un « passage à la limite » p-adique sur k. De façon plus précise, soit k un élément pair de $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ tel que $rk \neq 0$ et choisissons une suite d'entiers pairs $k_i \geqslant 4$ tels que

$$|k_i| \to +\infty \qquad \text{et} \qquad k_i \to k \text{ dans } X.$$

Les $a_n(g_{k_i})$, $n \geqslant 1$, convergent uniformément lorsque $i \to \infty$. On en conclut que les g_{k_i} ont une limite g_k^* qui est une forme modulaire p-adique de poids rk. Les coefficients $a_n(g_k^*)$, $n \geqslant 1$, sont donnés par une formule analogue à celle donnant les $a_n(g_k)$ (à cela près que la sommation porte seulement sur les idéaux $\mathfrak{a}$ qui sont premiers à p). Le terme constant $a_0(g_k^*)$ est noté $2^{-r}\,\zeta_K^*(1-k)$. La fonction ζ_K^* ainsi définie est la fonction zêta p-adique de K.

2.4. *Propriétés de* ζ_K^*.

(i) On peut calculer $\zeta_K^*(1-k)$ lorsque k est de la forme (n,u), où n est un entier > 0. Le résultat est particulièrement simple lorsque $n \equiv u$ (mod.$(p-1)$) : on a

$$\zeta_K^*(1-k) = \zeta_K(1-n) \prod_{\mathfrak{p} \mid p} (1 - N\mathfrak{p}^{n-1}).$$

(ii) Pour $u \in \mathbf{Z}/(p-1)\mathbf{Z}$ fixé, avec $ru \neq 0$, la fonction

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

appartient à l'algèbre d'Iwasawa $\Lambda = \mathbf{Z}_p[[T]]$. En particulier c'est une fonction holomorphe de s dans un disque strictement plus grand que le disque unité ; ses valeurs sont des entiers p-adiques, liés entre eux par des congruences analogues à la « congruence de Kummer ».

(iii) Lorsque $ru = 0$, la fonction $s \mapsto \zeta_K^*(1-s,\ 1-u)$ est de la forme $h(T)/((1+T)^r - 1)$, avec $h \in \Lambda$; elle est méromorphe dans un disque plus grand que le disque unité, et a (au plus) un pôle simple en $s = 1$.

Les démonstrations des résultats résumés ci-dessus se trouvent dans le vol. III de la « Summer School on Modular Functions » (Springer-Verlag, Lecture Notes in Math. n° 350).

Missions

Séminaire à l'Institute for Advanced Study, Princeton (octobre-décembre 1972).

Conférences à l'Ecole d'Eté d'Anvers (juillet 1972), Haverford College (octobre 1972), Columbia University (novembre 1972), Harvard (décembre 1972), Grenoble (février 1973), Bordeaux (avril 1973), Cambridge (avril 1973) et Londres (avril 1973).