

Astérisque

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, 1975, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

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 \tilde{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 $\tilde{M} = \mathbf{F}_\ell[[\tilde{\Delta}]]$, où $\tilde{\Delta} = \sum \tilde{\tau}(n)q^n$ est la réduction (mod. ℓ) de $\Delta = q \prod (1-q^n)^{24}$.

Si $\ell \geq 5$, on a $\tilde{M} = \mathbf{F}_\ell[\tilde{Q}, \tilde{R}] / (\tilde{A}(\tilde{Q}, \tilde{R}) - 1)$, 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 \tilde{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 \tilde{M}^α de \tilde{M} de degré α est réunion des \tilde{M}_k , $k \in \alpha$, où \tilde{M}_k désigne la réduction (mod. ℓ) des formes de poids k à coefficients ℓ -entiers. On a $\tilde{M}_k \subset \tilde{M}_{k+\ell-1}$ et $\tilde{M}_k = 0$ si k est impair.

Soit $f = \sum a_n q^n$ un élément de \tilde{M} (resp. de \tilde{M}^α si $\ell \geq 5$). On pose

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

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

Les séries $f|U$ et $f|T_p$ appartiennent à \tilde{M} , et même à \tilde{M}_k si $f \in \tilde{M}_k$. Les opérateurs de Hecke U et T_p commutent entre eux, et respectent la filtration $\tilde{M}_k \subset \tilde{M}_{k+\ell-1} \subset \dots$ de chaque \tilde{M}^α . 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 $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$

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

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

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 $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$:

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

$$\rho : G \rightarrow \text{GL}_2(\mathbb{F}),$$

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

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

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 $\chi_\ell : G \rightarrow \mathbb{F}_\ell^*$ (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 \mathbb{F}_ℓ^* ; 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 $f = \sum a_n q^n$ "normalisée", i. e. telle que $a_1 = 1$.

3) Les dérivées itérées $\theta_{G_k}^i$ 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 $f = \sum a_n q^n$ est normalisée,

on peut prendre pour f_m la série $\theta^m f = \sum n^m a_n q^n$, 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 \tilde{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 $F \otimes \tilde{M}$, et soit V_a le sous-espace propre correspondant de $F \otimes \tilde{M}$. 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 :

ii₁) 0 est la seule valeur propre de U dans V_a (autrement dit U est localement nilpotent sur V_a),

ii₂) 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 $\rho : G \rightarrow GL_2(F)$ 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 :

Conjecture. - Le cas ii₂) 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 $\rho(I_\ell)$ opère trivialement sur le quotient 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 $\rho(\text{Frob}_\ell)$ opérant sur F^2/V_ℓ .

4. - FINITUDE DES SYSTÈMES DE VALEURS PROPRES DES T_p

On s'intéresse aux systèmes de valeurs propres (a_p) appartenant à une clôture algébrique $\bar{\mathbf{F}}_\ell$ de \mathbf{F}_ℓ . Ces valeurs propres appartiennent en fait à des extensions de degré borné de \mathbf{F}_ℓ : 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}_ℓ ; les extensions galoisiennes de \mathbf{Q} correspondant aux noyaux de ces représentations sont donc de degré borné, et non ramifiées en dehors de ℓ ; d'après un théorème classique d'Hermitte, elles sont en nombre fini. D'où :

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

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

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".

Remarques

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

2) Une autre méthode, due à Kuga (resp. Deligne), pour prouver des congruences entre les $\text{Tr}_k(T_p)$ 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 $GL_2(\mathbb{F}_\ell)$ 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

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

$\ell = 3, 5, 7$ / 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 $\rho : G \rightarrow GL_2(\mathbf{F}_\ell)$ correspondante est surjective.

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

$\ell = 23$ / A part les systèmes $a_p \equiv p^m + p^n \pmod{\ell}$, on trouve (à torsion près) :

5 systèmes à valeurs dans \mathbf{F}_ℓ , 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}_{ℓ^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}_ℓ^* .

-:-:-

BIBLIOGRAPHIE

- [1] P. DELIGNE et J.-P. SERRE. - Formes modulaires de poids 1. (Ann. Sci. E. N. S., 7 (4), 1974, p. 507-530).
- [2] M. EICHLER. - The basis problem for modular forms and the traces of the Hecke operators (Lecture Notes in Math., n° 320, Springer, 1973, p. 75-151).
- [3] A. SELBERG. - Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series (J. Indian math. soc., 20, 1956, p. 47-87).
- [4] J.-P. SERRE. - Congruences et formes modulaires (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 congru-
ences 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