Astérisque

PIERRE DELIGNE

Représentations ℓ-adiques

Astérisque, tome 127 (1985), p. 249-255

<http://www.numdam.org/item?id=AST_1985__127__249_0>

Exposé IX

REPRÉSENTATIONS ℓ-ADIQUES

Pierre DELIGNE

L'exposé contient la démonstration du théorème suivant de G. Faltings, et quelques commentaires.

1.- THÉORÈME : *Soient* k *un corps de nombres,* $\bar{k}$ *une clôture algébrique de* k, S *un ensemble fini de places finies de* k, ℓ *un nombre premier et* d *un entier. Il existe un ensemble fini* T *de places finies de* k, *disjoint de* S, *tel qu'une représentation* ℓ*-adique semi-simple de dimension* d, $\rho : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Gl}(d,\mathbb{Q}_\ell)$, *non ramifiée en dehors de* S, *soit uniquement déterminée (à isomorphisme de représentations près) par les traces* $\mathrm{Tr}(\rho(F_v))$, *pour* $v \in T$.

On sait (Hermite) qu'il n'existe qu'un nombre fini d'extensions galoisiennes k' de k, non ramifiées en dehors de S et de degré borné. D'après Čebotarev, il existe donc un ensemble fini T de places de k, disjoint de S, tel que les classes de conjugaison des Frobenius géométriques F_v $(v \in T)$ remplissent tout $\mathrm{Gal}(k'/k)$, pour toute extension galoisienne k' de k, non ramifiée en dehors de S, de degré $\leq \ell^{2d^2}$. Prouvons que T convient.

Soient donc ρ_1, ρ_2 deux représentations ℓ-adiques du type dit, avec $\mathrm{Tr}\ \rho_1(F_v) = \mathrm{Tr}\ \rho_2(F_v)$ pour $v \in T$. Nous voulons montrer que ρ_1 et ρ_2 ont même caractère, donc, étant semi-simples, sont isomorphes. Soit M l'image de l'algèbre $\mathbb{Z}_\ell[\mathrm{Gal}(\bar{k}/k)]$ par

$$\rho_1 \times \rho_2 : \mathbb{Z}_\ell[\mathrm{Gal}(\bar{k}/k)] \longrightarrow M_d(\mathbb{Q}_\ell) \times M_d(\mathbb{Q}_\ell).$$

Il s'agit de vérifier que, sur M, la forme linéaire $\delta(m_1,m_2) := \mathrm{Tr}(m_1) - \mathrm{Tr}(m_2)$ est identiquement nulle. L'algèbre M est un $\mathbb{Z}_\ell$-module de rang $\leq 2d^2$. L'image de $\mathrm{Gal}(\bar{k}/k)$ dans le quotient $(M/\ell M)^*$ a donc moins de ℓ^{2d^2} éléments et, par hypothèse, chaque élément de cette image est un $(\rho_1 \times \rho_2)(F_v)$, $v \in T$. Par Nakayama, les $(\rho_1 \times \rho_2)(F_v)$ $(v \in T)$ engendrent $\mathbb{Z}_\ell$-linéairement M. Sur eux, la forme linéaire δ s'annule par hypothèse, d'où $\delta = 0$ sur M.

COROLLAIRE 1.- *Soient* k,$\bar{k}$,S,ℓ *et* d *comme dans le théorème, et* w *un entier* ≥ 0. *Il n'existe qu'un nombre fini de classes d'isomorphie de représentations* ℓ*-adiques semi-simples de dimension* d, $\rho : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Gl}(d,\mathbb{Q}_\ell)$, *non ramifiées en dehors*

de S *et entières de poids* w, *i.e. telle que pour toute place* $v \notin S$, *notant* q_v *le nombre d'éléments du corps résiduel, on ait*

a) le polynôme caractéristique de $\rho(F_v)$ *est à coefficients entiers ;*

b) ses racines inverses, i.e. les conjugués complexes des valeurs propres de Frobenius, sont de valeur absolue complexe $q_v^{w/2}$.

Soit T un ensemble fini de places, tel que garanti par le théorème. Pour chaque place $v \notin S$, la trace $Tr(F_v)$ est un entier de valeur absolue $\leq d q_v^{w/2}$. Il n'y a donc qu'un nombre fini de possibilités pour le système des $(Tr(F_v))_{v \in T}$, et on applique le théorème.

Une fois acquise la conjecture de Tate sur les homomorphismes de schémas abéliens, on en déduit :

COROLLAIRE 2.- *Soient* k *un corps de nombres et* S *un ensemble fini de places de* k. *Il n'y a qu'un nombre fini de classes d'isogénie de variétés abéliennes de dimension* g *sur* k, *à bonne réduction en dehors de* S.

On fixe un nombre premier ℓ et on applique le corollaire 1 à $S_\ell := S \cup \{\text{places divisant } \ell\}$, d = 2g et w = 1. Pour chaque variété abélienne A du type considéré, la représentation ℓ-adique $V_\ell(A) := T_\ell(A) \otimes \mathbb{Q}_\ell$ est semi-simple (ceci est inclus dans la conjecture de Tate) de dimension d, non ramifiée en dehors de S_ℓ et d'après A. Weil, sa duale est entière de poids 1. On conclut par le corollaire 1 et la conjecture de Tate.

2.- VARIANTES

A. Soient $k, \bar{k}, S, \ell$ et d comme dans le théorème, et f un entier ≥ 1. Il existe T comme dans le théorème, tel que pour toute extension E_λ de $\mathbb{Q}_\ell$, de corps résiduel à ℓ^f éléments, une représentation λ-adique semi-simple de dimension d : $\rho : Gal(\bar{k}/k) \to Gl(d, E_\lambda)$, non ramifiée en dehors de S, soit uniquement déterminée par les $Tr\ \rho(F_v)$ $(v \in T)$.

La preuve est la même, avec ℓ^{2d^2} remplacé par $(\ell^f)^{2d^2}$, $\mathbb{Z}_\ell$ par l'anneau de valuation $\mathcal{O}_\lambda$ de E_λ et la réduction mod ℓ par la réduction mod λ.

A'. Soient $k,\bar{k},S,\ell,d$ et w comme dans le corollaire 1, n un entier ≥ 1, et E_λ une extension finie de $\mathbb{Q}_\ell$. Il n'existe qu'un nombre fini de classes d'isomorphie de représentations λ-adiques semi-simples de dimension d, $\rho : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Gl}(d,E_\lambda)$, non ramifiées en dehors de S, et telle que pour $v \notin S$, les valeurs propres de $\rho(F_v)$ soient des entiers algébriques de degré $\leq n$, dont tous les conjugués complexes soient de valeur absolue $q_v^{w/2}$.

On procède comme pour le corollaire 1 : on utilise qu'il n'y a qu'un nombre fini d'entiers algébriques de degré et de valeurs absolues archimédiennes bornés, et on invoque A au lieu du théorème.

B. Des résultats analogues valent pour k un corps de fonctions d'une variable sur un corps fini, à cela près qu'il ne suffit plus de fixer S, il faut en plus préciser quelle ramification on permet en chaque $v \in S$: on suppose donné des nombres $(a_v)_{v \in S}$, et on ne considère que les représentations dont la restriction au groupe de décomposition en v est triviale sur le groupe de ramification d'indice a_v, en numérotation supérieure.

3.- RENDRE QUANTITATIF

Les versions effectives du théorème de Čebotarev pour $\mathrm{Gal}(k'/k)$ ne font intervenir k et k' que via $[k' : \mathbb{Q}]$ et le discriminant absolu de k'. Pour rendre effectif le théorème, il n'est donc pas nécessaire d'utiliser une version effective du théorème d'Hermite (voir toutefois 8). Le lecteur trouvera dans J-P. Serre [3] des énoncés effectifs. Ces énoncés présentent toutefois le défaut qu'on y suppose que S est exactement l'ensemble des places de k ramifiées dans k'. Les mêmes énoncés devraient valoir pour S quelconque si on y remplace le discriminant absolu $D(k')$ de k' par son produit $D_S(k')$ avec le produit des $Nv^{[k':k]}$ étendu aux places $v \in S$ non ramifiées dans k'. Nous noterons avec une étoile des références à des énoncés ainsi modifiés.

Si on admet ces variantes des énoncés de [3], on a, *sous l'hypothèse de Riemann généralisée*, que toute classe de conjugaison dans $\mathrm{Gal}(k'/k)$ est un Frobenius F_v, avec $v \notin S$ de norme $Nv \leq 70(\log D_S(k'))^2$ ([3] 2.5)*. Par ailleurs pour k'/k comme dans la preuve du théorème et pour P l'ensemble des caractéristiques résiduelles des places $v \in S$, on déduit de [3] 1.3 que

$$\log D_S(k') \leq \ell^{2d^2}(\log D(k) + [k : \mathbb{Q}](\sum_{p \in P} \log p + \log(\ell^{2d^2}))).$$

Sans hypothèse de Riemann, on n'est sûr d'avoir rencontré toutes les classes de conjugaison que pour $v \notin S$ de norme allant jusqu'à $2D_S(k')^c$, pour une constante absolue c ([3] 2.5)*.

Nous nous proposons maintenant de passer en revue des résultats connus analogues au théorème de Faltings. Tout d'abord, une remarque de J-P. Serre.

4.- PROPOSITION : *Soient E_1 et E_2 deux courbes elliptiques sur $\mathbb{Q}$, et supposons qu'elles soient de Weil, i.e. correspondent à des formes modulaires. Supposons que leur conducteur divise N. Alors, si les facteurs locaux L_p des fonctions L de E_1 et E_2 coïncident pour $p \leq \frac{N}{6} \cdot \prod_{p|N} (1 + \frac{1}{p})$, ils coïncident pour tout p.*

Posons $q = \exp(2\pi i z)$. Si $\Sigma a_i(n)n^{-s}$ est la fonction L attachée à E_i, on sait que $f_i := \Sigma a_i(n)q^n$ est une forme modulaire de poids 2 pour $\Gamma_0(N)$. Une telle forme s'interprète comme une section d'un faisceau inversible de degré $d \leq \frac{1}{6}[SL(2,\mathbb{Z}) : \Gamma_0(N)]$ sur le quotient compactifié du demi-plan de Poincaré par $\Gamma_0(N)$. On a $[SL(2,\mathbb{Z}) : \Gamma_0(N)] = \prod_{p|N} (1 + \frac{1}{p})\ N$, et l'hypothèse assure que $f_1 - f_2$ a un zéro d'ordre au moins $(d+1)$ à l'infini, donc s'annule.

5.- VARIANTES

A. Le même argument s'applique aux fonctions L attachées à des formes modulaires de poids k sur $\Gamma_0(N)$, de nebentypus donné. Il suffit de remplacer $\frac{N}{6} \prod_{p|N} (1 + \frac{1}{p})$ par $\frac{kN}{12} \cdot \prod_{p|N} (1 + \frac{1}{p})$. Le cas du poids 1 est traité explicitement dans J-P. Serre [2] 5.3 .

B. Dans la preuve de la proposition, nous n'avons fait usage que de la pointe "évidente". Supposons que E_1 et E_2 aient même conducteur N et que pour chaque $p|N$, les restrictions au groupe de décomposition en p des représentations ℓ-adiques attachées à E_1 et E_2 soient isomorphes. D'après Carayol [1] (que nous avons d'ailleurs déjà utilisé pour identifier les conducteurs géométriques et analytiques), les p-facteurs $(p|N)$ des représentations automorphes correspondant à E_1 et E_2 sont alors isomorphes.

On en déduit que les p-composantes des fonctions de Whittaker des "new form" f_i attachées aux E_i coïncident. La connaissance des facteurs locaux L_p pour $p \leq A$, pour un entier A, permet alors le calcul des (A+1) premiers coefficients du développement de f_i en n'importe quelle pointe. Puisqu'il y a $\sum_{f|N} \inf(f,N/f)$ pointes, on montre comme en 4 que tous les facteurs L_p coïncident pour E_1 et E_2 dès qu'il coïncident pour

$$p \leq \frac{1}{6} \cdot \prod_{p|N} (1 + \frac{1}{p}) \cdot N \cdot (1/\sum_{f|N} \inf(f,N/f)).$$

Exemple : Supposons N premier. Dans ce cas, E_i admet un modèle sur $\mathbb{Z}_p$ de réduction mod p une cubique nodale. Ici, connaître la représentation du groupe de décomposition revient à connaître le facteur local L_p. Cela revient aussi à savoir si les tangentes au point singulier de la cubique nodales sont définies sur $\mathbb{F}_p$, ou conjuguées sur $\mathbb{F}_{p^2}$.

Ceci détermine le comportement de la nouvelle forme sous l'involution d'Atkin - Lehner w_N, qui échange les deux pointes. De là le gain d'un facteur 2 par rapport au n° 4.

C. Soit S un ensemble fini de nombre premiers et, pour $p \in S$, soit $d_i(p)$ le degré du facteur enlérien L_p pour E_i. Soit N_i le conducteur de E_i et posons

$$N_i(S) = N_i \cdot \prod_{p \in S} p^{d_i(p)}.$$

La fonction $f_i^S = \Sigma' a_i(n) q^n$, où la somme est étendue aux n premiers aux $p \in S$, peut s'écrire, pour des λ_a convenables

$$f_i^S(z) = \Sigma \lambda_a f_i(az),$$

où a parcourt les diviseurs de $\prod_{p \in S} p^{d_i(p)}$. Si $N_i(S)$ divise N, f_i^S est donc une forme modulaire sous $\Gamma_0(N)$. Raisonnant comme en 4. et utilisant que la coïncidence des facteurs L_p pour $p \notin S$ l'implique pour tout p, on obtient le résultat suivant.

Pour E_1 et E_2 de Weil, si $N_i(S)|N$ $(i = 1,2)$ et que les facteurs locaux L_p coincident pour $p \notin S$, $p \leq \frac{N}{6} \cdot \prod_{p|N} (1 + \frac{1}{p})$, ils coïncident pour tout p.

6.- Dans [3], J-P. Serre introduit la méthode suivante pour comparer deux représentations ℓ-adiques. On suppose qu'elles appartiennent l'une et l'autre à un système compatible de représentations ℓ-adiques de dimension d, que les traces des Frobenius sont des entiers, et que les représentations sont pures d'un poids w. Supposons que les polynômes caractéristiques des Frobenius coïncident pour $p \leq A$. Soit ℓ' premier, et considérons les réductions mod ℓ' des représentations. On déduit de Čebotarev que pour $\ell' < B(A)$, ces représentations mod ℓ' ont des semi-simplifiées isomorphes. Les traces des F_p^i sont donc des entiers congrus mod $\prod_{\ell'<B(A)} \ell'$. Pour $2^d \cdot p^{dw/2} < \frac{1}{2} \prod_{\ell'<B(A)} \ell'$, les polynômes caractéristiques de F_p, coïncident donc dans les deux représentations. Si $A' := \left[\frac{1}{2^{d+1}} \cdot \prod_{\ell'<B(A)} \ell'\right]^{2/dw}$ est $> A$, on peut recommencer, avec A remplacé par A',.... Pour que cette méthode marche, il faut disposer d'une forme de Čebotarev suffisamment précise pour pouvoir prendre $B(A)$ grand par rapport à $\log A$. Serre n'a pu y arriver que modulo l'hypothèse de Riemann généralisée (GRH).

7.- Serre me signale que la méthode suivie par Faltings permet d'améliorer certains résultats de [3].

Soient S un ensemble fini de nombres premiers et $N = \prod_{\ell \in S} \ell$. Si deux courbes elliptiques sur $\mathbb{Q}$, E et E', ont bonne réduction en dehors de S et si les traces de Frobenius sont les mêmes pour E et E' pour tout $p \notin S$ vérifiant

$$p \leq c_{37}(\log N)^2 \quad \text{(sous GRH)},$$

resp. $$p \leq N^{c_{38}} \quad \text{(inconditionnellement)},$$

alors ces traces coïncident pour tout p et, d'après la conjecture de Tate prouvée par Faltings, les courbes sont isogènes. Cf [3] 8.3 Th. 21. Si E a bonne réduction en dehors de S et est sans multiplication complexe, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ s'envoie sur $\mathrm{Gl}(T_\ell(E))$ pour tout

$$\ell \geq c_{39} \log N \quad \text{(sous GRH)}, \text{ resp.}$$

$$\ell \geq N^{c_{40}} \quad \text{(inconditionnellement)}.$$

Cf [3] 8.4 Th. 22. Les c_i (i = 37 à 40) sont des constantes absolues, en principe explicitables. Ces résultats seront racontés par Serre dans son cours au Collège de France 1984/85.

8.- Je dis au n° 3 que rendre effectif le théorème de Faltings ne requiert pas une version effective du théorème d'Hermite. Pour obtenir un algorithme utilisable, il peut toutefois être préférable de dresserla liste des extensions galoisiennes k'/k à considérer et, pour chacune d'elles, de calculer explicitement jusqu'où il faut aller pour que les Frobenius F_p remplissent Gal(k'/k) : en pratique, beaucoup moins loin que ce qui est garanti par les Čebotarev effectifs. Cette méthode, suggérée par Serre, a été utilisée par Mestre pour prouver l'isogénie de deux courbes elliptiques sur $\mathbb{Q}$ à bonne réduction en dehors de 5077 (l'une d'équation explicite, l'autre de Weil).

Je remercie J-P. Serre d'une lecture critique d'une première version de ce texte.

B I B L I O G R A P H I E

[1] H. CARAYOL.- *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert.* ($2^{ème}$ partie de sa thèse).

[2] J-P. SERRE.- *Modular forms of weight one and Galois representations. In : algebraic number fields.* Edited by A. Fröhlich. Acad. Press 1977.

[3] J-P. SERRE.- *Quelques applications du théorème de densité de Čebotarev.* Publ. Math. IHES 54 (1981) p. 123-202.

P. DELIGNE
I.H.E.S
35 route de Chartres
Le Bois Marie
91440 BURES SUR YVETTE