COLLÈGE
DE
FRANCE
—
CHAIRE D'ALGÈBRE ET GÉOMÉTRIE

Paris, le 6 mai 1986

Cher Fontaine,

Voici, comme promis, la recette qui permet de calculer le poids d'une forme modulaire (mod p) associée à une représentation linéair de $G_Q = Gal(\overline{Q}/Q)$.

Je te rappelle d'abord les notations de ma lettre à Mestre sur ce sujet.

On se donne une représentation continue irréductible

$$\rho : G_Q \to GL(V),$$

où V est un espace vectoriel de dimension 2 sur $\overline{F}_p$. On suppos que $\det\rho : G_Q \to \overline{F}_p^*$ est impair, autrement dit que

$\det \rho(c) = -1$, où $c \in G_Q$ désigne la conjugaison complexe (Si $p = 2$, cette condition est toujours satisfaite. Si $p \neq 2$, elle signifie que $\rho(c)$ peut être représenté par la matrice $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.)

La <u>conjecture</u> dit qu'une telle représentation provient d'une forme modulaire (parabolique, bien sûr) d'un certain niveau N, poids k, et caractère ε. Il s'agit de préciser N, k, ε. Pour N et ε, c'est fait dans ma lettre à Mestre :

N est le <u>conducteur d'Artin de</u> ρ, si j'ose dire ; par définition, il est premier à p ;

ε et k (mod $(p-1)$) sont caractérisés par la formule

$$\det\rho = \varepsilon.\chi^{k-1},$$

où $\chi : G_Q \to F_p^*$ est le caractère cyclotomique.

Bien sûr, cette dernière formule ne décrit k que modulo $(p-1)$. Il s'agit, dans ce qui suit, d'être plus précis, et de décrire un <u>entier</u> $k = k(\rho)$ bien défini. Plus précisément, on désire :

a) que $k = k(\rho)$ soit le <u>plus petit</u> possible (parmi les entiers ≥ 2 de la classe (mod $(p-1)$) considérée) ;

b) que k ne dépende que des <u>propriétés locales</u> de ρ en p,

et même plus précisément que de la restriction de ρ au groupe d'inertie en p de G_Q.

c)On désire aussi donner la valeur propre correspondante de l'opérateur U_p de Hecke, opérant sur la forme f considérée :

$$U_p f = a_p f \quad , \text{ avec } \quad a_p \in \overline{F}_p .$$

Cette valeur propre est également locale, i.e. ne dépend que de la restriction de ρ au groupe de décomposition en p.

Il se trouve que la réponse à c) est simple à énoncer, et je la donne tout de suite :

Si ρ (restreinte au groupe de décomposition en p) admet un quotient de dimension 1 sur lequel l'inertie opère trivialement (i.e. un quotient étale), et si λ est la valeur propre de Frobenius sur ce quotient, on peut choisir f de telle sorte que

$$U_p f = \lambda f.$$

Si aucun tel quotient n'existe, on peut choisir f pour que $U_p f = 0$

(De plus, les seules valeurs propres possibles de U_p sont celles données par cet énoncé. Note le cas particulier intéressant où ρ est non ramifiée en p, auquel cas, il y a (en général) deux valeurs propres possibles λ et μ pour U_p, qui sont les deux valeurs propres de Frob_p agissant sur V. Leur produit est $\varepsilon(p)$.)

J'en viens maintenant à la détermination de $k = k(\rho)$. Je supposerai d'abord que p est $\geqslant 3$ (le cas $p = 2$ est analogue, et j'en parlerai à la fin).

Appelons ρ_p la représentation ρ restreinte à $G_{Q_p} = \mathrm{Gal}(\overline{Q}_p/Q_p)$, et ρ_p^I la restriction de ρ_p au groupe d'inertie. Les recettes que je vais donner vont en fait s'appliquer à toute représentation de degré 2 de G_{Q_p} : à une telle représentation on va attacher un entier $k \geqslant 2$ qui mesurera sa " complication " .

(Note que je m'interdis de prendre $k = 1$; il y a de bonnes raisons à cela, j'y reviendrai peut-être plus loin.)

La 1ère chose à faire est de regarder le semi-simplifié de ρ_p^I, et les caractères modérés qui y interviennent. On voit tout de suite

que ces caractères, s'ils sont $\neq 1$, sont de niveau 1 ou 2. Séparons alors les cas :

1er cas. Niveau 2

On suppose que ces caractères sont de niveau 2, et pas de niveau inférieur. Ils sont alors conjugués entre eux, et la représentation ρ_p est semi-simple. Si l'on note ψ et $\psi' = \psi^p$ les deux caractère fondamentaux de niveau 2 (au sens de mon vieil article d'Inventione les caractères intervenant dans ρ_p^I peuvent s'écrire

$$\psi^a \psi'^b \quad \text{et} \quad \psi^b \psi'^a \quad , \text{ avec} \quad 0 \leqslant a,b \leqslant p-1.$$

De plus, on a $a \neq b$: sinon, en effet, ces caractères seraient des puissances du caractère cyclotomique $\chi = \psi\psi'$, et seraient de niveau $\leqslant 1$. Quitte à permuter les caractères en question, on peut supposer que $a < b$. Ceci étant, la recette pour $k = k(\rho)$ est la suivante :

$$\boxed{(1) \quad k = 1 + pa + b.}$$

Note le cas particulier $a = 0$, qui donne $k = b + 1$; et le cas encor plus particulier $a = 0$, $b = 1$, qui donne $k = 2$ et correspond au cas où ρ se prolonge en un schéma en groupes sur Z_p (i.e. ρ est " fini en p ", suivant la terminologie de ma lettre à Mestre).

(Bien sûr, je me suis convaincu que (1) devait être vrai à partir du cas $a = 0$, où l'on n'a guère le choix si l'on veut un poids $\leqslant p+1$, et en ramenant par torsion le cas général à celui-là. L'effet de la torsion sur le poids est décrit dans le cor.3 de mon exposé Bourbaki de 71/72 " Congruences et formes modulaires ".)

2ème cas. Niveau 1 - ramification modérée

Je suppose que l'action de l'inertie est modérée (ou, ce qui revient au même, qu'elle est semi-simple), et qu'elle se fait par des caractères de niveau 1, autrement dit par des puissances χ^a et χ^b du caractère cyclotomique χ. Ici encore, je peux normaliser a et b par $0 \leqslant a \leqslant b \leqslant p-2$.

La recette pour $k = k(\rho)$ est alors :

$$\boxed{(2) \quad \begin{cases} k = 1 + pa + b & \text{si } (a,b) \neq (0,0) \\ k = p & \text{si } a = 0 \text{ et } b = 0. \end{cases}}$$

Note le cas exceptionnel $a = 0$, $b = 0$ qui correspond à une représentation non ramifiée en p ; dans ce cas, mon invariant k est pris égal à p (et non à 1, comme le suggèrerait la formule générale). Ce choix est dicté par des raisons globales : j'ai fort peu de chances de trouver des formes de poids 1 ! C'est pour cela que j'ai écarté d'avance le poids 1; mais d'un point de vue purement local, il serait peut-être raisonnable de l'accepter (après tout, $k-1$ se comporte comme une espèce de conducteur local en p, et il serait normal qu'une représentation non ramifiée ait un conducteur égal à 0).

3ème cas. Niveau 1 - ramification sauvage

C'est le cas où la représentation ρ_p^I n'est pas semi-simple. On peut l'écrire matriciellement sous la forme

$$\begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$$

où χ^α et χ^β sont des puissances du caractère cyclotomique χ. Note qu'ici on doit distinguer χ^α de χ^β : le caractère χ^α est celui qui intervient " en quotient " et le caractère χ^β " en sous-truc " . D'ailleurs, il est commode de les normaliser de façon différente ; je choisirai α et β tels que

$$0 \leq \alpha \leq p-2 \quad \text{et} \quad 1 \leq \beta \leq p-1 \quad \text{(attention !)}.$$

Je poserai:

$$a = \mathrm{Inf}(\alpha,\beta) \quad \text{et} \quad b = \mathrm{Sup}(\alpha,\beta).$$

La recette pour $k = k(\rho)$ est alors :

$$\boxed{(3) \quad k = 1 + pa + b}$$ (sauf dans le cas exceptionnel ci-après)

Le cas exceptionnel se présente lorsque $\beta = \alpha + 1$; en effet, tu sais bien que, dans ce cas, la ramification sauvage peut être plus ou moins sauvage si j'ose dire. Il y a le cas " peu ramifié " (i.e. ρ finie en p) et le cas " très ramifié " ; le premier corresppnd

en quelque sorte à adjoindre $u^{1/p}$, où u est une unité, et le second à adjoindre $q^{1/p}$, avec $v_p(q) \not\equiv 0 \pmod{p}$. Ce que j'appel le cas exceptionnel, c'est le cas très ramifié. Alors :

(4) Pour $\beta = \alpha + 1$, et ρ_p^I très ramifiée, on a $\boxed{k = \beta(p+1)}$.

Cela revient à dire que, dans le cas exceptionnel, on ajoute $p-1$ à ce que donnerait la règle (3).

Pour justifier (un peu !) ces recettes de cuisine, remarque que l'on trouve $k \leqslant p+1$ si et seulement si $\alpha = 0$, i.e. si et seulement si ρ_p^I a un quotient étale de dimension 1 : c'est un cas que tu connais bien. Le fait que $2 \leqslant k \leqslant p+1$ suffit alors à décider de la valeur de k, puisque celle-ci est connue mod $(p-1)$; il y a une exception : celle où $k \equiv 2 \pmod{(p-1)}$, i.e. $\beta = 1$, où l'on peut a priori avoir $k = 2$ ou $k = p+1$; les recettes ci-dessu disent que l'on doit prendre $k = 2$ dans le cas peu ramifié, et $k = p+1$ dans le cas très ramifié.

Une fois que l'on s'est convaincu de ce qu'il faut faire pour $\alpha = 0$, on passe au cas général par torsion. (Ce n'est pas très agréable à écrire, mais ça se fait au moyen des " cycles de Tate " décrits dans N.Jochnowitz, TAMS 270 (1982), 253-267.)

Voilà mes recettes pour le calcul de $k = k(\rho)$, lorsque $p \neq 2$. Lorsque $p = 2$, c'est plus simple :

$$\begin{cases} k = 2 & \text{si } \rho_2^I \text{ est semi-simple, ou peu ramifiée ;} \\ k = 4 & \text{sinon.} \end{cases}$$

(Je suis obligé de prendre k pair, vu que le caractère ε est pair (et que je le relève de façon évidente, j'ai oublié de le préciser).)

Il serait bien agréable de trouver une définition générale de k évitant d'avoir à regarder autant de cas particuliers. Peux-tu faire ça avec tes chers modules ? Je suppose que oui, tant que k est $\leqslant p+1$, mais il faudrait aussi traiter le cas général.

Bien à toi

J.-P. Serre.

J-P.Serre

PS - En rentrant de Bordeaux, j'ai refait le calcul de la réduction en 2 de la courbe de Frey, et ça marche bien comme je le disais au tableau : il y a réduction multiplicative.

Par contre, je me suis fichu dedans quand je vous ai décrit ce qui se passe pour $x^p + y^p = 7z^p$: le niveau est alors 2.7 et non 7^2 comme je l'avais prétendu. Mea culpa ! Vu cette erreur, notre score reste donc à 1 - 1 .