JEAN-PIERRE SERRE

Valeurs propres des opérateurs de Hecke modulo ℓ

Astérisque, tome 24-25 (1975), p. 109-117

<http://www.numdam.org/item?id=AST_1975__24-25__109_0>

Société Mathématique de France
Astérisque 24-25 (1975)

VALEURS PROPRES DES OPÉRATEURS DE HECKE MODULO ℓ

par

Jean-Pierre SERRE

-:-:-:-

Soit ℓ un nombre premier. On se propose de "classer" les systèmes de valeurs propres des opérateurs de Hecke T_p (p premier $\neq \ell$), opérant sur les formes modulaires (mod. ℓ). Pour simplifier, on se borne au cas des formes modulaires "usuelles", i. e. relatives au groupe $SL_2(\mathbf{Z})$.

1. - RAPPELS SUR LES FORMES MODULAIRES (mod. ℓ), cf. [4], [5], [7]

Soit $\widetilde{M}$ l'algèbre des formes modulaires (mod. ℓ) ; c'est une sous-algèbre de l'algèbre $\mathbf{F}_\ell[[q]]$ des séries formelles en q , à coefficients dans $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$.

Si $\ell = 2$ ou 3 , on a $\widetilde{M} = \mathbf{F}_\ell[\widetilde{\Delta}]$, où $\widetilde{\Delta} = \Sigma\, \widetilde{\tau(n)}\, q^n$ est la réduction (mod. ℓ) de $\Delta = q \prod (1-q^n)^{24}$.

Si $\ell \geq 5$, on a $\widetilde{M} = \mathbf{F}_\ell[\widetilde{Q},\widetilde{R}]/(\widetilde{A}(\widetilde{Q},\widetilde{R})-1)$, où A est le polynôme isobare de poids $\ell-1$ qui exprime la série d'Eisenstein $E_{\ell-1}$ au moyen de $E_4 = Q$ et de $E_6 = R$. L'algèbre $\widetilde{M}$ est graduée, de groupe des degrés $\mathbf{Z}(\ell-1)\mathbf{Z}$; si α est un élément de $\mathbf{Z}/(\ell-1)\mathbf{Z}$, la composante $\widetilde{M}^\alpha$ de $\widetilde{M}$ de degré α est réunion des $\widetilde{M}_k$, $k\in\alpha$, où $\widetilde{M}_k$ désigne la réduction (mod. ℓ) des formes de poids k à coefficients ℓ-entiers. On a $\widetilde{M}_k \subset \widetilde{M}_{k+\ell-1}$ et $\widetilde{M}_k = 0$ si k est impair.

Soit $f = \Sigma\, a_n q^n$ un élément de $\widetilde{M}$ (resp. de $\widetilde{M}^\alpha$ si $\ell \geq 5$). On pose

$$f|U = \Sigma\, a_{\ell n} q^n ,$$

$$f|T_p = \Sigma\, a_{pn} q^n + p^{\alpha-1}\, \Sigma\, a_n q^{pn} \qquad (\text{ p premier } \neq \ell).$$

Les séries $f|U$ et $f|T_p$ appartiennent à $\widetilde{M}$, et même à $\widetilde{M}_k$ si $f\in\widetilde{M}_k$. Les opérateurs de Hecke U et T_p commutent entre eux, et respectent la filtration $\widetilde{M}_k \subset \widetilde{M}_{k+\ell-1} \subset \ldots$ de chaque $\widetilde{M}^\alpha$. A la différence du cas classique, ces opérateurs ne sont pas semi-simples ; pour $\ell = 2$, ils sont même nilpotents, cf. §5.

2. - SYSTÈMES DE VALEURS PROPRES ET REPRÉSENTATIONS DE $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$

Soit F une extension finie du corps $\mathbf{F}_\ell$; les opérateurs U et T_p s'étendent par linéarité à l'algèbre $F\otimes\widetilde{M}$ des formes modulaires à coefficients dans F . Soit f un élément non nul d'un $F\otimes\widetilde{M}_k$ qui soit vecteur propre des T_p , i. e. tel que

$$f|T_p = a_p f \quad , \quad \text{avec } a_p \in F ,$$

pour tout p premier $\neq \ell$.

D'après un résultat de Deligne (cf. [1], th. 6.7), un tel système de valeurs propres définit une représentation "modulaire" du groupe de Galois $G = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$:

THÉORÈME 1. - Il existe une représentation semi-simple continue

$$\rho : G \to GL_2(F) ,$$

qui est non ramifiée en dehors de ℓ, et telle que

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = a_p \quad \underline{\text{et}} \quad \det(\rho(\mathrm{Frob}_p)) = p^{k-1}$$

pour tout p premier $\neq \ell$.

De plus, cette représentation est unique, à isomorphisme près.

Remarques

1) Le caractère $\det(\rho)$ est la puissance $(k-1)$-ième du caractère fondamental $\chi_\ell : G \to \mathbf{F}_\ell^*$ (celui qui donne l'action de G sur les racines $(\ell-1)$-ièmes de l'unité). On notera que c'est un caractère impair, i. e. qu'il transforme la conjugaison complexe c en l'élément -1 de $\mathbf{F}_\ell^*$; pour $\ell = 2$, c'est le caractère unité.

2) Si f est une constante, on a $a_p \equiv 1 + p^{-1} \pmod{\ell}$, et la représentation correspondante est $1 \oplus \chi_\ell^{-1}$. Tout autre système de valeurs propres peut être obtenu au moyen d'une forme $f = \Sigma\, a_n q^n$ "normalisée", i. e. telle que $a_1 = 1$.

3) Les dérivées itérées $\theta^i G_k$ des séries d'Eisenstein correspondent aux représentations réductibles $\chi_\ell^i \oplus \chi_\ell^j$, avec $i+j$ impair.

4) Pour tout entier $m \geq 0$, il existe un vecteur propre non nul f_m des T_p correspondant aux valeurs propres $p^m a_p$ (si $f = \Sigma\, a_n q^n$ est normalisée,

on peut prendre pour f_m la série $\theta^m f = \Sigma\, n^m a_n q^n$, cf. [4] , [5]). La représentation ρ_m associée aux $(p^m a_p)$ est $\rho \otimes \chi_\ell^m$, autrement dit elle se déduit de ρ par "torsion" par le caractère χ_ℓ^m .

3. - PROBLÈMES

i) Réciproque du théorème 1

Soit $\rho : G \rightarrow GL_2(F)$ une représentation semi-simple continue non ramifiée en dehors de ℓ . Son déterminant $\det(\rho)$ est nécessairement de la forme $\chi_\ell^{\alpha-1}$, avec $\alpha \in \mathbf{Z}/(\ell-1)\mathbf{Z}$. Supposons que α soit pair, autrement dit que $\det(\rho)$ soit impair. Est-il vrai que ρ soit associée (par le procédé du th. 1) à un système de valeurs propres (a_p) des T_p sur un $\widetilde{M}_k$ convenable (avec $k \in \alpha$) ? C'est vrai pour $\ell = 2$: Tate a en effet démontré (par un argument basé sur une majoration de discriminant) qu'une telle représentation ρ est nécessairement la représentation unité. Il est probable que le cas $\ell = 3$ peut être traité de manière analogue, grâce aux résultats récents de Odlyzko. J'ignore ce qui se passe pour $\ell \geq 5$.

ii) Inertie en ℓ et valeurs propres de U

Supposons $\ell \neq 2$. Soit $a = (a_p)$ un système de valeurs propres des T_p dans $F \otimes \widetilde{M}$, et soit V_a le sous-espace propre correspondant de $F \otimes \widetilde{M}$. Du fait que U commute aux T_p , il applique V_a dans lui-même, et l'on peut parler des valeurs propres de U dans V_a ; on déduit facilement de [5] , th. 6, qu'il n'y a que deux possibilités :

ii$_1$) 0 est la seule valeur propre de U dans V_a (autrement dit U est localement nilpotent sur V_a), ii$_2$) outre 0 , l'endomorphisme U a une valeur propre $\lambda \in F^*$ sur V_a , qui appartient au sous-corps de F engendré par les a_p .

Soit maintenant $\rho : G \to GL_2(F)$ la représentation de G associée aux (a_p) . Choisissons une place de $\bar{\mathbf{Q}}$ prolongeant ℓ, et soit D_ℓ (resp. I_ℓ) le groupe de décomposition (resp. d'inertie) correspondant ; on a $I_\ell \subset D_\ell \subset G$. Les quelques exemples que j'ai pu traiter suggèrent :

<ins>Conjecture.</ins> - Le cas ii$_2$) ci-dessus se produit si et seulement si il existe un F-sous-espace vectoriel V_ℓ de dimension 1 de F^2 qui est stable par $\rho(D_\ell)$, et tel que $\rho(I_\ell)$ <ins>opère trivialement sur le quotient</ins> F^2/V_ℓ . De plus, s'il en est ainsi, la valeur propre non nulle λ de U sur V_a est égale à la valeur propre de $\rho(\mathrm{Frob}_\ell)$ opérant sur F^2/V_ℓ .

4. - <ins>FINITUDE DES SYSTÈMES DE VALEURS PROPRES DES</ins> T_p

On s'intéresse aux systèmes de valeurs propres (a_p) appartenant à une clôture algébrique $\bar{\mathbf{F}}_\ell$ de $\mathbf{F}_\ell$. Ces valeurs propres appartiennent en fait à des extensions de degré borné de $\mathbf{F}_\ell$: en effet, les T_p laissent stables les $\tilde{M}_k$, et les quotients successifs $\tilde{M}_{k+\ell-1}/\tilde{M}_k$ ont une dimension bornée par une constante $d(\ell) \leq (\ell+13)/12$. Les représentations ρ correspondantes prennent donc leurs valeurs dans des groupes $GL_2(F)$ provenant de sous-extensions F de $\bar{\mathbf{F}}_\ell$ de degré $\leq d(\ell)$ sur $\mathbf{F}_\ell$; les extensions galoisiennes de $\mathbf{Q}$ correspondant aux noyaux de ces représentations sont donc de <ins>degré borné</ins>, et <ins>non ramifiées en dehors de</ins> ℓ ; d'après un théorème classique d'Hermite, elles sont en nombre fini. D'où :

THÉORÈME 2. - <u>Les systèmes de valeurs propres</u> (a_p) <u>des</u> T_p <u>dans</u> $\bar{\mathbf{F}}_\ell \otimes \widetilde{M}$ <u>sont en nombre fini.</u>

En d'autres termes, il existe un poids $k(\ell)$ tel que tout système de valeurs propres des T_p soit réalisable par une forme de poids $\leq k(\ell)$. Ce résultat qualitatif peut être précisé :

THÉORÈME 3. - <u>Tout système de valeurs propres des</u> T_p <u>se déduit par torsion</u> (au sens du §2, Rem. 4)) <u>d'un système provenant d'une forme de poids</u> $\leq \ell+1$.

Ce théorème a d'abord été établi par Atkin pour $\ell \geq 5$, et avec une majoration moins bonne que $\ell+1$. J'ai traité ensuite les cas $\ell = 2$ et $\ell = 3$ au moyen de la formule de Selberg (cf. [2], [3], [6]) ; cette méthode a été reprise par Tate qui a montré que, pour $\ell \geq 5$, elle fournit la borne $\ell+1$, qui est "la meilleure possible".

<u>Remarques</u>

1) La formule de Selberg donne la trace $\mathrm{Tr}_k(T_p)$ de T_p agissant sur les formes paraboliques de poids k . Elle est très commode pour prouver des congruences entre les $\mathrm{Tr}_k(T_p)$ pour diverses valeurs de k .

2) Une autre méthode, due à Kuga (resp. Deligne), pour prouver des congruences entre les $\mathrm{Tr}_k(T_p)$ consiste à utiliser l'isomorphisme d'Eichler-Shimura (resp. la cohomologie ℓ -adique) et le fait que les puissances symétriques $(k-2)$-ièmes de la représentation identique de $GL_2(\mathbf{F}_\ell)$ se ramènent à celles relatives à $k \leq \ell+1$. Il est probable que cette méthode conduit aussi à une démonstration du théorème 3.

5. - EXEMPLES

$\ell = 2$ / Il y a un seul système de valeurs propres, à savoir $a_p = 0$ pour tout p, qui correspond à la représentation unité de G dans le groupe $GL_2(\mathbf{F}_2)$. Cela revient à dire que les T_p sont nilpotents (mod. 2), ou encore que, pour tout $i \geq 0$, $\Delta^i | T_p$ est combinaison linéaire (mod. 2) des Δ^j avec $j < i$. Ce dernier résultat peut d'ailleurs être précisé : pour tout p premier $\neq 2$, $\Delta^i | T_p$ est congru (mod. 8) à un polynôme en Δ de la forme

$$(p+1)\, \Delta^i + a_1 \Delta^{i-1} + \ldots + a_i \quad , \quad \text{avec } a_1, \ldots, a_i \in \mathbf{Z} \; .$$

$\ell = 3, 5, 7$ / Les seuls systèmes de valeurs propres sont les

$$a_p \equiv p^m + p^n \pmod{\ell} \; , \quad m, n \in \mathbf{Z}/(\ell-1)\mathbf{Z} \; , \quad m+n \text{ impair.}$$

Ils correspondent aux représentations réductibles $\chi_\ell^m \oplus \chi_\ell^n$ de déterminant impair. Leur nombre est $(\ell-1)^2/4$.

$\ell = 11, 13, 17, 19$ / A part les systèmes $a_p \equiv p^m + p^n \pmod{\ell}$ comme ci-dessus, on trouve des systèmes correspondant à des représentations irréductibles ρ, à valeurs dans $GL_2(\mathbf{F}_\ell)$. A torsion près, ce sont les suivants :

$\ell = 11, 13$ - Le système $a_p = \tilde{\tau}(p)$ associé à la forme parabolique Δ de poids 12. La représentation $\rho : G \to GL_2(\mathbf{F}_\ell)$ correspondante est surjective.

$\ell = 17$ - Il y a 3 systèmes a_p, ceux associés aux formes paraboliques de poids 12, 16, 18. Les représentations $\rho : G \to GL_2(\mathbf{F}_\ell)$ correspondantes sont surjectives.

$\ell = 19$ - Il y a 4 systèmes a_p, associés aux formes paraboliques de poids 12, 16, 18, 20. Les représentations ρ correspondantes sont surjectives, sauf celle relative au poids 16 dont l'image est le sous-groupe de $GL_2(\mathbf{F}_{19})$ formé des éléments dont le déterminant est un cube dans $\mathbf{F}^*_{19}$.

<u>$\ell = 23$</u>/ A part les systèmes $a_p \equiv p^m + p^n$ (mod. ℓ), on trouve (à torsion près) :

5 systèmes à valeurs dans $\mathbf{F}_\ell$, associés aux formes paraboliques de poids 12, 16, 18, 20, 22 ; les représentations correspondantes ont pour image $GL_2(\mathbf{F}_\ell)$, à l'exception de la première dont l'image est isomorphe au groupe symétrique $\mathfrak{S}_3$, cf. [7], p. 33-34 ;

2 systèmes conjugués à valeurs dans $\mathbf{F}_{\ell^2}$, associés aux deux formes paraboliques de poids 24 conjuguées sur $\mathbf{Q}(\sqrt{144169})$ (noter que 144169 n'est pas un carré mod. 23) ; les représentations correspondantes ont pour image le sous-groupe de $GL_2(\mathbf{F}_{\ell^2})$ formé des éléments dont le déterminant appartient à $\mathbf{F}^*_\ell$.

-:-:-:-

BIBLIOGRAPHIE

[1] P. DELIGNE et J.-P. SERRE. - <u>Formes modulaires de poids</u> 1. (Ann. Sci. E.N.S., 7 (4), 1974, p. 507-530).

[2] M. EICHLER. - <u>The basis problem for modular forms and the traces of the Hecke operators</u> (Lecture Notes in Math., n° 320, Springer, 1973, p. 75-151).

[3] A. SELBERG. - <u>Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series</u> (J. Indian math. soc., 20, 1956, p. 47-87).

[4] J.-P. SERRE. - <u>Congruences et formes modulaires</u> (d'après H.P.F. Swinnerton-Dyer) (Sém. Bourbaki, 1971/72, exposé 416, Lecture Notes in Math., n° 317, Springer, 1973, p. 319-338).

[5] J.-P. SERRE. - Formes modulaires et fonctions zêta p-adiques (Lecture Notes in Math., n° 350, Springer, 1973, p. 191-268).

[6] G. SHIMURA. - On the trace formula for Hecke operators (Acta Math., 132, 1974, p. 245-281).

[7] H. P. F. SWINNERTON-DYER. - On ℓ-adic representations and congruences for coefficients of modular forms (Lecture Notes in Math., n° 350, Springer, 1973, p. 1-55).

-:-:-:-

Jean-Pierre SERRE
Collège de France
11, place Marcelin Berthelot
75231 PARIS CEDEX 05