Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Guy Henniart

Une forme icosaédrale de poids 1

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, nº 2 (1976-1977), exp. nº 24, p. 1-7

<http://www.numdam.org/item?id=SDPP_1976-1977__18_2_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 24, 7 p.

2 mai 1977

UNE FORME ICOSAÉDRALE DE POIDS 1

par Guy HENNIART

1. Introduction.

On conjecture l'existence d'une bijection naturelle entre certaines formes modulaires de poids 1 pour des sous-groupes de congruence de $SL_2(\mathbb{Z})$ et les représentations impaires de dimension 2 de $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (Une représentation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ est dite impaire si $\det \rho$ envoie la conjugaison complexe sur -1). Dans cette bijection, la fonction L_f de Hecke, associée à une forme modulaire f, devrait être égale à la fonction L_ρ d'Artin associée à la représentation ρ correspondant à f. De même, les conducteurs de f et ρ seraient égaux.

THÉORÈME 1 [2]. - Soit f une forme primitive de poids 1, de caractère ε, pour $\Gamma_0(N)$. Alors il existe une représentation impaire $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ de conducteur N et de déterminant ε, telle que $L_f(s) = L_\rho(s)$.

THÉORÈME 2 [6]. - Soit ρ une représentation impaire de dimension 2 de $G_{\mathbb{Q}}$, de conducteur N et de déterminant ε. On suppose que ρ, et toutes ses tordues par les caractères Ψ de $G_{\mathbb{Q}}$, vérifient la conjecture d'Artin (c'est-à-dire que les fonctions $L_{\rho\otimes\Psi}$ sont entières). Alors il existe une forme modulaire f de poids 1, de caractère ε, pour $\Gamma_0(N)$ telle que $L_f = L_\rho$.

Remarquons que dans le théorème 1, la conjecture d'Artin est vraie pour ρ puisque L_f est entière.

Soit $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ une représentation de $G_{\mathbb{Q}}$. L'image de ρ dans $PGL_2(\mathbb{C})$ est un sous-groupe fini de $PGL_2(\mathbb{C})$, et ρ détermine une représentation fidèle $r : \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow PGL_2(\mathbb{C})$ du groupe de Galois sur $\mathbb{Q}$ d'une extension finie de $\mathbb{Q}$. Un sous-groupe fini de $PGL_2(\mathbb{C})$ est soit cyclique, soit diédral, soit encore isomorphe à un des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$. Si l'image de ρ dans $PGL_2(\mathbb{C})$ est cyclique (resp. diédrale, isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$), on dira que ρ est cyclique (resp. diédrale, tétraédrale, octaédrale, icosaédrale).

La conjecture d'Artin est vraie pour les représentations cycliques (ce sont les représentations réductibles) et pour les représentations diédrales (ce sont les représentations irréductibles induites). LANGLANDS [3] a montré récemment que la conjecture d'Artin est vraie pour les représentations tétraédrales et la moitié des représentations octaédrales. Reste donc le cas des représentations icosaédrales, où $\mathrm{Gal}(K/\mathbb{Q})$ est le groupe simple $\mathfrak{A}_5$.

Si f est une forme modulaire comme dans le théorème 1, on dira que f est diédrale, tétraédrale, octaédrale ou icosaédrale, suivant la nature de ρ associée à f .

La thèse de J. BUHLER [1], dont nous dégagerons ici les grandes lignes, a pour couronnement le théorème suivant.

THÉORÈME 3. - Il existe une forme icosaédrale de poids 1 et de conducteur 800.

COROLLAIRE. - Il existe une représentation icosaédrale ρ de $G_{\mathbb{Q}}$, de conducteur 800, vérifiant la conjecture d'Artin.

2. Représentation projective et relèvement.

Nous donnons maintenant les grandes lignes de la démonstration de BUHLER.

On commence par construire une représentation icosaédrale de $G_{\mathbb{Q}}$.

(a) Le premier pas est de chercher une extension K de $\mathbb{Q}$ de groupe de Galois $\mathfrak{A}_5$. On prend K comme le corps des racines d'un polynôme f du 5e degré. L'ordinateur permet d'examiner environ 10^8 polynômes, par une procédure assez systématique pour assurer que tout corps de discriminant $\leq 40\,000$ est obtenu. Mais bien d'autres corps sont obtenus.

Pour voir si le corps K des racines de f a le groupe de Galois $\mathfrak{A}_5$ sur $\mathbb{Q}$, on utilise différents critères successifs :

1° Il faut que le discriminant de f soit un carré ;

2° Il faut que f soit irréductible. On teste l'irréductibilité de f modulo les petits premiers. Les f examinés étaient, soit réductibles (sur $\mathbb{Q}$), soit irréductibles modulo un premier ≤ 20.

3° Si le discriminant de f est un carré, le groupe de Galois de K sur $\mathbb{Q}$ peut être le groupe cyclique C_5, le groupe diédral D_5, ou bien $\mathfrak{A}_5$. Si, modulo un premier p, f se factorise en le produit de deux termes linéaires distincts et d'un terme cubique, alors le groupe de Galois est $\mathfrak{A}_5$. On examine ainsi les p inférieurs à 100. Si aucun ne se factorise de cette façon, on utilise la résolvante de degré 6 de f : c'est un polynôme de degré 6 sur $\mathbb{Q}$ qui a une racine rationnelle si, et seulement si, $\mathrm{Gal}(K/\mathbb{Q})$ n'est pas $\mathfrak{A}_5$.

(b) Le pas suivant est de déterminer l'anneau des entiers de K, par une modification de l'algorithme de Zassenhaus. Cela détermine le comportement des différents premiers, en particulier pour la ramification. Plus précisément, il est facile de classer les 19 cas possibles pour les groupes de ramification en p des premiers p ramifiés. On constate alors que la connaissance du discriminant de K et de la factorisation de p dans K détermine les groupes de ramification en p, sauf pour $p = 5$, $v_5(D_K) = 8$, où, pour distinguer entre la suite de groupes de ramification C_5, C_5, C_5 et la suite D_5, C_5, C_5, on doit utiliser le lemme suivant.

LEMME. - Soit $F = \mathbb{Q}_5(x)$ une extension ramifiée de degré 5 de $\mathbb{Q}_5$. On suppose que x vérifie une équation d'Eisenstein $f(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$, et que $v_5(a_1) = 1$. Alors F est une extension galoisienne de $\mathbb{Q}_5$ si, et seulement si, on a

$$v_5(a_4) \geqslant 2 \ , \ v_5(a_3) \geqslant 2 \ , \ v_5(a_2) \geqslant 2 \ , \ v_5(a_1 + a_5) \geqslant 2 \ .$$

(c) On a donc une représentation projective

$$r : G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{PGL}_2(\mathbb{C}) \ .$$

Il s'agit de la relever en une représentation dans $\mathrm{GL}_2(\mathbb{C})$, et en particulier de trouver un relèvement de conducteur minimal. En fait, SERRE et TATE ont montré [4] que cela se ramène à un problème local. Soient $r_p : G_{\mathbb{Q}_p} \longrightarrow \mathrm{Gal}(K_p/\mathbb{Q}_p) \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ les représentations locales dissociées à r, et $A(r_p)$ le conducteur minimal d'un relèvement de r_p en une représentation de $G_{\mathbb{Q}_p}$ dans $\mathrm{GL}_2(\mathbb{C})$. Alors le conducteur minimal d'un relèvement de r à $\mathrm{GL}_2(\mathbb{C})$ est $A(r) = \prod_p A(r_p)$.

Mais $A(r_p)$ se déduit de la connaissance des groupes de ramification en p. C'est assez facile à voir pour des représentations réductibles ou induites (i. e. si l'image de r_p est cyclique ou diédrale). C'est plus difficile pour des représentations projectives primitives (i. e. dont les relèvements sont irréductibles et non induits ; dans le cas des représentations de degré 2, cela signifie que l'image de r_p est $\mathfrak{A}_4$ ou $\mathfrak{S}_4$). En fait, BUHLER généralise considérablement la situation.

THÉORÈME 4. - *Soit* F *un corps local de caractéristique résiduelle* p, *et* $r : G_F \longrightarrow \mathrm{PGL}_\ell(\mathbb{C})$ *une représentation projective primitive de degré premier de* $G_F = \mathrm{Gal}(\overline{F}/F)$. *Alors* $\ell = p$.

Si K *est le corps fixé par* $\mathrm{Ker}(r)$, e *l'indice de ramification modérée de* K *sur* F, $(G_i)_{i\in\mathbb{N}}$ *les groupes de ramification de* $G = \mathrm{Gal}(K/F)$ *en numérotation inférieure, et* α *le plus grand entier* n *tel que* $G_n \neq 0$, *le conducteur minimal d'un relèvement de* r *à* $\mathrm{GL}_\ell(\mathbb{C})$ *a pour exposant* $p + ((p+1)/e)\alpha$.

(d) Avant de poursuivre l'exposé de la démonstration du théorème 3, donnons des applications du théorème 4.

J. TUNNELL [5] a utilisé ce résultat pour compléter la correspondance de Langlands entre les représentations admissibles supercuspidales de $\mathrm{GL}_2(F)$, F un corps local, et les représentations irréductibles de degré 2 du groupe de Weil de $\overline{F}$ sur F ; il a résolu le dernier cas encore en suspens, à savoir le cas où F est une extension finie de $\mathbb{Q}_2$.

D'autre part, on connaît depuis WEIL [7] les 4 représentations projectives primitives de $G_{\mathbb{Q}_2}$. La méthode de BUHLER permet de calculer les conducteurs minimaux des relèvements. On a le tableau suivant : si $r : G_{\mathbb{Q}_2} \longrightarrow \mathrm{Gal}(K/\mathbb{Q}_2) \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ est primitive, G désigne le groupe $\mathrm{Gal}(K/\mathbb{Q}_2)$, f un polynôme dont les racines engendrent K , et a le conducteur minimal d'un relèvement de r

G	f	a
$\mathfrak{A}_4$	$x^4 + 2x^3 - 2x^2 + 2$	5
$\mathfrak{S}_4$	$x^4 - 2x + 2$	3
$\mathfrak{S}_4$	$x^4 - 4x + 2$	7
$\mathfrak{S}_4$	$x^4 - 4x^2 + 4x - 2$	7

(e) Pour chaque extension K de groupe de Galois $\mathfrak{A}_5$ sur $\underset{\sim}{Q}$, on peut donc calculer le conducteur minimal des relèvements de la représentation projective donnée par K . On trouve 183 corps K , dont le conducteur minimal associé est inférieur à 10 000 .

Désormais nous prendrons K le corps des racines de

$$f(x) = x^5 + 10x^3 - 10x^2 + 35x - 18 \ ;$$

le discriminant de f est

$$D_f = 2^6\ 5^8\ 11^2 = 3\ 025\ 000\ 000 \ ,$$

celui de K est

$$D_K = 2^6\ 5^8 = 25\ 000\ 000 \ .$$

Le conducteur minimal est

$$2^5\ 5^2 = 800 \ .$$

Le choix de ce corps présente plusieurs intérêts :

1° C'est le plus petit conducteur minimal trouvé pour les différents corps K examinés ;

2° Il est nécessaire d'utiliser le lemme cité plus haut pour trouver la ramification en 5. On montre que K_5 est une extension cyclique ramifiée de degré 5 de $\underset{\sim}{Q}_5$.

3° Plus encore, il sera difficile de calculer le coefficient a_5 de la fonction L d'un relèvement de conducteur 800. Pour cela, il faudra distinguer entre les deux représentations projectives non équivalentes de $\mathfrak{A}_5$ (elles se déduisent l'une de l'autre par la conjugaison complexe, et le conducteur minimal ne dépend pas du choix de l'une ou de l'autre).

4° Enfin, K_2 est l'unique extension de $\underset{\sim}{Q}_2$ de groupe de Galois $\mathfrak{A}_4$, c'est-à-dire que r_2 est l'unique représentation locale primitive qui pouvait intervenir dans le problème !

3. Fonction L et forme icosaédrale.

On sait maintenant qu'il existe une représentation icosaédrale ρ de conducteur 800. L'on veut calculer les coefficients a_n de la fonction L_ρ d'Artin de ρ . Cela impose de connaître ρ explicitement.

En fait, ρ se factorise par le groupe de Weil $W(K^{ab}/\mathbb{Q})$, et détermine sur $C_K \subset W(K^{ab}/\mathbb{Q})$, le groupe des classes d'idèles de K , un caractère χ : l'image de C_K est composée de matrices scalaires.

On a le diagramme commutatif suivant :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_K & \longrightarrow & W(K^{ab}/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(K/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow \chi & & \downarrow \rho & & \downarrow r & & \\ 1 & \longrightarrow & \mathbb{C}^\times & \longrightarrow & GL_2(\mathbb{C}) & \longrightarrow & PGL_2(\mathbb{C}) & \longrightarrow & 1 \end{array}$$

De plus, χ détermine ρ , et la connaissance de χ permet de calculer les coefficients a_n de $L_\rho(s) = \sum a_n n^{-s}$, pour n premier, avec la difficulté déjà signalée pour a_5 .

Mais χ est un caractère de C_K groupe des classes d'idèles de K , corps de degré 60 sur $\mathbb{Q}$! Heureusement, l'on montre que χ peut s'écrire $\Psi \circ N_{K/E}$, où E est un sous-corps de K fixé par le groupe diédral D_5 (E est en fait le corps des racines de la résolvante de degré 6 de f ; il est de degré 6 sur $\mathbb{Q}$), et Ψ est un caractère de C_E . L'on est ramené à travailler dans C_E , ce qui est beaucoup plus facile. A l'aide de l'ordinateur, J. BUHLER a ainsi déterminé les valeurs de Ψ (on peut prendre Ψ d'ordre 4) et les coefficients a_p pour p premier, $p \leqslant 360$, d'où les coefficients a_n , $n \leqslant 360$. On détermine également le caractère dét $\rho = \varepsilon$ de ρ .

Posons $f = \sum_{n=1}^{\infty} a_n q^n$, $q = e^{2\pi i z}$. On espère que f sera une forme modulaire de poids 1, de caractère ε , pour $\Gamma_0(800)$. Prenons g une forme modulaire de poids 1, de caractère ε^{-1} pour $\Gamma_0(800)$. On espère donc que $h = fg$ est une forme modulaire de poids 2, de caractère trivial, pour $\Gamma_0(800)$. On procède alors en plusieurs étapes.

(a) On détermine les 360 premiers coefficients de plusieurs formes modulaires g_i de poids 1, caractère ε^{-1} , pour $\Gamma_0(800)$. On utilise pour cela le théorème 2, en partant de représentations réductibles ou induites.

(b) On détermine les 360 premiers coefficients de formes formant une base de l'espace des formes modulaires h de poids 2, caractère trivial, pour $\Gamma_0(800)$ (cet espace a pour dimension 97). Pour cela, on multiplie des formes de poids 1 et caractère ε^{-1} par des formes de poids 1 et caractère ε .

(c) Prenant des formes g_i comme en (a) et h_i comme en (b), on établit des congruences

$$f\, g_i \equiv h_i \pmod{q^{360}} .$$

(d) On considère $f' = h_1/g_1$. C'est une forme modulaire de poids 1, de caractère ε , pour $\Gamma_0(800)$ à ceci près qu'on ne sait pas si elle est holomorphe. En fait, en considérant plusieurs expressions $f' = h_i/g_i$, on peut montrer que f' est holomorphe. De plus, on connaît assez de coefficients de f' pour montrer que f' est vecteur propre de l'opérateur de Hecke T_3 , avec la valeur propre $\beta = e^{6\pi i/20}$.

(e) On montre qu'il n'y a pas de représentation tétraédrale ou octaédrale de conducteur divisant 800. Par le théorème 1, il n'y a pas de formes tétraédrales ou octaédrales pour $\Gamma_0(800)$. De plus, l'on connaît, par le théorème 2, les formes diédrales et les formes non paraboliques (correspondant aux représentations réductibles) de caractère ε , pour $\Gamma_0(800)$. Or aucune d'elles n'a la valeur propre β pour T_3 . La seule possibilité est qu'il existe une forme icosaédrale f'' de caractère ε pour $\Gamma_0(800)$, et on voit facilement qu'elle doit être primitive.

On a donc démontré le théorème.

Mais il se pose plusieurs questions :

- Est-ce que f' est vecteur propre pour tous les opérateurs de Hecke ?
- Est-ce que la représentation ρ' donnée par f' est égale à ρ ?
- Est-ce qu'on a $f = f' = f''$?

En utilisant des techniques de majoration de discriminant, J. BUHLER montre le théorème suivant.

THÉORÈME 5. - Supposons que f' est un vecteur propre pour T_{11} , ou bien que l'hypothèse généralisée de Riemann est vraie. Alors

(i) f' est vecteur propre pour tous les opérateurs de Hecke,

(ii) ρ et ses tordues par les caractères de $G_{\underset{\sim}{Q}}$ vérifient la conjecture d'Artin,

(iii) $\rho = \rho'$, ρ' étant la représentation associée à f' .

(iv) $f = f'$.

S'il est difficile de vérifier l'hypothèse généralisée de Riemann, pour vérifier que f' est vecteur propre pour T_{11} , il suffit de connaître les mille premiers coefficients du développement de f .

Une lettre récente de J. BUHLER annonce qu'il a démontré le théorème 5.

Terminons cet exposé par une remarque due à J.-P. SERRE. Soit K le corps de groupe de Galois $\mathfrak{A}_5$ sur $\underset{\sim}{Q}$, considéré par BUHLER. Soit χ un caractère irréductible de $\mathrm{Gal}(K/\underset{\sim}{Q})$. Alors la fonction L_χ est holomorphe (sauf peut-être en 0 et 1). C'est le premier exemple de corps de type $\mathfrak{A}_5$ sur $\underset{\sim}{Q}$ tel que toutes les fonctions L associées soient holomorphes.

BIBLIOGRAPHIE

[1] BUHLER (J.). - Icosaedral Galois representations, Thèse, Harvard, 1977.

[2] DELIGNE (P.) et SERRE (J.-P.). - Formes modulaires de poids 1, Ann. scient. Ec. Norm. Sup., 4e série, t. 7, 1974, p. 507-530.

[3] LANGLANDS (R. P.). - Base change for GL(2) (preprint).

[4] SERRE (J.-P.) et TATE (J.). - Algèbre et géométrie. Cours au Collège de France, 1974/75 (non publié).

[5] TUNNELL (J.). - Isomorphism $\sigma \longmapsto \Pi(\sigma)$, Harvard, 1977 (preprint).

[6] WEIL (A.). - Dirichlet series and automorphic forms. - Berlin, Springer-Verlag, 1971 (Lecture Notes in Mathematics, 189).

[7] WEIL (A.). - Exercices dyadiques, Invent. Math., t. 27, 1974, p. 1-22.

(Texte reçu le 9 mai 1977)

Guy HENNIART
28 rue de Saussure
75017 PARIS