

Modularité de représentations galoisiennes : progrès récents.

Introduction.

Soit p un nombre premier. On s'intéresse à $\rho : G_Q \rightarrow GL_d(*)$ continue ($* = E, \mathbf{F}$), \mathbf{F} corps fini de caractéristique p , ou E extension finie de Q_p . On suppose ρ absolument irréductible. Dans le cas E , ρ est conjuguée d'une représentation dans $GL_d(O_E)$ (O_E anneau des entiers de E). Se donner ρ revient à se donner une suite compatible, si π_E est une uniformisante, de représentations dans $GL_d(O_E/\pi_E^n O_E)$. Exemple : caractère cyclotomique $\chi_p : G_Q \rightarrow \mathbf{Z}_p^*$ défini par $\sigma(\epsilon) = \epsilon^{\chi_p(\sigma)}$ pour $\epsilon^{p^*} = 1$. Si $\mathbf{F} = O_E/\pi_E$ est le corps résiduel, la représentation $\bar{\rho}$ à valeurs dans $GL_d(\mathbf{F})$ est appelée la réduction. Sa semi-simplifiée (somme directe des quotients d'une suite de Jordan-Hölder) ne dépend pas du choix de la conjugaison. ρ est un relèvement de $\bar{\rho}$.

Le thème de l'exposé est que certaines de ces représentations proviennent de formes "modulaires". Dans le cas E , ceci signifie essentiellement que l'on peut associer à ρ une fonction L généralisant la fonction ζ de Riemann. Fontaine et Mazur conjecturent que les représentations "géométriques" sont modulaires. Très grossièrement, ρ "géométrique" signifie "pas trop ramifiée". Pour $\ell = p$, c'est au sens de la théorie de Hodge- p -adique (Fontaine). Soit $M = \bar{\mathbf{Q}}^{\ker(\rho)}$. Par définition de ρ géométrique, M n'est ramifié qu'en un ensemble fini de premiers ℓ . On note S l'ensemble fini des premiers ℓ qui sont ramifiés pour ρ (au sens de la théorie de Hodge p -adique si $\ell = p$).

Pour $\ell \neq p$, le facteur eulérien $L_\ell(s)$ défini par , si $\ell \notin S$:

$$L_\ell(s)^{-1} = \det((\text{id} - \ell^{-s} \rho(\text{Frob}_\ell)),$$

et

$$L_\ell(s)^{-1} = \det((\text{id} - \ell^{-s} \rho(\text{Frob}_\ell))|_{V^{I_\ell}}).$$

sinon, I_ℓ étant le sous-groupe d'inertie et V le E -espace vectoriel sous-jacent à ρ . La définition de $L_p(s)$ utilise la théorie de Hodge p -adique.

Les $L_\ell(s)^{-1}$ sont des polynômes en ℓ^{-s} à coefficients dans E , mais en fait il fait partie de la modularité de ρ que les coefficients de ces polynômes

sont dans un corps de nombres que l'on plonge dans \mathbf{C} . Il est demandé que le produit eulérien $L(\rho, s) = \prod_{\ell} L_{\ell}(s)$ converge pour $\text{re}(s)$ suffisamment grand, admet un prolongement méromorphe à \mathbf{C} et une équation fonctionnelle qui généralise l'équation fonctionnelle de la fonction ζ de Riemann. En particulier, c'est utile pour faire de la théorie analytique des nombres avec ρ .

Cas des caractères : $d = 1$.

Soit $\chi : G_{\mathbf{Q}} \rightarrow E^*$ à image un groupe fini C (cyclique). On choisit un plongement $C \subset \mathbf{C}^*$. Soit M le corps fixe par le noyau de χ . On a le théorème de Kronecker-Weber (Hilbert 1896) : $M \subset \mathbf{Q}(\mu_N)$ pour un N , $\mathbf{Q}(\mu_N)$ engendré par les racines N -ièmes de l'unité. On choisit N minimal et on obtient le conducteur (les premiers de S sont ceux qui divisent N). Donc on peut voir χ comme un caractère de $(\mathbf{Z}/N\mathbf{Z})^*$. Avec cette identification, on a pour ℓ premier à N : $\chi(\text{Frob}_{\ell}) = \chi(\ell)$, plus précisément $\chi(\text{Frob}_{\ell}) = \chi(\bar{\ell})$, $\bar{\ell}$ l'image de ℓ dans $(\mathbf{Z}/N\mathbf{Z})^*$. Cette identité a un contenu arithmétique : pour χ d'ordre 2 c'est essentiellement la loi de réciprocité quadratique. Elle permet que la fonction $L(\chi, s)$ ci-dessous se prête au calcul.

On prolonge χ par 0 à $\mathbf{Z}/N\mathbf{Z}$. On a :

$$L(\chi, s) = \prod_{\ell} \frac{1}{(1 - \chi(\ell)\ell^{-s})}$$

Je prends le cas de χ le caractère trivial. L est la fonction ζ de Riemann.

$$\zeta(s) = \prod_{\ell} \frac{1}{(1 - \ell^{-s})},$$

convergent pour $\text{re}(s) > 1$. $\zeta(s)$, complétée par son facteur $L_{\infty}(s) = \pi^{-s/2}\Gamma(s/2)$, est la transformée de Mellin d'une fonction thêta : si $\Lambda(s) = L_{\infty}(s)\zeta(s)$:

$$\Lambda(s) = 1/2 \int_0^{\infty} (\theta(iy) - 1)y^{\frac{s}{2}} \frac{dy}{y},$$

avec :

$$\theta(z) = \sum_{n \in \mathbf{Z}} e^{\pi i n^2 z},$$

convergent sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbf{C}, \text{im}(z) > 0\}$. La formule de Poisson entraîne l'équation fonctionnelle :

$$\theta(-1/z) = \sqrt{\frac{z}{i}}\theta(z),$$

qui permet le prolongement en une fonction méromorphe pour la fonction $\Lambda(s)$ avec l'équation fonctionnelle $\Lambda(s) = \Lambda(1-s)$. La forme modulaire est θ . La théorie s'étend aux caractères des groupe de Galois des corps de nombres (Dirichlet, Hecke, théorie du corps de classes élaborée en gros sur un siècle à cheval sur 1900).

Représentations dans GL_2 à image finie.

Soit $\rho_{\text{proj}} : G_{\mathbf{Q}} \rightarrow \text{PGL}_2(\mathbf{C})$ une représentation à image D_{2n} groupe diédral d'ordre $2n \geq 4$, A_4 , S_4 ou A_5 . D'après Tate, elle se relève en une représentation ρ dans $GL_2(\mathbf{C})$. Le théorème de Brauer sur les caractères des groupes finis entraîne que $L(\rho, s)$ admet un prolongement méromorphe avec équation fonctionnelle et ρ "provient d'une forme modulaire" si $L(\rho, s)$ est holomorphe (conjecture d'Artin). Si ρ est impaire ($\det(\rho(c)) = -1$, c conjugaison complexe), cela veut dire que $L(\rho, s)$ est la transformée de Mellin d'une forme modulaire holomorphe sur \mathcal{H} de poids 1 pour $\Gamma_1(N)$. Si ρ est paire ($\det(\rho(c)) = 1$), $L(\rho, s)$ provient par transformation de Mellin d'une forme non holomorphe, forme de Maass.

Théorème (Langlands-Tunnell 1981) Si l'image de ρ_{proj} n'est pas A_5 , la conjecture d'Artin est vraie.

La preuve utilise que l'image est résoluble, mais est difficile (utilise la formule des traces de Selberg).

On sait très peu de choses dans le cas pair, et donc on va se concentrer sur le cas impair.

$d = 2$. Formes modulaires (holomorphes).

Soit $\Gamma_1(N)$ le groupe des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbf{Z}), c \equiv 0 \pmod{N}, a \equiv d \equiv 1 \pmod{N}$. Une forme modulaire parabolique de poids $k \geq 1$ pour $\Gamma_1(N)$

est une fonction holomorphe sur le demi-plan de Poincaré qui vérifie :

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z)$$

pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. De plus, on a des conditions de croissance au bord de \mathcal{H} . idem pour $\Gamma_0(N)$ où l'on impose que $c \equiv 0 \pmod{N}$. θ ne rentre pas exactement dans ce cadre : c'est une forme de poids $1/2$ pour un autre sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$.

La période 1 et les conditions de croissance au bord font que l'on a un développement de Fourier $f(z) = a_1 q + \sum_{n \geq 2} a_n q^n$, $q = e^{2\pi iz}$. Soit $S_k(\Gamma_1(N))$ le \mathbf{C} -espace vectoriel des formes paraboliques. Il est de dimension finie. Il a une partie nouvelle qui est la plus intéressante, et qui a une base de formes propres pour les opérateurs de Hecke, que l'on peut normaliser par $a_1 = 1$: ce sont les formes primitives. Pour une telle forme, les a_n sont dans un corps de nombres.

C'est explicite. On peut demander à un ordinateur les premiers coefficients des formes primitives de poids k et de niveau N . Pour $k \geq 2$, le théorème de Riemann-Roch donne des formules simples pour la dimension.

Exemple : $S_k(\mathrm{SL}_2(\mathbf{Z})) = (0)$ si $2 \leq k < 12$, $\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$ engendre $S_{12}(\mathrm{SL}_2(\mathbf{Z}))$. $S_2(\Gamma_0(\ell)) = 0$ si $\ell = 2, 3, 5, 7$ et $S_2(\Gamma_0(11))$ est de dimension 1 engendré par : $f_{11} = q \prod_{n \geq 1} (1 - q^n)^2 \prod_{n \geq 1} (1 - q^{11n})^2$.

Si f est une forme primitive, sa fonction $L(f, s)$ est définie par transformée de Mellin. Pour $f \in S_k(\Gamma_0(N))$, $L_\ell(s)^{-1} = 1 - l^{-s} a_\ell + \ell^{k-1-2s}$ pour $\ell \notin S$, S ensemble des nombres premiers qui divisent N . Elle se prolonge en une fonction holomorphe avec équation fonctionnelle.

Le théorème réciproque de Weil dit en gros que les fonctions L avec équation fonctionnelle de type précisé correspondent à ces formes modulaires.

Il est alors naturel d'associer aux formes primitives des représentations galoisiennes.

Deligne a associé à une forme primitive pour chaque p une représentation p -adique dont la fonction L est la transformée de Mellin de f pour $k \geq 2$; Deligne-Serre pour $k = 1$. Les représentations sont impaires. On obtient un système compatible : pour chaque p , on a $\rho_p(f)$ et elles ont toutes la même fonction L .

$d = 2$. Courbes elliptiques modulaires sur \mathbf{Q} .

Soit \mathcal{E} une courbe elliptique sur \mathbf{Q} : cubique projective $y^2 = x^3 - g_2x - g_3$ avec g_2 et g_3 rationnels, où même entiers après changement de repère, le discriminant $g_2^3 - 27g_3^2$ non nul. On a une paramétrisation $\mathcal{E}(\mathbf{C}) = \mathbf{C}/L$, L réseau, donc on a naturellement une loi de groupe sur $\mathcal{E}(\mathbf{C})$ et $\mathcal{E}(\mathbf{C})_{p^n} \simeq \mathbf{Z}/p^n\mathbf{Z} \oplus \mathbf{Z}/p^n\mathbf{Z}$, d'où une représentation $\rho_p(\mathcal{E}) : G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{Z}_p)$.

On peut former la fonction $L(\mathcal{E}, s)$: c'est la fonction L des $\rho_p(\mathcal{E})$. On a en particulier pour $\ell \notin S$ (en particulier ℓ qui ne divisent pas $g_2^3 - 27g_3^2$). $a_\ell = \ell + 1 - \mathrm{card}(\mathcal{E}(\mathbf{F}_\ell))$. On dit que \mathcal{E} est modulaire s'il existe $f \in S_2(\Gamma_1(N))$ tel que $L(\mathcal{E}, s) = L(f, s)$.

Théorème (Wiles, Taylor, Breuil, Conrad, Diamond, 2001) Soit \mathcal{E} une courbe elliptique sur \mathbf{Q} . Alors, \mathcal{E} est modulaire.

La preuve utilise l'isomorphisme : $\mathrm{PGL}_2(\mathbf{F}_3) = S_4$ et le théorème de Langlands Tunnell. Puis un théorème du type : $\bar{\rho}$ modulaire + ρ géométrique, implique ρ modulaire. Ce qui rend abordable un tel théorème est que le noyau de $\mathrm{GL}_d(O_E) \rightarrow \mathrm{GL}_d(\mathbf{F})$ est un pro- p groupe, donc résoluble.

Il en résulte le théorème de Fermat. A une solution de l'équation de Fermat $a^p + b^p = c^p$ est associée une courbe elliptique de Frey $y^2 = x(x - a^p)(x + b^p)$ et la représentation sur les points d'ordre p est irréductible par Mazur si $p > 7$, modulaire par Wiles, la même que celle d'une forme modulaire de poids 2 et de niveau 2 par Ribet. Une telle forme n'existe pas.

$d = 2$ Conjecture de Serre.

Théorème (Khare, W) Soit $\bar{\rho} : G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\mathbf{F})$ qui est absolument irréductible et impaire. Alors $\bar{\rho}$ est la réduction d'une représentation $\rho_p(f)$ associée à une forme primitive de $S_k(\Gamma_1(N))$ pour $k \geq 2$.

En fait, Serre avait défini $k(\bar{\rho})$ ($2 \leq k(\bar{\rho}) \leq p^2 - 1$ si $p \neq 2$; 2,4 si $p = 2$). ne dépendant que de la ramification de $\bar{\rho}$ en p et $N(\bar{\rho})$ ne dépendant que de la ramification en dehors de p tels que l'on puisse choisir $f \in S_{k(\bar{\rho})}(\Gamma_1(N(\bar{\rho})))$. Cette forme précisée de la conjecture est une conséquence de Mazur, Ribet,...

Le théorème implique que pour $k(\bar{\rho}) = 12$, $N = 1$ ($\bar{\rho}$ non ramifié hors de p), $\bar{\rho}$ est, si cette réduction est irréductible, la réduction de $\rho_p(\Delta)$. On sait par Serre et Swinnerton-Dyer que la réduction de $\rho_p(\Delta)$ est irréductible si p n'est pas 2,3,5,7,691. Pour $p \geq 13$, si la restriction $\bar{\rho}|_{D_p}$ de $\bar{\rho}$ au groupe de

décomposition D_p est réductible, être de poids 12 signifie que cette restriction est extension d'un caractère non ramifié par un caractère dont la restriction à l'inertie est la puissance 11-ième de la réduction $\overline{\chi_p}$ de χ_p .

La stratégie de Wiles ne peut s'appliquer telle quelle, car on n'a pas le choix du nombre premier et que le corps résiduel est quelconque. L'image de $\bar{\rho}$ est le plus souvent non résoluble.

Stratégie de la preuve pour $k = 2, N = 1$.

On relève $\bar{\rho}$ en une représentation ρ géométrique de poids 2 et de niveau 1 : relèvement avec contrôle de la ramification. Pour ce faire on utilise, un théorème de Taylor disant que $\bar{\rho}$ est potentiellement modulaire (est modulaire après extension à une extension finie F en particulier totalement réelle). Taylor utilise une variété abélienne définie sur un F dont la représentation modulo p est la restriction de $\bar{\rho}$ à F et dont une autre réduction est diédrale. Le théorème de Taylor implique de plus l'existence d'un système compatible (ρ_ℓ) tel que $\rho_p = \rho$. La représentation 3-adique ρ_3 n'existe pas car le fait que la ramification en 3 est contrôlée (par la théorie de Hodge p -adique) entraîne qu'elle serait réductible (Abrashkin, Fontaine). C'est une lointaine généralisation d'un théorème d'Hermite-Minkowski : si F est un corps de nombre $\neq Q$, son discriminant est $\neq 1$. Le théorème utilise les bornes (inférieures) sur les discriminants (BD).

Cas $k = 12, N = 1$.

Par un raisonnement analogue au précédent, on élimine le cas $p < 11$ et on se ramène au cas $p = 11$.

On relève $\bar{\rho}_{11}$ en une représentation géométrique de poids 2 et semi-stable de niveau 11. Elle provient d'une variété abélienne semi-stable ayant bonne réduction en dehors de 11 par Taylor. Schoof a prouvé qu'une telle variété abélienne est isogène à un produit de $J_0(11)$ (BD). Elle est modulaire. (On a la congruence $\Delta \bmod 11 = f_{11} \bmod 11$).

Principe de Récurrence sur k (ou p) et N . On se ramène à des petits poids en réduisant des systèmes compatibles en des petits premiers et on élimine les premiers divisant N en réduisant en ces premiers. Point de départ de la récurrence : théorème du type (BD) et théorème de Skinner-Wiles ($\bar{\rho}$ réductible et ρ géométrique entraîne ρ modulaire).

On a la conjecture d'Artin pour les représentation icosaédrales impaires (en fait était déjà connue dans beaucoup de cas par Buzzard, Dickinson, Shepherd-Barron, Taylor).

On a aussi dans de nombreux cas la conjecture de Fontaine-Mazur : $d = 2$, ρ à valeurs dans E , géométrique, impaire est modulaire (Kisin).

$d > 2$.

Soit \mathcal{E} une courbe elliptique sur \mathbf{Q} telle que $j(E)$ ne soit pas entier. Clozel, Harris, Shepherd-Barron et Taylor ont prouvé récemment la potentielle automorphie des puissances symétriques $\text{sym}^n(\rho_p(E))$ pour n impair. Cela entraîne pour ces courbes elliptiques la conjecture de Sato-Tate : les $(1 + \ell - \text{card}(\mathcal{E}(\mathbf{F}_\ell)))/2\sqrt{\ell}$, qui d'après Hasse (cas particulier des conjectures de Weil), sont dans $[-1, 1]$ sont équidistribués pour la mesure $(2/\pi)\sqrt{1-t^2}dt$.

Problème pour $d > 4$: la théorie modulaire marche relativement bien dans le cas des d poids (pour la théorie de Hodge p -adiques, pour $d = 2$ les poids sont $0, k - 1$) distincts et les théorèmes (BD) pour les poids $\in [0, 3]$.

Bibliographie (textes d'introduction au sujet).

R. Taylor. Reciprocity laws and density theorems.

<http://www.math.harvard.edu/~rtaylor/>

H. Darmon, F. Diamond, R. Taylor, Fermat's last theorem. Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993), 2–140, Int. Press, Cambridge, MA, 1997.