Algèbre et géométrie

M. Jean-Pierre Serre, professeur

Le cours a comporté deux parties, l'une sur les fonctions L, l'autre sur les formes modulaires.

1. *Fonction zêta et fonctions L*

Il s'agit de la fonction zêta de Riemann $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ et des fonctions L de Dirichlet $L(s,\chi) = \sum_{n=1}^{\infty} \chi\,(n)n^{-s}$, relatives au corps $\mathbf{Q}$ des nombres rationnels ; le cas d'un corps de nombres quelconque fera l'objet du cours de 1972-1973.

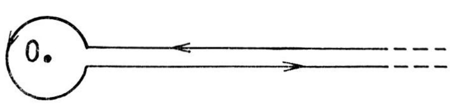
On a commencé par établir les principales propriétés élémentaires de ces fonctions : région de convergence, prolongement analytique, comportement sur la droite $R(s) = 1$, équation fonctionnelle. La méthode suivie a été celle introduite par A. Hurwitz en 1882 (*Math. Werke*, I, p. 72-88) ; elle est basée sur la fonction

$$\zeta(s,a) = \sum_{n=0}^{\infty} (n + a)^{-s}, \qquad 0 < a \leqslant 1,$$

et son expression intégrale

$$\zeta(s,a) = \frac{e^{-i\pi s}\,\Gamma(1 - s)}{2i\pi} \int_C \frac{e^{-az}}{1 - e^{-z}}\, z^s\, \frac{dz}{z},$$

où C désigne le contour d'intégration :



.

D'autres propriétés des fonctions ζ et L ont été résumées sans démonstration, notamment celles liées aux *majorations* du terme d'erreur $\varepsilon(x)$ dans le théorème des nombres premiers

$$\pi(x) = \int_2^x dt/\log t + \varepsilon(x),$$

ainsi que dans le théorème de la progression arithmétique.

On a surtout insisté sur les *valeurs des fonctions ζ et L aux entiers négatifs.* Ces valeurs s'expriment de façon simple en fonction des polynômes de Bernoulli $B_k(X)$ et des nombres de Bernoulli b_k : on a

$$\zeta(1 - k,a) = - B_k(a)/k \text{ et en particulier } \zeta(1 - k) = - b_k/k$$

pour tout entier $k \geqslant 2$. Ce résultat, connu depuis près d'un siècle, a été récemment le point de départ de la théorie des *fonctions L p-adiques* de KUBOTA-LEOPOLDT. Il y a intérêt à présenter cette théorie comme l'a fait TATE dans le cas archimédien, i.e. en considérant la fonction de KUBOTA-LEOPOLDT comme une *fonction méromorphe* $\mathscr{L}(\psi)$ *d'un caractère* ψ (et non plus d'une « variable » s). Comme l'a suggéré B. MAZUR, on peut définir $\mathscr{L}(\psi)$ comme une « transformée de Mellin » d'une certaine mesure p-adique :

Soit p un nombre premier, et soit m_0 un entier $\geqslant 1$, premier à p. L'anneau $T = \mathbf{Z}/m_0\mathbf{Z} \times \mathbf{Z}_p$ est limite projective des $\mathbf{Z}/m\mathbf{Z}$, où m est de la forme m_0p^α, avec $\alpha \to \infty$. Si k est un entier $\geqslant 1$, soit φ_k la fonction sur $\mathbf{Z}/m\mathbf{Z}$ définie par

$$\varphi_k(x) = m^{k-1} B_k(x/m),$$

où $x \in \mathbf{Z}/m\mathbf{Z}$ est identifié à un entier positif $< m$, et où $B_k(X)$ désigne le k-ième polynôme de Bernoulli. On constate que, lorsque m varie, les φ_k sont compatibles en un sens évident, et définissent sur T une distribution Φ_k, que l'on peut appeler la *k-ième distribution de Bernoulli.* Cette distribution n'est pas continue pour la topologie p-adique (ce n'est pas une « mesure p-adique » : elle ne permet pas d'intégrer les fonctions continues, mais seulement les fonctions localement constantes). Toutefois, si c est un entier premier à m_0p, la distribution

$$\Phi_{k,c}(x) = \Phi_k(x) - c^k\Phi_k(c^{-1}x)$$

est une mesure p-adique sur T. Soit alors $\Gamma = (\mathbf{Z}/m_0\mathbf{Z})^* \times \mathbf{Z}_p^*$ le groupe des éléments inversibles de T. Si ψ est un homomorphisme continu $\neq 1$ de Γ dans les unités d'une extension finie de $\mathbf{Q}_p$, on pose

$$\mathscr{L}(\psi) = \frac{1}{k(\psi(c) - 1)} \int_\Gamma \psi(x)\ \chi^{-k}(x)\ \Phi_{k,c}(x), \qquad k \geqslant 1,$$

où χ désigne l'homomorphisme naturel de Γ sur $\mathbf{Z}_p^*$. On montre que $\mathscr{L}(\psi)$ ne dépend, ni du choix de c (pourvu que $\psi(c) \neq 1$), ni du choix de k. La fonction $\psi \mapsto \mathscr{L}(\psi)$ est la fonction de KUBOTA-LEOPOLDT. Si ψ est d'ordre fini, on a

$$\mathscr{L}(\psi\chi^n) = L(1 - n,\psi) \qquad \text{pour tout entier } n \geqslant 1.$$

Il serait très intéressant de généraliser les « distributions de Bernoulli » Φ_k aux corps de nombres totalement réels quelconques. On dispose de quelques résultats partiels encourageants, cf. notamment 2.3 ci-dessous.

2. *Propriétés p-adiques des formes modulaires sur* $\mathbf{SL}_2(\mathbf{Z})$

Cette seconde partie du cours a été présentée sous forme de séminaire. Elle a consisté à donner un certain nombre d'applications d'un résultat récent de SWINNERTON-DYER :

Notons E_k la série d'Eisenstein normalisée de poids k :

$$E_k = 1 - \frac{2k}{b_k} \sum_{m,n=1}^{\infty} m^{k-1}q^{mn} \qquad (k \text{ pair} \geqslant 4).$$

Si p est un nombre premier $\geqslant 5$, on a

$$\mathrm{E}_{p-1} \equiv 1 \ (\mathrm{mod}.p).$$

De plus, cette relation *engendre* (en un sens facile à préciser) l'idéal des relations entre les réductions (mod.p) des formes modulaires sur $\mathbf{SL}_2(\mathbf{Z})$.

Les applications de ce résultat sont les suivantes :

2.1. *Formes modulaires p-adiques*

On appelle ainsi toute série $f = \sum_{n=0}^{\infty} a_n q^n$, à coefficients a_n entiers p-adiques, telle que, pour tout $N \geqslant 1$, il existe une forme modulaire f_N à coefficients p-entiers, de poids k_N dépendant de N, telle que

$$f \equiv f_N \ (\mathrm{mod}.p^N).$$

S'il en est ainsi, et si $f \neq 0$, on montre que les k_N ont une limite dans le groupe

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

groupe que l'on peut identifier à celui des homomorphismes continus de $\mathbf{Z}_p^*$ dans $\mathbf{Z}_p^*$. Cette limite est le *poids* de f. C'est un élément pair de X. Inversement, pour tout $k \in 2X$, on peut définir une *série d'Eisenstein* G_k de poids k, qui dépend de façon méromorphe de k (avec pôle pour $k = 0$) ; son terme constant est essentiellement la fonction de KUBOTA-LEOPOLDT pour le caractère k.

Signalons également que toute forme modulaire à coefficients p-entiers sur le groupe de congruence $\Gamma_0(p)$ est une forme p-adique sur $\mathbf{SL}_2(\mathbf{Z})$ au sens ci-dessus. Si f est modulaire p-adique de poids k, la série

$$\theta f = q\ df/dq = \sum_{n=0}^{\infty} na_n q^n$$

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

2.2. *Représentations l-adiques attachées aux formes modulaires*

P. DELIGNE a démontré, il y a quelques années, que toute forme modulaire parabolique à coefficients entiers qui est fonction propre des opérateurs de HECKE correspond à un système de représentations l-adiques

$$\varrho_l : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{Z}_l).$$

L'analogie avec le cas des courbes elliptiques (traité dans le cours 1970-1971) laissait penser que, pour presque tout l, l'image de ϱ_l est « grosse », i.e. contient $\mathbf{SL}_2(\mathbf{Z}_l)$. La méthode de SWINNERTON-DYER permet de montrer qu'il en est bien ainsi : si $\mathrm{Im}(\varrho_l)$ était « petite », on en déduirait certaines congruences entre formes modulaires qui, pour presque tout l, contrediraient le théorème de structure donné au début.

Ainsi, pour la forme Δ de poids 12, on trouve que $\mathrm{Im}(\varrho_l)$ est « grosse » pour $l \neq 2,3,5,7,23,691$. Cela entraîne un théorème de densité du type Dirichlet : si a,b,m,n sont des entiers $\geqslant 1$, avec $(a,m) = 1$, et n non divisible par 2,3,5,7,23,691, il existe une infinité de nombres premiers p tels que

$$p \equiv a \ (\mathrm{mod.}\, m) \qquad \text{et} \qquad \tau(p) \equiv b \ (\mathrm{mod.}\, n),$$

où $\tau(p)$ désigne le coefficient de q^p dans le développement de Δ.

D'autres exemples peuvent également être traités numériquement. La forme $E_4\Delta$ de poids 16 a un comportement spécialement intéressant pour $l = 59$: il semble (mais ce n'est pas démontré pour l'instant) que la représentation ϱ_{59} correspondante ait une image dans $\mathbf{PGL}_2(\mathbf{F}_{59})$ isomorphe au groupe symétrique $\mathfrak{S}_4$.

2.3. *Valeurs des fonctions zêta aux entiers négatifs*

Soient K un corps de nombres totalement réel de degré r, ζ_K la fonction zêta de K, et m un entier pair $\geqslant 2$. On sait que $\zeta_K(1 - m)$ est un nombre *rationnel* $\neq 0$. La méthode de KLINGEN et SIEGEL consiste à étudier ce nombre au moyen d'une certaine série

$$f_m = \sum_{n=0}^{\infty} a_m(n)q^n,$$

jouissant des propriétés suivantes :

a) f_m est une forme modulaire sur $\mathbf{SL}_2(\mathbf{Z})$ de poids $k = rm$ (mis à part le cas $r = 1$, $m = 2$, exclu dans ce qui suit) ;

b) son terme constant $a_m(0)$ est égal à $2^{-r}\zeta_K(1 - m)$;

c) ses autres coefficients $a_m(n)$, $n \geqslant 1$, sont des *entiers*, donnés par une formule explicite, qui se réduit à $a_m(n) = \sigma_{m-1}(n)$ lorsque $K = \mathbf{Q}$.

On peut exploiter les propriétés d'intégralité et de congruence des

$$a_m(n),\ n \geqslant 1,$$

pour obtenir des propriétés analogues pour $\zeta_K(1 - m)$. C'est ainsi que, si p est premier, et si

$$rm \not\equiv 0 \ (\text{mod.}(p - 1)),$$

on démontre que $\zeta_K(1 - m)$ est *p-entier* ; si en outre

$$m' \equiv m \ (\text{mod.}(p - 1)) \text{ et } m' \geqslant 2,$$

on a

$$\zeta_K(1 - m') \equiv \zeta_K(1 - m) \ (\text{mod.}p).$$

Pour $K = \mathbf{Q}$, on retrouve une congruence de KUMMER sur les nombres de Bernoulli.

Les résultats de 2.2 et 2.3 ont également fait l'objet d'un exposé au Séminaire BOURBAKI de juin 1972.

SÉMINAIRE

Barry MAZUR a fait deux exposés sur la construction de fonctions analytiques p-adiques attachées aux formes modulaires de poids 2 sur le groupe de congruence $\Gamma_0(N)$. Ses résultats, obtenus en collaboration avec SWINNERTON-DYER, montrent une remarquable analogie avec ceux de KUBOTA-LEOPOLDT et IWASAWA ; ils sont en rapport étroit avec ceux publiés récemment par MANIN.

Nicholas KATZ a fait un exposé sur l'interprétation en termes de courbes elliptiques de certains résultats sur les formes modulaires utilisés dans le cours. Il a notamment expliqué, au moyen de la connexion de Gauss-Manin, le fait que l'algèbre des formes modulaires modulo p soit stable par l'opérateur de dérivation θ.

PUBLICATIONS

J.-P. SERRE, *Représentations linéaires des groupes finis*, 2ᵉ édition refondue (Paris, Hermann, 1971).

— *Sur les groupes de congruence des variétés abéliennes II* (*Izv. Akad. Nauk CCCP,* 35, 1971, p. 731-737).

— *Cohomologie des groupes discrets* (*Ann. of Math. Studies*, n° 70, p. 77-169, Princeton Univ. Press, 1971).

— *Conducteurs d'Artin des caractères réels* (*Invent. math.*, 14, 1971, p. 173-183).

— *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (*Invent. math.*, 15, 1972, p. 259-331).

MISSIONS

Conférences aux Universités de Londres (novembre 1971), Bordeaux (février 1972) et Marseille (mars 1972).