Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le but initial du cours était d'exposer certaines conjectures sur les relations entre formes modulaires et représentations galoisiennes (mod p), cf. *Duke Math. J.* 54 (1987), p. 179-230. En fait, le côté modulaire a pris le dessus, et l'aspect galoisien n'a joué qu'un rôle épisodique.

1. *Formes modulaires de niveau N*

Soit N un entier ≥ 3. On note $X(N)$ la courbe modulaire de niveau N sur Spec $\mathbf{Z}[1/N]$. Les points de cette courbe correspondent aux courbes elliptiques E (généralisées, au sens de DELIGNE-RAPOPORT, LN 349, p. 143-316), munies d'une rigidification de niveau N, i.e. d'un isomorphisme de $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ sur le noyau de la multiplication par N dans E. La courbe $X(N)$ est projective et lisse sur $\mathbf{Z}[1/N]$; elle est absolument irréductible sur $\mathbf{Z}[1/N, \mu_N]$.

Le dual de l'algèbre de Lie de E définit un faisceau inversible ω sur $X(N)$; si ω^k désigne la puissance tensorielle k-ème de ω, on pose

$$M_k(N) = H^0(X(N), \omega^k),$$

et, plus généralement :

$$M_k(N,A) = H^0(X(N), A \otimes \omega^k),$$

pour tout $\mathbf{Z}[1/N]$-module A. Un élément de $M_k(N,A)$ est une « forme modulaire de poids k et de niveau N à coefficients dans A », au sens de N. KATZ, LN 350, p. 69-190.

Si $k \geq 2$, on a $M_k(N,A) = A \otimes M_k(N)$; en particulier, si p est un nombre premier ne divisant pas N, toute forme modulaire (mod p) « se relève » en une forme de même poids et de même niveau en caractéristique 0. Ce résultat ne subsiste pas pour $k = 1$: en effet, J.-F. MESTRE a construit des exemples

de formes modulaires (mod 2) de poids 1 et de niveau $N = 1429, 1613, 1693$, etc, qui conduisent à des représentations galoisiennes à image $\mathbf{SL}_2(\mathbf{F}_8)$, et ne se relèvent donc pas en caractéristique 0, même si l'on accepte d'agrandir le niveau N.

Le groupe $G_N = \mathbf{GL}_2(\mathbf{Z}/N\mathbf{Z})$ opère sur $X(N)$ et sur les $M_k(N,A)$. Si p est un nombre premier $\neq 2,3$ qui ne divise pas N, on peut montrer que le $\mathbf{Z}_p[G_N]$-module $M_k(N,\mathbf{Z}_p)$ est *projectif*, pour $k \geqslant 2$. Il y a un énoncé analogue pour $p = 2$ et 3, à condition d'éliminer les facteurs qui correspondent à des représentations galoisiennes (mod p) de type diédral associées aux corps quadratiques de discriminant -4 et -3 respectivement. (De tels facteurs exceptionnels existent effectivement, par exemple pour $N = 13$, $k = 2$; à cause d'eux, les conjectures de *Duke Math. J.*, *loc. cit.*, doivent être légèrement modifiées.)

2. *Formes modulaires en caractéristique p*

A partir de maintenant, p désigne un nombre premier fixé, ne divisant pas N ; on choisit une clôture algébrique $\overline{\mathbf{F}}_p$ de $\mathbf{F}_p$. On note $\overline{X}(N)$ la réduction de $X(N)$ modulo p, et l'on pose :

$\overline{\omega}^k = \overline{\mathbf{F}}_p \otimes \omega^k$,

$\overline{M}_k(N) = M_k(N,\overline{\mathbf{F}}_p) = H^0(\overline{X}(N), \overline{\omega}^k)$.

Dans $\overline{M}_{p-1}(N)$ on dispose d'un élément remarquable, *l'invariant de Hasse* A, dont tous les développements aux pointes sont égaux à 1 ; il ne dépend pas de N (en un sens évident). La multiplication par A définit une injection du faisceau $\overline{\omega}^{k-(p-1)}$ dans le faisceau $\overline{\omega}^k$; le conoyau ω_{ss}^k de cette injection est concentré sur le lieu supersingulier $X(N)_{ss}$ de $\overline{X}(N)$. La suite exacte de faisceaux

$$0 \to \overline{\omega}^{k-(p-1)} \xrightarrow{A} \overline{\omega}^k \to \omega_{ss}^k \to 0$$

donne la suite exacte de cohomologie

$$0 \to \overline{M}_{k-(p-1)}(N) \to \overline{M}_k(N) \to S_k(N) \to H^1(\overline{X}(N), \overline{\omega}^{k-(p-1)}) \to \ldots$$

où $S_k(N) = H^0(X(N)_{ss}, \omega_{ss}^k)$ est l'espace des « formes modulaires (mod p) de poids k sur les courbes supersingulières ».

Lorsque $k \geqslant p+1$, on a $H^1(\overline{X}(N), \overline{\omega}^{k-(p-1)}) = 0$, et la suite exacte ci-dessus se réduit à

$$0 \to \overline{M}_{k-(p-1)}(N) \to \overline{M}_k(N) \to S_k(N) \to 0.$$

Les opérateurs de Hecke T_ℓ, avec $(\ell, pN) = 1$, commutent à la multiplication par A, et opèrent de façon naturelle sur $S_k(N)$. On déduit de là que, si (a_ℓ) est une famille d'éléments de $\overline{\mathbf{F}}_p$, il y a équivalence entre :

(α) Les (a_ℓ) sont les valeurs propres des T_ℓ pour un vecteur propre commun de ceux-ci dans un $\overline{M}_k(N)$, k convenable ;

(β) Même énoncé, avec $\overline{M}_k(N)$ remplacé par $S_k(N)$.

L'avantage des $S_k(N)$ est qu'ils dépendent de façon simple de k. Par exemple :

(1) L'espace $S_k(N)$, muni des opérateurs T_ℓ, *ne dépend que de la classe de* k mod $p^2 - 1$ (N et p étant fixés).

Cela résulte du fait que toute courbe supersingulière E sur $\overline{\mathbf{F}}_p$ a une structure canonique sur $\mathbf{F}_{p^2}$, à savoir celle où son endomorphisme de Frobenius est égal à $-p$; l'espace vectoriel $\omega^{p-1}(E)$ a donc une base canonique.

(2) Il existe $B \in S_{p+1}(N)$ tel que la multiplication par B définisse un *isomorphisme de* $S_k(N)$ *sur* $S_{k+p+1}(N)$, et que

$$T_\ell(Bf) = \ell B\, T_\ell(f) \qquad \text{si } (\ell, pN) = 1 \text{ et } f \in S_k(N).$$

En d'autres termes, l'espace à opérateurs $S_{k+p+1}(N)$ est isomorphe au « tordu » $S_k(N)[1]$ de $S_k(N)$.

Si $p \geqslant 5$, on peut prendre pour B la série d'Eisenstein E_{p+1}, cf. G. ROBERT, *Invent. Math.* 61 (1980), p. 103-158. Si $p = 2$ (resp. $p = 3$), on peut prendre $B = a_3$ (resp. $B = b_4$), avec des notations standard.

Vu (1), il est naturel de définir l'espace gradué

$$S(N) = \bigoplus_k S_k(N),$$

où l'indice k parcourt $\mathbf{Z}/(p^2 - 1)\mathbf{Z}$. Les T_ℓ opèrent sur $S(N)$.

3. *Interprétation des valeurs propres* (mod p) *des opérateurs de Hecke en termes de quaternions*

Soit D un corps de quaternions sur $\mathbf{Q}$ ramifié seulement en $\{p, \infty\}$ (on sait qu'un tel corps est unique, à isomorphisme près). Notons G le groupe multiplicatif de D, vu comme groupe algébrique sur $\mathbf{Q}$: pour toute $\mathbf{Q}$-algèbre commutative L, G(L) est égal à $(L \otimes D)^\times$; en particulier $G(\mathbf{Q}) = D^\times$. Soit A la $\mathbf{Q}$-algèbre des adèles de $\mathbf{Q}$; le groupe $G(\mathbf{Q})$ est un sous-groupe discret de G(A).

Soit F le $\overline{\mathbf{F}}_p$-espace vectoriel formé des fonctions $f : G(A) \to \overline{\mathbf{F}}_p$ qui sont :

continues, i.e. localement constantes ;

invariantes à droite par $G(\mathbf{Q})$, i.e. telles que $f(g\gamma) = f(g)$ pour tout $g \in G(A)$ et tout $\gamma \in G(\mathbf{Q})$.

Le groupe adélique G(A) opère sur F par translations à gauche. On obtient ainsi une représentation de dimension infinie de G(A) avec laquelle on peut jouer au jeu traditionnel des représentations locales, opérateurs de Hecke, etc.

On a tout d'abord :

THÉORÈME 1 - *Les systèmes de valeurs propres des opérateurs de Hecke fournis par l'action de* G(A) *sur* F *sont les mêmes que ceux fournis par les formes modulaires modulo* p *de tout niveau.*

(Cet énoncé répond, au moins en partie, à une question posée dans *Duke Math. J.*, *loc. cit.*, n° 3.4.)

De façon plus précise, notons U_p le groupe des unités du corps de quaternions $\mathbf{Q}_p \otimes D$, et U_p^1 le noyau de la projection canonique $U_p \to \mathbf{F}_p^{\times 2}$. Le groupe U_p^1 est le plus grand sous-groupe de $(\mathbf{Q}_p \otimes D)^\times = G(\mathbf{Q}_p)$ qui soit un pro-p-groupe ; le plongement naturel de $G(\mathbf{Q}_p)$ dans G(A) l'identifie à un sous-groupe fermé de G(A). Notons F^1 le sous-espace de F formé des éléments fixés par U_p^1. Le théorème 1 résulte des deux faits suivants :

(a) Tout système de valeurs propres des opérateurs de Hecke réalisable dans F est aussi réalisable dans F^1.

En effet, comme U_p^1 est un pro-p-groupe, tout sous-espace non nul de F qui est stable par U_p^1 contient un élément non nul fixé par U_p^1.

(b) L'espace F^1 est isomorphe à la limite inductive (pour N variable) des espaces $S(N)$ définis au §2.

Cela résulte de la correspondance, due à Deuring et Eichler, entre courbes supersingulières et quaternions.

(L'isomorphisme (b) n'est canonique qu'une fois choisie une courbe elliptique « origine », munie des rigidifications nécessaires.)

Le th.1 incite à étudier la structure du G(A)-module F. On est tenté d'imiter la théorie classique (sur $\mathbf{C}$, et non sur $\overline{\mathbf{F}}_p$), et de déterminer les *sous-modules simples* de F. Le résultat est surprenant ; il y en a très peu :

THÉORÈME 2 - *Les seuls sous-*G(A)*-modules simples de* F *sont les sous-modules de dimension* 1 *engendrés par les caractères* $G(A) \to \overline{\mathbf{F}}_p^\times$ *triviaux sur* $G(\mathbf{Q})$.

(De tels caractères se factorisent par la norme réduite $G \to G_m$.)

En fait, les sous-modules de F les plus intéressants ne sont pas de longueur finie ; ce sont des produits tensoriels (infinis) de modules locaux de longueurs 1, 2 ou 3 que l'on peut décrire en termes d'*arbres*.

MISSIONS

Exposés

— *Why Modular Forms ?*, Wuppertal, juillet 1987 ;

— *A quaternion approach to modular forms* mod p, Hambourg, septembre 1987 ;

— *Groupes de Galois sur* **Q**, séminaire Bourbaki, novembre 1987 ; Bordeaux, novembre 1987 ; Marseille, février 1988 ;

— *On the Ramanujan function*, Bombay, janvier 1988 ;

— *On Galois representations*, Bombay, janvier 1988 ;

— *Solutions de* $x^4 + y^4 + z^4 = t^4$, *d'après N. Elkies*, Séminaire de Théorie des Nombres, Paris, février 1988 ;

— *L'analogie entre les corps de fonctions et les corps de nombres*, E.N.S., mars 1988 ;

— *L'hypothèse de Riemann : pourquoi ?*, Genève, avril 1988 ;

— *Groupes de Galois des points de torsion des courbes elliptiques : bornes effectives*, Séminaire de Théorie des Nombres, Paris, avril 1988 ;

— *Groupes d'homotopie*, E.N.S., mai 1988 ;

— *Extensions de Frattini et opérateur* Ω, E.N.S., juin 1988.

DISTINCTION

Médaille d'or du C.N.R.S., décembre 1987.