JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Nicolas BILLEREY et Filippo A. E. NUCCIO MORTARINO MAJNO DI CAPRIGLIO

Représentations galoisiennes diédrales et formes à multiplication complexe

Tome 30, n° 2 (2018), p. 651-670.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_651_0>

Journal de Théorie des Nombres
de Bordeaux **30** (2018), 651–670

Représentations galoisiennes diédrales et formes à multiplication complexe

par Nicolas BILLEREY et Filippo A. E. NUCCIO MORTARINO MAJNO DI CAPRIGLIO

Résumé. Pour une représentation galoisienne diédrale en caractéristique ℓ on établit (sous certaines hypothèses) l'existence d'une newform à multiplication complexe, dont on contrôle le poids, le niveau et le caractère, telle que la représentation ℓ-adique associée est congrue modulo ℓ à celle de départ.

Abstract. Given a dihedral Galois representation in characteristic ℓ, we establish (under some assumption) the existence of a CM newform, whose weight, level and Nebentypus we pin down, such that its ℓ-adic representation is congruent modulo ℓ to the one we started with.

1. Introduction

Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$, ℓ un nombre premier et $\overline{\mathbf{F}_\ell}$ une clôture algébrique du corps $\mathbf{F}_\ell$ à ℓ éléments. Par représentation galoisienne, on entend ici une représentation irréductible et continue $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}_\ell})$ où $\mathrm{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On dit qu'une telle représentation galoisienne est modulaire si elle est isomorphe à la réduction d'une représentation ℓ-adique associée à une forme parabolique propre f de poids ≥ 2. Dans ce cas, on dit alors aussi que ρ provient de la forme f.

On dit qu'une représentation galoisienne ρ est diédrale si son image projective dans $\mathrm{PGL}_2(\overline{\mathbf{F}_\ell})$, est isomorphe au groupe diédral D_n d'ordre $2n$ avec $n \geq 3$. Soit C_n l'unique sous-groupe cyclique d'ordre n de D_n. On note alors K le sous-corps quadratique de $\overline{\mathbf{Q}}$ laissé fixe par le noyau du caractère

$$\mathrm{G}_{\mathbf{Q}} \xrightarrow{\mathbf{P}\rho} D_n \longrightarrow D_n/C_n \simeq \{\pm 1\}$$

où $\mathbf{P}\rho$ est la composée de ρ avec la projection $\mathrm{GL}_2(\overline{\mathbf{F}_\ell}) \to \mathrm{PGL}_2(\overline{\mathbf{F}_\ell})$.

Manuscrit reçu le 5 décembre 2016, révisé le 16 mai 2017, accepté le 16 juin 2017.

Classification Mathématique (2010). 11F80, 11R37.

Mots-clefs. Représentations galoisiennes, théorie du corps de classes, formes modulaires à multiplication complexe.

N.B. remercie le projet ANR-14-CE25-0015 Gardio de l'Agence Nationale de la Recherche et la Fédération de Recherche en Mathématiques Rhône-Alpes-Auvergne (CNRS FR 3490) pour leur soutien financier.

Lors de la rédaction de ce travail, F.N. a bénéficié d'une décharge de service de l'Université Jean Monnet de Saint-Étienne, et tient à remercier les collègues qui l'ont rendue possible.

On rappelle qu'une newform $g = \sum_{n\geq 1} c_n q^n$ est dite à multiplication complexe s'il existe un caractère de Dirichlet non trivial ν tel que pour tout p dans un ensemble de nombres premiers de densité 1, on a $c_p = \nu(p)c_p$. On montre alors que le corps F correspondant au noyau de ν est quadratique imaginaire et on dit aussi que g a multiplication complexe par F.

Il est bien connu que les représentations galoisiennes attachées aux formes à multiplication complexe sont, en général, diédrales. Par ailleurs, c'est un cas particulier de la célèbre conjecture de modularité de Serre (qui était connu longtemps avant la démonstration générale de Khare–Wintenberger) qu'une représentation diédrale impaire provient d'une forme modulaire de poids ≥ 2. On trouve une preuve moderne de ce résultat dans [28], optimale par rapport au poids et au niveau, mais qui ne fournit pas de renseignement sur la nature de la forme modulaire correspondante. La construction d'une telle forme de poids ≥ 2 est aussi esquissée dans [6], en combinant l'exemple p. 517 avec les §6.9 et 6.10 ; là encore, rien ne justifie qu'elle soit à multiplication complexe.

Dans ce travail, on s'intéresse à la question plus précise de déterminer si une représentation galoisienne diédrale ρ donnée provient d'une forme modulaire *à multiplication complexe de poids* $k(\rho)$, où $k(\rho) \geq 2$ désigne le poids de Serre de la représentation ρ (défini dans [18, §2]). Dans ce cas, on souhaite également déterminer le niveau minimal de la forme correspondante.

Le résultat que l'on obtient dans cette direction est le suivant où l'on a noté $N(\rho)$ la partie première à ℓ du conducteur d'Artin de ρ (*loc. cit.*, n° 1.2) et $\varepsilon(\rho)$ le caractère associé à ρ par Serre (*loc. cit.*, n° 1.3).

Théorème 1.1. *Soit ρ une représentation galoisienne diédrale. Avec les notations précédentes, on suppose :*

(i) *K est quadratique imaginaire ;*
(ii) *$2 \leq k(\rho) \leq \ell - 1$ et $\ell \geq 5$.*

Alors, ρ est modulaire et provient d'une newform à multiplication complexe par le corps K, de poids $k(\rho)$ et de niveau

$$N' = \begin{cases} N(\rho) & \textit{si } \ell \textit{ est non ramifié dans } K; \\ \ell^2 N(\rho) & \textit{si } \ell \textit{ est ramifié dans } K. \end{cases}$$

De plus, on a les propriétés suivantes :

(1) *si ℓ est ramifié dans K, alors $\ell \in \{2k(\rho) - 1,\ 2k(\rho) - 3\}$;*
(2) *si $\varepsilon(\rho)$ est trivial, alors la forme à multiplication complexe peut être choisie de caractère trivial et de niveau divisant N'.*

Remarques 1.2.

(1) Dans le cas $\varepsilon(\rho) = 1$ et $k(\rho) = 2$, le théorème 1.1 est démontré dans [10].

(2) Le résultat est optimal au sens suivant. D'une part, si ρ provient d'une newform (à multiplication complexe ou non), alors celle-ci est de niveau divisible par $N(\rho)$: cela résulte d'un théorème de Carayol (voir [3, théorème (A)] et [4, §1–2]). D'autre part, l'exemple 4.1 de la section 4 montre que le niveau proposé ne peut, en général, être abaissé dans le cas où ℓ est ramifié dans K.

(3) L'hypothèse que K soit imaginaire entraîne en particulier que ρ est impaire, dans le sens que le déterminant de $\rho(c)$ vaut -1 pour toute conjugaison complexe $c \in \mathrm{G}_{\mathbf{Q}}$.

Soit $A/\mathbf{Q}$ une variété abélienne simple. On note $\mathrm{End}_{\mathbf{Q}}(A)$ l'anneau de ses endomorphismes définis sur $\mathbf{Q}$. Suivant une terminologie de Ribet, on dit que A est de type GL_2 si $E = \mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ est un corps de nombres de degré $\dim(A)$. Pour toute place finie λ de E au-dessus de ℓ de corps résiduel $\mathbf{F}_\lambda$, on note alors

$$\rho_{A,\lambda} : \mathrm{G}_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda)$$

la représentation donnant l'action de $\mathrm{G}_{\mathbf{Q}}$ sur $A[\lambda]$ (voir [13, p. 7]). Le corollaire suivant au théorème 1.1 ci-dessus généralise [5, Theorem 1.6] et justifie [7, Remark 4.4] ; c'est essentiellement une conséquence de [10, Theorem 1]. Pour les définitions et propriétés des sous-groupes de Cartan, voir [16, §2] ou [9, Chapter XI, §2].

Corollaire 1.3. *Soit $A/\mathbf{Q}$ une variété abélienne de type GL_2 de conducteur N_A et λ une place finie de $E = \mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ au-dessus de ℓ. On suppose $\ell \geq 5$, $\ell \nmid N_A$ et l'image de $\rho_{A,\lambda}$ contenue dans le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_\lambda)$. Alors, $\rho_{A,\lambda}$ provient d'une newform à multiplication complexe de poids 2 et de niveau $N(\rho_{A,\lambda})$ (divisant N_A) qui, de plus, est de caractère trivial lorsque E est totalement réel et A a tous ses endomorphismes définis sur $\mathbf{Q}$.*

Démonstration. D'après [13, Lemma 3.1], on a $\det(\rho_{A,\lambda}) = \epsilon\chi$, où χ désigne le caractère cyclotomique mod ℓ et ϵ est un caractère non ramifié hors de N_A et même trivial lorsque E est totalement réel et A a tous ses endomorphismes définis sur $\mathbf{Q}$ [12, Lemma 4.5.1]. Soit G_ℓ un groupe de décomposition en ℓ de $\mathrm{G}_{\mathbf{Q}}$ et I_ℓ son sous-groupe d'inertie. On sait que la semi-simplifiée de $\rho_{A,\lambda}|_{I_\ell}$ se factorise par l'inertie modérée et qu'elle est donc diagonalisable ([16, proposition 4 et s.]). On note ϕ et ϕ' les deux caractères correspondant. D'après [11, corollaire 3.4.4], on peut écrire $\phi = \psi_2^a \psi_2'^b$ et $\phi' = \psi_2^n \psi_2'^m$ où ψ_2 et ψ_2' sont les deux caractères fondamentaux de niveau 2 ([16, n$^\mathrm{o}$ 1.7]) et où a, b, n et m sont des entiers égaux à 0 ou 1. Comme

$\phi\phi' = \chi = \psi_2\psi_2'$, il vient :

$$\{\phi, \phi'\} = \{\psi_2, \psi_2'\} \quad \text{ou} \quad \{\phi, \phi'\} = \{1, \chi\}.$$

Le premier cas donne $k(\rho_{A,\lambda}) = 2$ d'après (2.8.1) de [18, proposition 3]. En particulier, on a $\varepsilon(\rho_{A,\lambda}) = \epsilon$. Par ailleurs, l'image de $\rho_{A,\lambda}$ ne contient pas d'élément d'ordre ℓ. Dans le second cas, on a donc

$$\rho_{A,\lambda}|_{I_\ell} \simeq \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}$$

et on conclut à $k(\rho_{A,\lambda}) = 2$ d'après (2.8.2) de *loc. cit.* Or, la représentation $\rho_{A,\lambda}$ est impaire d'après [13, Lemma 3.2]. Pour toute conjugaison complexe $c \in \mathrm{G}_{\mathbf{Q}}$, l'élément $\rho_{A,\lambda}(c)$ est donc conjugué à la matrice diagonale de valeurs propres $\{-1, +1\}$. Comme celles-ci ne sont pas conjuguées sur $\mathbf{F}_\lambda$, l'élément $\rho_{A,\lambda}(c)$ n'est contenu dans aucun sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_\lambda)$ ([9, p. 181]). En particulier, la représentation $\rho_{A,\lambda}$ est diédrale et le corps quadratique K correspondant est imaginaire. Comme $\ell \geq 5$ et $k(\rho_{A,\lambda}) = 2$, on déduit du théorème 1.1 le résultat voulu. □

L'article est organisé de la façon suivante. La section 2 contient des rappels sur les Größencharaktere et un résultat (proposition 2.1) essentiel à la démonstration du théorème principal (théorème 1.1) qui, elle, occupe la section 3. La dernière section est consacrée à deux exemples numériques.

Remerciements. Les auteurs remercient Gebhard Böckle pour une question ayant mené à ce travail. N.B. est également reconnaissant envers Imin Chen, Luis Dieulefait, Pierre Lezowski et Joan Nualart pour d'intéressantes discussions.

2. Une proposition de la théorie du corps de classes

Dans cette section, on rappelle quelques notions sur les Größencharaktere puis on démontre une proposition (proposition 2.1) de la théorie du corps de classes qui nous sera utile au paragraphe 3.4. Dans toute la suite, K désigne un corps quadratique imaginaire contenu dans $\overline{\mathbf{Q}}$. On identifie $\overline{\mathbf{Q}}$ à un sous-corps de $\mathbf{C}$ et on fixe, une fois pour toutes, un plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$ où $\overline{\mathbf{Q}}_\ell$ désigne une clôture algébrique de $\mathbf{Q}_\ell$ de corps résiduel $\overline{\mathbf{F}}_\ell$. Cela induit une place de $\overline{\mathbf{Q}}$ au-dessus de ℓ notée v.

On adopte par ailleurs les notations suivantes :

- $\mathcal{O}_K$ est l'anneau des entiers de K, $\mathcal{O}_K^\times$ son groupe des unités et $-D_K$ son discriminant ;
- Σ_K est l'ensemble des places ultramétriques de K ;
- K_w est le complété de K en w ($w \in \Sigma_K$) ;
- $\mathcal{O}_w^\times$, π_w, p_w sont respectivement le groupe des unités, une uniformisante et la caractéristique résiduelle du corps local K_w ($w \in \Sigma_K$) ;

- $\mathcal{O}_w^{(m)}$ est l'ensemble des unités $u \in \mathcal{O}_w^\times$ congrues à 1 modulo π_w^m avec $m \geq 1$ entier ($w \in \Sigma_K$) ;
- $\mathfrak{p}_w$ est l'idéal premier de $\mathcal{O}_K$ induit par w ($w \in \Sigma_K$) ;
- $\mathbf{A}_K^\times$ est le groupe des idèles de K ; si $a \in \mathbf{A}_K^\times$ et $w \in \Sigma_K$, on note a_w la composante de a en w ;
- $C_K = \mathbf{A}_K^\times / K^\times$ est le groupe des classes d'idèles de K ;
- $\mathbf{A}_{K,\mathrm{f}}^\times$ (resp. $\mathbf{A}_{K,\infty}^\times$) est l'ensemble des idèles finis (resp. infinis) de K.
- Étant donnés une place $w \in \Sigma_K$ et un idéal fractionnaire $\mathfrak{m}$ de K, on note $\mathrm{ord}_w(\mathfrak{m})$ la valuation de $\mathfrak{m}$ en l'idéal premier $\mathfrak{p}_w$. On définit
$$U_\mathfrak{m} = \left\{ a \in \mathbf{A}_K^\times \,\middle|\, w(a_w - 1) \geq \mathrm{ord}_w(\mathfrak{m}),\ \forall\, w \in \Sigma_K \right\}$$
et $E_\mathfrak{m} = U_\mathfrak{m} \cap \mathcal{O}_K^\times$.
- Enfin, si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$, on note $\pi_\mathfrak{p}$ une uniformisante locale en la place de K induite par $\mathfrak{p}$.

2.1. Par Größencharakter χ de K on entend ici un homomorphisme de groupes continu
$$\chi : \mathbf{A}_K^\times \longrightarrow \mathbf{C}^\times$$
tel que $\chi(K^\times) = 1$. Si $w \in \Sigma_K$, on note χ_w la composante en w de χ et on désigne par χ_f (resp. χ_∞) la partie finie (resp. infinie) de χ. On dit que χ est ramifié en $w \in \Sigma_K$ s'il existe une unité $u \in \mathcal{O}_w^\times$ telle que $\chi_w(u) \neq 1$. Dans le cas contraire, on dit que χ est non ramifié en w. Par continuité, χ est non ramifié en toutes les places de K sauf un nombre fini. Si χ est ramifié en $w \in \Sigma_K$, il existe un entier $m_w \geq 1$ minimal tel que $\chi_w(\mathcal{O}_w^{(m_w)}) = 1$. Le conducteur de χ est alors, par définition, l'idéal de $\mathcal{O}_K$
$$\mathfrak{f}_\chi = \prod_w \mathfrak{p}_w^{m_w}$$
où $w \in \Sigma_K$ parcourt l'ensemble des places où χ est ramifié.

On dit enfin qu'un Größencharakter χ est de type à l'infini (m, n) avec $m, n \in \mathbf{Z}$ lorsque
$$\chi_\infty(z) = \frac{1}{z^m (z^c)^n}, \quad \text{pour tout } z \in \mathbf{A}_{K,\infty}^\times \simeq \mathbf{C}^\times,$$
où z^c désigne le conjugué complexe de z. Un tel Größencharakter est de type (A_0) dans la terminologie de Weil ([27, p. 4]).

2.2. On note $z \mapsto \overline{z}$ l'homomorphisme de réduction $\overline{\mathbf{Z}}_\ell \to \overline{\mathbf{F}}_\ell$ où $\overline{\mathbf{Z}}_\ell$ désigne l'anneau des entiers de $\overline{\mathbf{Q}}_\ell$.

Soit $\overline{\mathbf{Z}}$ l'anneau des entiers de $\overline{\mathbf{Q}}$. Il existe alors ([26, Chapter 2]) un unique homomorphisme de groupes $\overline{\mathbf{F}}_\ell^\times \to \overline{\mathbf{Z}}^\times$ noté $x \mapsto \widetilde{x}$ à valeurs dans les racines de l'unité d'ordre premier à ℓ tel que
$$x = \overline{\widetilde{x}}, \quad \text{pour tout } x \in \overline{\mathbf{F}}_\ell^\times.$$

Par ailleurs, si ζ est une racine de l'unité d'ordre premier à ℓ, on a $\zeta = \overline{\widetilde{\zeta}}$.

Étant donné un groupe G et un caractère $\varphi : G \to \overline{\mathbf{F}}_\ell^\times$, on définit le relèvement de Teichmüller (ou multiplicatif)

$$\widetilde{\varphi} : G \longrightarrow \overline{\mathbf{Q}}^\times$$

de φ comme le composé de φ avec le morphisme $x \mapsto \widetilde{x}$ ci-dessus. C'est le seul caractère à valeurs dans les racines de l'unité d'ordre premier à ℓ de $\overline{\mathbf{Q}}$ vérifiant

$$\overline{\widetilde{\varphi}(x)} = \varphi(x), \quad \text{pour tout } x \in G.$$

2.3. Étant donné un Größencharakter χ de K de type à l'infini (m, n) avec $m, n \geq 0$, on vérifie que pour toute place $w \in \Sigma_K$, on a $\chi(\pi_w) \in \overline{\mathbf{Z}}$, où l'on note encore $\pi_w \in \mathbf{A}_{K,\mathrm{f}}^\times$ l'idèle ayant composantes triviales en dehors de w et qui coïncide avec l'uniformisante π_w choisie en w. En effet, si h désigne le nombre de classes de K, l'idéal $\mathfrak{p}_w^h$ est principal et engendré par, disons, $a \in \mathcal{O}_K$. Soit x l'idèle $\pi_w^h a^{-1}$. Alors x est une unité en toute place finie de K et on a

$$\chi(\pi_w)^h = \chi\left(\pi_w^h\right)\chi\left(a^{-1}\right) = \chi(x) = \chi_{\mathrm{f}}(x) a^m (a^c)^n \in \overline{\mathbf{Z}}.$$

La proposition suivante est le résultat principal de cette section ; elle généralise notamment [5, Proposition 3.1].

Proposition 2.1. *Supposons $\ell \geq 5$. Soit α un Größencharakter de K d'image finie et de conducteur $\mathfrak{f}_\alpha$, et soit k un entier ≥ 2. Alors, il existe un Größencharakter δ de K de type à l'infini $(k-1, 0)$ et conducteur $\mathfrak{f}_\delta$ vérifiant*

$$\operatorname{ord}_w(\mathfrak{f}_\delta) = \operatorname{ord}_w(\mathfrak{f}_\alpha) \quad \textit{pour toute place } w \in \Sigma_K \setminus \{v\} \tag{2.1}$$

et tel quel pour toute place $w \in \Sigma_K \setminus \{v\}$ première à $\mathfrak{f}_\alpha$, on a

$$\overline{\delta(\pi_w)} = \overline{\alpha(\pi_w)}. \tag{2.2}$$

De plus, on a

(1) *si* $\operatorname{ord}_v(\mathfrak{f}_\alpha) \geq 2$, *alors* $\operatorname{ord}_v(\mathfrak{f}_\delta) = \operatorname{ord}_v(\mathfrak{f}_\alpha)$ *;*

(2) *si* $\operatorname{ord}_v(\mathfrak{f}_\alpha) = 1$, *alors*

$$\operatorname{ord}_v(\mathfrak{f}_\delta) = \begin{cases} 0 & \textit{si pour toute unité } u \in \mathcal{O}_v^\times \textit{ on a } \alpha_v(u) = \widetilde{\overline{u}}^{1-k} \\ 1 & \textit{sinon ;} \end{cases}$$

(3) *si* $\operatorname{ord}_v(\mathfrak{f}_\alpha) = 0$, *alors*

$$\operatorname{ord}_v(\mathfrak{f}_\delta) = \begin{cases} 0 & \textit{si } \ell^f - 1 \mid k - 1 \\ 1 & \textit{sinon,} \end{cases}$$

où f est le degré résiduel de K en ℓ.

Démonstration. Comme on a supposé K quadratique imaginaire et $\ell \geq 5$, on a, avec les notations précédentes, $E_{\mathfrak{p}_v} = U_{\mathfrak{p}_v} \cap \mathcal{O}_K^\times = \{1\}$. D'après [16, p. 286], il existe alors $f \in \mathrm{Hom}(\mathbf{A}_K^\times, \mathbf{C}^\times)$ tel que

(I) $f(x) = 1$ pour tout $x \in U_{\mathfrak{p}_v}$,
(II) $f(x) = x^{k-1}$ pour tout $x \in K^\times$.

Posons alors

$$\beta(x) = f(x)x_\infty^{1-k}, \quad \text{pour tout } x \in \mathbf{A}_K^\times,$$

où $x_\infty \in \mathbf{A}_{K,\infty}^\times$ désigne la composante à l'infini de l'idèle x. Comme $U_{\mathfrak{p}_v}$ est ouvert dans $\mathbf{A}_K^\times$ et contenu dans le noyau de f, il s'en suit que f, puis l'homomorphisme β, sont continus. Par ailleurs, si $x \in K^\times$, on a d'après la propriété (II) ci-dessus

$$\beta(x) = f(x)x^{1-k} = 1.$$

Autrement dit, β est un Größencharakter de K. De plus, si $w \in \Sigma_K$ et $x \in \mathcal{O}_w^\times \cap U_{\mathfrak{p}_v}$, on a $\beta_w(x) = 1$. En particulier, β est de conducteur divisant $\mathfrak{p}_v$. Enfin, si $x \in \mathbf{A}_{K,\infty}^\times$, on a $x \in U_{\mathfrak{p}_v}$, puis $\beta_\infty(x) = x^{1-k}$. Le Größencharakter β est donc de type à l'infini $(k-1, 0)$.

Comme l'a montré Weil dans [27, p. 5], il existe une extension finie L de $\mathbf{Q}$, qu'on regarde plongée dans $\overline{\mathbf{Q}}$, qui contient les valeurs de β_w pour toute place w. Quitte à l'élargir, on peut de plus supposer qu'elle contient K. On note L_v le complété de L en la place de L induite par la place v de $\overline{\mathbf{Q}}$ et on commence par définir un caractère $\gamma_0 : \mathbf{A}_K^\times \to L_v^\times$ par la règle

$$\begin{cases} (\gamma_0)_w = \beta_w^{-1} & (w \in \Sigma_K \setminus \{v\}) \\ (\gamma_0)_v = \beta_v^{-1} \cdot (-)^{k-1} & \\ (\gamma_0)_\infty = 1 & \end{cases}$$

où $(-)^{k-1}$ désigne l'élévation à la puissance $k-1$. En tant que produit de caractères continus, γ_0 est continu. Soit $a \in K^\times$. On a alors

$$\begin{aligned} \gamma_0(a) &= \left(\prod_{w \in \Sigma_K \setminus \{v\}} \beta_w(a)^{-1} \right) \cdot \beta_v(a)^{-1} \cdot a^{k-1} \\ &= \beta_{\mathrm{f}}(a)^{-1} \cdot a^{k-1} = \beta_\infty(a) \cdot a^{k-1} = 1 \end{aligned}$$

car β est trivial sur les idèles principaux et de type à l'infini $(k-1, 0)$. Il s'en suit que l'on peut regarder γ_0 en tant que caractère continu de C_K et aussi du quotient $C_K/\mathbf{A}_{K,\infty}^\times$. Comme K est totalement imaginaire, l'isomorphisme de réciprocité de la théorie du corps de classes globale identifie ce quotient avec l'abélianisé $\mathrm{G}_K^{\mathrm{ab}}$ de G_K, et montre en particulier qu'il s'agit d'un groupe compact. L'image de l'homomorphisme continu γ_0 est donc contenue dans le groupe $\mathcal{O}_{L_v}^\times$ des unités de L_v. On note

$$\overline{\gamma_0} : \mathbf{A}_K^\times \longrightarrow \overline{\mathbf{F}}_\ell^\times$$

la composée de γ_0 avec l'homomorphisme de réduction $\overline{\mathbf{Z}}_\ell \to \overline{\mathbf{F}}_\ell$. C'est un caractère d'image finie. On définit alors

$$\gamma = \widetilde{\overline{\gamma_0}} : \mathbf{A}_K^\times \longrightarrow \overline{\mathbf{Z}}^\times \subset \mathbf{C}^\times$$

comme étant le relèvement de Teichmüller de $\overline{\gamma_0}$ détaillé au paragraphe 2.2. Il s'agit donc d'un Größencharakter de type à l'infini $(0,0)$, type dit « trivial ».

Pour compléter la preuve de la proposition, posons $\delta = \alpha\beta\gamma$: il s'agit bien d'un Größencharakter de type à l'infini égal au type à l'infini de β, à savoir $(k-1,0)$, puisque tant α que γ ont un type à l'infini trivial. Il reste à présent à déterminer $\mathfrak{f}_\delta$ et à démontrer les congruences (2.2).

Montrons tout d'abord les congruences (2.2). Soit $w \in \Sigma_K \setminus \{v\}$ une place ultramétrique de K en laquelle α est non ramifié. D'après ce qui précède, on a $\gamma_0(\pi_w) = \beta(\pi_w)^{-1} \in \overline{\mathbf{Z}}_\ell^\times$ et, par ailleurs, $\alpha(\pi_w) \in \overline{\mathbf{Z}}_\ell$. Par réduction, il vient donc

$$\overline{\delta(\pi_w)} = \overline{\alpha(\pi_w)}\,\overline{\beta(\pi_w)}\,\overline{\beta(\pi_w)^{-1}} = \overline{\alpha(\pi_w)}$$

et le résultat souhaité.

Étudions à présent le conducteur $\mathfrak{f}_\delta$. Soit w une place finie de K distincte de v et $u \in \mathcal{O}_w^\times$. Comme β est non ramifié en w, on a $\beta_w(u) = 1 = \gamma_w(u)$ et donc $\delta_w(u) = \alpha_w(u)$, ce qui entraîne (2.1).

Passons maintenant à la démonstration des points (1)–(3). Soit $u \in \mathcal{O}_v^\times$. Comme $\mathfrak{f}_\beta \mid \mathfrak{p}_v$, le caractère β_v est trivial sur $\mathcal{O}_v^{(1)}$ et $\beta_v(u)$ est une racine de l'unité d'ordre premier à ℓ. On a donc $\gamma_v(u) = \beta_v(u)^{-1}\widetilde{\overline{u}}^{k-1}$, puis

$$\delta_v(u) = \alpha_v(u)\widetilde{\overline{u}}^{k-1}. \tag{2.3}$$

En particulier, on a $\delta_v(u) = \alpha_v(u)$, pour toute unité $u \in \mathcal{O}_v^{(1)}$.

(1) Supposons $\operatorname{ord}_v(\mathfrak{f}_\alpha) \geq 2$. Alors, il existe une unité $u \in \mathcal{O}_v^{(1)}$ telle que $\delta_v(u) = \alpha_v(u) \neq 1$. D'où $\operatorname{ord}_v(\mathfrak{f}_\delta) \geq 2$ et $\operatorname{ord}_v(\mathfrak{f}_\delta) = \operatorname{ord}_v(\mathfrak{f}_\alpha)$ car les restrictions de δ_v et α_v à $\mathcal{O}_v^{(1)}$ coïncident.

(2) Supposons $\operatorname{ord}_v(\mathfrak{f}_\alpha) = 1$. Pour toute unité $u \in \mathcal{O}_v^{(1)}$, on a alors $\delta_v(u) = 1$, d'où $\operatorname{ord}_v(\mathfrak{f}_\delta) \leq 1$. Par ailleurs, d'après (2.3), on a $\operatorname{ord}_v(\mathfrak{f}_\delta) = 1$ si, et seulement si, il existe une unité $u \in \mathcal{O}_v^\times$ telle que $\alpha_v(u) \neq \widetilde{\overline{u}}^{1-k}$.

(3) Supposons $\operatorname{ord}_v(\mathfrak{f}_\alpha) = 0$. Alors pour toute unité $u \in \mathcal{O}_v^\times$, on a $\delta_v(u) = \widetilde{\overline{u}}^{k-1}$ et donc le caractère δ_v est trivial sur $\mathcal{O}_v^{(1)}$, c'est-à-dire $\operatorname{ord}_v(\mathfrak{f}_\delta) \leq 1$. Par ailleurs, le quotient $\mathcal{O}_v^\times/\mathcal{O}_v^{(1)}$ s'identifie

à $(\mathcal{O}_K/\mathfrak{p}_v)^\times$. En particulier, on a $\mathrm{ord}_v(\mathfrak{f}_\delta) = 0$ si, et seulement si, $\ell^f - 1$ divise $k-1$.

Cela termine la démonstration de la proposition 2.1. $\square$

3. Démonstration du théorème principal

3.1. Étude locale. On commence par rappeler la définition centrale suivante.

Définition 3.1. Une représentation irréductible continue $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ est dite diédrale si son image projective dans $\mathrm{PGL}_2(\overline{\mathbf{F}}_\ell)$, est isomorphe au groupe diédral D_n d'ordre $2n$ avec $n \geq 3$.

Soit $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ une représentation galoisienne satisfaisant aux hypothèses du théorème 1.1. On vérifie à l'aide de la classification des sous-groupes finis de $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ (voir par exemple [2, Theorem 3.4]) que l'ordre de l'image de ρ est nécessairement premier à ℓ. Avec les notations de l'Introduction, on a donc en particulier $\mathrm{pgcd}(n, \ell) = 1$. Par construction, $\mathbf{P}\rho(\mathrm{G}_K) = C_n$ est cyclique, avec $\mathrm{G}_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$. Comme $\mathbf{P}\rho(\mathrm{G}_K)$ s'obtient à partir de $\rho(\mathrm{G}_K)$ après passage au quotient par des éléments de son centre, on en déduit que $\rho(\mathrm{G}_K)$ est abélienne. Ainsi, il existe deux caractères

$$\varphi, \varphi' : \mathrm{G}_K \longrightarrow \overline{\mathbf{F}}_\ell^\times$$

tels que $\varphi \neq \varphi'$ et $\rho|_{\mathrm{G}_K} \simeq \varphi \oplus \varphi'$. Soit $\sigma \in \mathrm{G}_{\mathbf{Q}} \setminus \mathrm{G}_K$. On définit $\widehat{\varphi} : \mathrm{G}_K \to \overline{\mathbf{F}}_\ell^\times$ par $\widehat{\varphi}(\tau) = \varphi(\sigma^{-1}\tau\sigma)$ pour tout $\tau \in \mathrm{G}_K$: cette définition est indépendante de σ car l'image de φ est abélienne. Soit v un vecteur propre pour $\rho|_{\mathrm{G}_K}$ de valeur propre $\varphi(\tau)$ pour tout $\tau \in \mathrm{G}_K$. On a alors, pour tout $\tau \in \mathrm{G}_K$,

$$\rho(\tau)\rho(\sigma)v = \rho(\sigma\sigma^{-1}\tau\sigma)v = \rho(\sigma)\rho(\sigma^{-1}\tau\sigma)v = \widehat{\varphi}(\tau)\rho(\sigma)v$$

d'où l'on déduit $\varphi' = \widehat{\varphi}$. On a donc $\rho \simeq \mathrm{Ind}_{\mathrm{G}_K}^{\mathrm{G}_{\mathbf{Q}}}(\varphi) \simeq \mathrm{Ind}_{\mathrm{G}_K}^{\mathrm{G}_{\mathbf{Q}}}(\widehat{\varphi})$. Dans la base $\{v, \rho(\sigma)v\}$, la matrice de $\rho(\sigma)$ s'écrit

$$\begin{pmatrix} 0 & \varphi(\sigma^2) \\ 1 & 0 \end{pmatrix}. \tag{3.1}$$

L'objectif de ce paragraphe est d'étudier la ramification de φ et de K en ℓ. Soit G_ℓ le groupe de décomposition de $\mathrm{G}_{\mathbf{Q}}$ relatif au plongement fixé $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$ et I_ℓ son sous-groupe d'inertie. On note pour simplifier $k = k(\rho)$, avec $k(\rho)$ comme dans [18, §2]. On rappelle que l'on a supposé $2 \leq k \leq \ell - 1$ et $\ell \geq 5$.

L'image de ρ est d'ordre premier à ℓ. En particulier, $\rho|_{I_\ell}$ se factorise par l'inertie modérée et est diagonalisable ([16, proposition 4 et s.]). On note ϕ et ϕ' les deux caractères correspondants. Ils sont de niveau 1 ou 2 et lorsqu'ils sont de niveau 2, on a $\phi' = \phi^\ell$ ([18, proposition 1]). On rappelle que $\mathfrak{p}_v$ désigne l'idéal premier de K au-dessus de ℓ induit par la place v (c'est-à-dire par le plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$). On considère alors les groupes de décomposition $\mathrm{G}_{\mathfrak{p}_v} \leq \mathrm{G}_\ell$ et d'inertie $I_{\mathfrak{p}_v} \leq I_\ell$.

(1) On suppose que ϕ et ϕ' sont de niveau 1. Comme l'image de ρ ne contient pas d'élément d'ordre ℓ, l'image par ρ de l'inertie sauvage est triviale. Comme on a supposé $2 \leq k \leq \ell - 1$, on a, d'après [18, (2.3.2)],

$$\rho|_{I_\ell} = \begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1} \end{pmatrix}$$

où χ désigne le caractère cyclotomique mod ℓ.

(a) Supposons ℓ non ramifié dans K. Alors, $I_{\mathfrak{p}_v}$ s'identifie à I_ℓ et, comme $\ell > k$, le caractère χ^{k-1} est non trivial. On en déduit que soit φ est non ramifié en $\sigma(\mathfrak{p}_v)$ et que sa restriction au sous-groupe d'inertie en $\mathfrak{p}_v$ est donnée par la puissance $(k-1)$-ième du caractère cyclotomique, ou qu'il en est ainsi pour φ'. Si $\sigma(\mathfrak{p}_v) = \mathfrak{p}_v$, c'est une contradiction dans les deux cas. On a donc montré que ℓ est décomposé dans K. Par ailleurs, quitte à remplacer v par σv, on peut supposer φ non ramifié en $\sigma(\mathfrak{p}_v)$ et modérément ramifié en $\mathfrak{p}_v$ avec, pour tout $\tau \in I_{\mathfrak{p}_v}$, $\varphi(\tau) = \chi^{k-1}(\tau)$.

(b) Supposons ℓ ramifié dans K. Alors, d'après la définition (donnée en Introduction) du corps K, on a $\mathbf{P}\rho(I_\ell) \not\subset C_n$. Or, l'image du caractère χ^{k-1} est d'ordre $(\ell-1)/\operatorname{pgcd}(\ell-1, k-1)$ et, en vue de la description de $\rho|_{I_\ell}$, elle coïncide avec l'image de $\mathbf{P}\rho(I_\ell)$, qui est donc cyclique et par suite d'ordre 2. On en tire $\ell - 1 = 2 \cdot \operatorname{pgcd}(\ell-1, k-1)$, d'où $\ell = 2k-1$ car $\ell > k$. En outre, le fait que $\mathbf{P}\rho(I_\ell)$ soit d'ordre 2 montre que l'indice de ramification de ℓ dans l'extension $\overline{\mathbf{Q}}^{\operatorname{Ker}(\mathbf{P}\rho)}/\mathbf{Q}$ est égal à 2 et par suite $\mathbf{P}\rho(I_{\mathfrak{p}_v}) = 1$. Il vient donc que φ est non ramifié en $\mathfrak{p}_v$.

(2) On suppose que ϕ et ϕ' sont de niveau 2. Alors, d'après [18, n° 2.2], $\rho|_{I_\ell}$ est irréductible. En particulier, cela exclut d'avoir $\mathrm{G}_\ell \subset \mathrm{G}_K$, i.e. ℓ décomposé dans K. Autrement dit, ℓ est inerte ou ramifié dans K et comme on a supposé $2 \leq k \leq \ell - 1$, on a d'après [18, (2.2.4)]

$$\rho|_{I_\ell} = \begin{pmatrix} \psi_2^{k-1} & 0 \\ 0 & \psi_2^{\ell(k-1)} \end{pmatrix},$$

où ψ_2 est un caractère fondamental de niveau 2 (pour sa définition, voir [16, n° 1.7]). On trouve que le caractère ψ_2^{k-1} est d'ordre

$$\frac{\ell^2 - 1}{\operatorname{pgcd}(\ell^2 - 1, k-1)} > 2$$

et n'est donc trivial sur aucun sous-groupe de I_ℓ d'indice ≤ 2. Par conséquent, tant φ que φ' sont ramifiés en $\mathfrak{p}_v$ et, quitte à remplacer φ avec φ', on a que $\varphi(\tau) = \psi_2^{k-1}(\tau)$ pour tout $\tau \in I_{\mathfrak{p}_v}$.

Supposons enfin ℓ ramifié dans K. Comme précédemment, l'image projective $\mathbf{P}\rho(I_\ell)$ n'est pas contenue dans C_n. Or, $\mathbf{P}\rho(I_\ell)$ est cyclique et s'identifie à l'image de $\psi_2^{(\ell-1)(k-1)}$. On en déduit que $\mathbf{P}\rho(I_\ell)$ est d'ordre 2, puis que $2 \cdot \operatorname{pgcd}(\ell^2 - 1, (\ell-1)(k-1)) = \ell^2 - 1$, et finalement $\ell = 2k - 3$.

On résume les résultats ci-dessus dans la proposition suivante.

Proposition 3.2. *Avec les hypothèses et notations de ce paragraphe, on peut supposer que l'on est dans l'une des situations suivantes.*

(1) *Supposons ϕ et ϕ' de niveau 1. Alors,*
   (a) *soit ℓ est décomposé dans K et dans ce cas φ est non ramifié en $\sigma(\mathfrak{p}_v)$, modérément ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \chi^{k-1}(\tau)$, où χ désigne le caractère cyclotomique mod ℓ.*
   (b) *soit ℓ est ramifié dans K et dans ce cas on a $\ell = 2k - 1$ et φ est non ramifié en $\mathfrak{p}_v$.*

(2) *Supposons ϕ et ϕ' de niveau 2. Alors,*
   (a) *soit ℓ est inerte dans K ;*
   (b) *soit ℓ est ramifié dans K et $\ell = 2k - 3$.*

   Dans les deux cas, φ est ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \psi_2^{k-1}(\tau)$, avec ψ_2 caractère fondamental de niveau 2.

3.2. On étudie ici la variation du conducteur d'Artin par rapport à l'opération d'induction. On rappelle que l'on a $\rho = \operatorname{Ind}_{\mathrm{G}_K}^{\mathrm{G}_{\mathbf{Q}}}(\varphi)$. On désigne par $\mathfrak{N}(\rho)$ (resp. $\mathfrak{N}(\varphi)$) le conducteur d'Artin de ρ (resp. de φ) défini dans [14, chapitre VI, §3]. Ce sont, par définition, des idéaux de $\mathbf{Z}$ et de $\mathcal{O}_K$, respectivement. On rappelle que, suivant la notation de Serre [18, n° 1.2], $N(\rho)$ désigne le générateur positif de la partie première à ℓ de $\mathfrak{N}(\rho)$.

Pour un entier naturel n, on note $n^{(\ell)}$ sa partie première à ℓ. Le résultat suivant résulte de [23, Corollary 1].

Lemme 3.3 (Taguchi)**.** *Avec les notations et hypothèses précédentes, on a*

$$N(\rho) = D_K^{(\ell)} \operatorname{Norm}_{K/\mathbf{Q}}(\mathfrak{N}(\varphi))^{(\ell)}.$$

Remarque 3.4. Dans [23] aucune preuve du Corollary 1 n'est offerte et l'auteur fait référence à [14, Chapter VI, §3], où le procédé de « globalisation » est traité dans le cas de représentations à coefficients complexes, et cela en utilisant la théorie des caractères. Il est bien connu (voir, par exemple, [17, §15.5]) que cette théorie s'étend aux représentations en caractéristique ℓ d'un groupe d'ordre premier à ℓ, ce qui est le contexte dans lequel nous travaillons à présent. Les arguments de [14, chapitre VI, §3] s'adaptent alors pour prouver la validité du résultat cité de Taguchi.

3.3. Dans ce paragraphe, on fixe une extension finie $L/\mathbf{Q}_\ell$. On note k_L son corps résiduel de sorte que l'on a $k_L = \mathbf{F}_q$ où $q = |k_L|$ désigne le cardinal de k_L. On note L^{ab} (resp. L^{nr}) l'extension abélienne (resp. non ramifiée) maximale de L contenue dans $\overline{\mathbf{Q}}_\ell$. Le morphisme $\theta_{q-1} : \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/L^{\mathrm{nr}}) \to k_L^\times$ construit par Serre dans [16, §1.3] (et dont les conjugués sur k_L forment l'ensemble des caractères fondamentaux de niveau r de $\overline{\mathbf{Q}}_\ell/L$, où $q = \ell^r$) se factorise par le groupe $I_t(L^{\mathrm{ab}}/L)$ d'inertie modérée de l'extension L^{ab}/L et on note encore

$$\theta_{q-1} : I_t(L^{\mathrm{ab}}/L) \longrightarrow k_L^\times$$

le morphisme passé au quotient. Par ailleurs, l'application de réciprocité de la théorie du corps de classes locale fournit un homomorphisme surjectif

$$\omega : k_L^\times \longrightarrow I_t(L^{\mathrm{ab}}/L).$$

Un calcul, détaillé dans [16, proposition 3], montre alors que l'on a

$$\theta_{q-1}(\omega(x)) = x^{-1}, \tag{3.2}$$

pour tout $x \in k_L^\times$. Ce résultat nous sera utile dans la démonstration qui suit.

3.4. Démonstration du théorème principal. On reprend les notations et hypothèses du paragraphe 3.1. Soit $\widetilde{\varphi} : \mathrm{G}_K \to \overline{\mathbf{Z}}^\times \subset \mathbf{C}^\times$ le relèvement multiplicatif de φ défini au paragraphe 2.2. Il se factorise par l'abélianisé $\mathrm{G}_K^{\mathrm{ab}}$ de G_K. On note

$$\mathrm{rec}_K : \mathbf{A}_K^\times \longrightarrow \mathrm{G}_K^{\mathrm{ab}}$$

l'application de réciprocité de la théorie du corps de classes globale et on pose

$$\alpha = \widetilde{\varphi} \circ \mathrm{rec}_K : \mathbf{A}_K^\times \longrightarrow \mathbf{C}^\times.$$

C'est un Größencharakter de K d'image finie, de conducteur $\mathfrak{f}_\alpha$ égal au conducteur d'Artin de φ (voir [14, chapitre VI, notamment p. 110]). D'après le lemme 3.3 et la construction de α, on a

$$N(\rho) = D_K^{(\ell)}\,\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{N}(\varphi))^{(\ell)} = D_K^{(\ell)}\,\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\alpha)^{(\ell)}. \tag{3.3}$$

Soit δ le Größencharakter de K fourni par la proposition 2.1 appliquée au Größencharakter α ci-dessus et à l'entier $k = k(\rho)$. On définit un caractère, noté δ_{H}, du groupe des idéaux fractionnaires de K premiers à $\mathfrak{f}_\delta$ de la façon suivante :

$$\delta_{\mathrm{H}}(\mathfrak{p}) = \delta(\pi_\mathfrak{p}) \quad \text{pour tout premier } \mathfrak{p} \nmid \mathfrak{f}_\delta \text{ de } \mathcal{O}_K,$$

où l'on note encore $\pi_\mathfrak{p} \in \mathbf{A}_{K,\mathrm{f}}^\times$ l'idèle ayant composantes triviales en dehors de la place induite par $\mathfrak{p}$ et qui coïncide avec l'uniformisante $\pi_\mathfrak{p}$ choisie en cette place. Soit η la fonction définie pour $m \in \mathbf{Z}$ par

$$\eta(m) = \frac{\delta_{\mathrm{H}}\,(m\mathcal{O}_K)}{m^{k(\rho)-1}},$$

où l'on convient que $\delta_{\mathrm{H}}\,(m\mathcal{O}_K) = 0$ lorsque $m\mathcal{O}_K$ et $\mathfrak{f}_\delta$ ne sont pas premiers entre eux. Une vérification rapide montre que η induit un caractère de Dirichlet modulo $M = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)$ (voir le lemme 3.7 pour un résultat plus précis).

Soit enfin $\left(\frac{-D_K}{\cdot}\right)$ le symbole de Kronecker correspondant au corps K vu comme caractère de Dirichlet modulo D_K et posons $\varepsilon = \left(\frac{-D_K}{\cdot}\right)\eta$, vu comme caractère de Dirichlet modulo MD_K. Pour $z \in \mathbf{C}$, de partie imaginaire $\Im(z) > 0$, on pose alors

$$g_\delta(z) = \sum_{\substack{(\mathfrak{a},\mathfrak{f}_\delta)=1 \\ \mathfrak{a} \text{ entier}}} \delta_{\mathrm{H}}(\mathfrak{a}) q^{\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{a})} = \sum_{n\geq 1} c_n q^n, \quad \text{avec } q = e^{2i\pi z}.$$

Le résultat suivant est dû à Hecke et Shimura (voir [8, p. 717] ainsi que [20, Lemma 3] et [21, p. 138]).

Théorème 3.5 (Hecke, Shimura)**.** *La série g_δ est le développement de Fourier d'une newform de poids $k(\rho)$, niveau MD_K et caractère ε à multiplication complexe par le corps K.*

Dans la démonstration du théorème 1.1 ci-dessous, on note pour simplifier k à la place de $k(\rho)$. D'après la proposition 2.1, $\mathfrak{f}_\alpha$ et $\mathfrak{f}_\delta$ coïncident hors de v. En particulier, on a

$$N(\rho) = D_K^{(\ell)}\,\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)^{(\ell)} = (MD_K)^{(\ell)}. \tag{3.4}$$

On calcule à présent la valuation de MD_K en ℓ afin de déterminer l'entier MD_K lui-même. On procède suivant les différents cas de la proposition 3.2 dont on reprend la terminologie et la notation.

(1) On distingue deux cas :

(a) Supposons ℓ décomposé dans K. D'après la proposition 3.2, φ est modérément ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \chi^{k-1}(\tau)$. Il suit que $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 1$ car il en est ainsi pour $\widetilde{\chi}\circ\mathrm{rec}_K$. Par ailleurs, le complété K_v de K en v s'identifie à $\mathbf{Q}_\ell$ et d'après [16, proposition 8] le caractère fondamental $\theta_{\ell-1}$ de niveau 1 est le caractère cyclotomique χ. Soit $u \in \mathcal{O}_v^\times$. On pose $x = \overline{u} \in \mathbf{F}_\ell^\times$. Avec les notations des paragraphes 2.2 et 3.3, il découle de l'égalité (3.2) et de la compatibilité entre les théories du corps de classes locale et globale que l'on a

$$\alpha_v(u) = \widetilde{\varphi(\omega(x))} = \widetilde{\theta_{\ell-1}(\omega(x))}^{\,k-1} = \widetilde{x}^{1-k} = \widetilde{\overline{u}}^{1-k}.$$

D'après le point (2) de la proposition 2.1, on a donc $\mathrm{ord}_v(\mathfrak{f}_\delta) = 0$. D'où il vient $\mathrm{ord}_\ell(MD_K) = 0$ et $MD_K = N(\rho)$ d'après (3.4).

(b) Supposons ℓ ramifié dans K, donc $\ell \mid D_K$. D'après la proposition 3.2, φ est non ramifié en $\mathfrak{p}_v$ et $\ell = 2k-1$. On a $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 0$ et $\ell(= 2k-1) > k$. En particulier, on déduit du point 3 de la proposition 2.1 que l'on a $\mathrm{ord}_v(\mathfrak{f}_\delta) = 1$, puis $\mathrm{ord}_\ell(MD_K) = 2$ et $MD_K = \ell^2 N(\rho)$.

(2) D'après la proposition 3.2, ℓ est inerte ou ramifié dans K, φ est ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \psi_2^{k-1}(\tau)$, avec ψ_2 caractère fondamental de niveau 2. Par suite, φ est modérément ramifié et $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 1$. Quitte à remplacer φ par φ', on peut de plus supposer que l'on a l'égalité $\varphi = \theta_{\ell^2-1}^{k-1}$ entre caractères de $I_{\mathfrak{p}_v}$.

(a) Supposons ℓ inerte dans K. Dans ce cas, l'extension $K_v/\mathbf{Q}_\ell$ est quadratique non ramifiée. Soit $u \in \mathcal{O}_v^\times$. On pose $x = \overline{u} \in \mathbf{F}_{\ell^2}^\times$. D'après l'égalité (3.2), on a comme précédemment,

$$\alpha_v(u) = \varphi\widetilde{(\omega(x))} = \theta_{\ell^2-1}\widetilde{(\omega(x))}^{k-1} = \widetilde{x}^{1-k} = \widetilde{\overline{u}}^{1-k}.$$

D'après le point (2) de la proposition 2.1, on a donc $\mathrm{ord}_v(\mathfrak{f}_\delta) = 0$. D'où il vient $MD_K = N(\rho)$.

(b) Supposons enfin ℓ ramifié dans K. Dans ce cas, l'extension $K_v/\mathbf{Q}_\ell$ est quadratique ramifiée. Soit $u \in \mathcal{O}_v^\times$. On pose $x = \overline{u} \in \mathbf{F}_\ell^\times$. Comme le produit des caractères fondamentaux de niveau 2 est le caractère fondamental de niveau 1, on déduit comme ci-dessus des égalités $\ell = 2k-3$ et (3.2) que l'on a

$$\begin{aligned}\alpha_v(u)^2 = \varphi\widetilde{(\omega(x))}^2 = \theta_{\ell^2-1}^{2(k-1)}\widetilde{(\omega(x))} = \theta_{\ell^2-1}^{\ell+1}\widetilde{(\omega(x))} \\ = \theta_{\ell-1}\widetilde{(\omega(x))} = \widetilde{x}^{-1} = \widetilde{\overline{u}}^{-1}.\end{aligned}$$

Or, on a $\widetilde{\overline{u}}^{2(1-k)} = \widetilde{x}^{-(\ell+1)} = \widetilde{x}^{-2} = \widetilde{\overline{u}}^{-2}$, qui n'est pas égal à $\widetilde{\overline{u}}^{-1}$ dès lors que $\overline{u} \neq 1$: en particulier $\alpha_v(u) \neq \widetilde{\overline{u}}^{1-k}$ dès lors que $u \in \mathcal{O}_v^\times \setminus \mathcal{O}_v^{(1)}$. D'après le point (2) de la proposition 2.1, on a donc $\mathrm{ord}_v(\mathfrak{f}_\delta) = 1$. D'où il vient $\mathrm{ord}_\ell(MD_K) = 2$, puis $MD_K = \ell^2 N(\rho)$.

On a donc montré que l'on a

$$MD_K = \begin{cases} N(\rho) & \text{si } \ell \text{ est non ramifié dans } K\,; \\ \ell^2 N(\rho) & \text{si } \ell \text{ est ramifié dans } K. \end{cases} \tag{3.5}$$

Prouvons à présent que ρ provient bien de g_δ (par réduction modulo v) : pour ce faire, nous allons vérifier que pour tout nombre premier $q \nmid N(\rho)\ell$, le polynôme caractéristique de $\rho(\mathrm{Frob}_q)$ est la réduction (modulo v) de

$$X^2 - c_q X + \varepsilon(q) q^{k-1},$$

où Frob_q est un représentant de Frobenius en q dans $\mathrm{G}_{\mathbf{Q}}$.

Cas inerte: On suppose q inerte dans K, de sorte qu'on peut choisir $\sigma = \mathrm{Frob}_q \in \mathrm{G}_{\mathbf{Q}} \setminus \mathrm{G}_K$ au début du paragraphe 3.1. On pose $\mathfrak{q} = q\mathcal{O}_K$. On a d'une part les égalités $c_q = 0$ et $\varepsilon(q)q^{k-1} = -\delta_{\mathrm{H}}(\mathfrak{q})$. D'autre part, l'écriture (3.1) entraîne $\mathrm{tr}\,\rho(\mathrm{Frob}_q) = 0$ ainsi que $\det\rho(\mathrm{Frob}_q) = -\varphi(\mathrm{Frob}_q^2)$. La théorie du corps de classes locale et la proposition 2.1 donnent alors

$$\varphi\left(\mathrm{Frob}_q^2\right) = \overline{\alpha(\pi_{\mathfrak{q}})} = \overline{\delta(\pi_{\mathfrak{q}})} = \overline{\delta_{\mathrm{H}}(\mathfrak{q})}.$$

Cas décomposé: On suppose q décomposé dans K et on note $\mathfrak{q}, \mathfrak{q}'$ les idéaux premiers de $\mathcal{O}_K$ au-dessus de q. Alors $\mathrm{Frob}_q \in \mathrm{G}_K$ est une substitution de Frobenius en $\mathfrak{q}$ et en $\mathfrak{q}'$. On a, d'une part, $c_q = \delta_{\mathrm{H}}(\mathfrak{q}) + \delta_{\mathrm{H}}(\mathfrak{q}')$ et $\varepsilon(q)q^{k-1} = \delta_{\mathrm{H}}(\mathfrak{q}\mathfrak{q}')$. D'autre part, on a comme précedemment,

$$\begin{aligned}\mathrm{tr}\,\rho(\mathrm{Frob}_q) &= \varphi(\mathrm{Frob}_q) + \widehat{\varphi}(\mathrm{Frob}_q) = \overline{\alpha(\pi_{\mathfrak{q}})} + \overline{\alpha(\pi_{\mathfrak{q}'})}\\ &= \overline{\delta(\pi_{\mathfrak{q}})} + \overline{\delta(\pi_{\mathfrak{q}'})} = \overline{c_q}\end{aligned}$$

et

$$\begin{aligned}\det\rho(\mathrm{Frob}_q) &= \varphi(\mathrm{Frob}_q)\widehat{\varphi}(\mathrm{Frob}_q) = \overline{\alpha(\pi_{\mathfrak{q}})}\,\overline{\alpha(\pi_{\mathfrak{q}'})}\\ &= \overline{\delta(\pi_{\mathfrak{q}})}\,\overline{\delta(\pi_{\mathfrak{q}'})} = \overline{\delta_{\mathrm{H}}(\mathfrak{q}\mathfrak{q}')}.\end{aligned}$$

On en déduit le résultat voulu avec [6, lemme 3.2].

Pour terminer la démonstration du théorème 1.1, il reste à vérifier l'affirmation sur le caractère. Soit $\varepsilon(\rho)$ le caractère associé à ρ par Serre comme dans [18, n° 1.3] : par construction, il est égal à la réduction (modulo v) de ε. On fait l'hypothèse que $\varepsilon(\rho)$ est trivial, i.e. $\det\rho = \chi^{k-1}$ avec χ le caractère cyclotomique mod ℓ. On doit alors montrer qu'il existe une forme à multiplication complexe vérifiant les conditions du théorème et dont le caractère est trivial. Pour cela, on va considérer une tordue de g_δ par un caractère de Dirichlet particulier. On a la décomposition suivante de l'entier M :

$$M = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta) = \prod_{\mathfrak{p}} \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)} = \prod_p p^{\sum_{\mathfrak{p}|p} f_{\mathfrak{p}/p}\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)},$$

où $f_{\mathfrak{p}/p}$ désigne le degré résiduel de l'idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus du premier p.

Lemme 3.6. *Lorsque* $\det\rho = \chi^{k-1}$ *la valuation* $\mathrm{ord}_p(M)$ *de* M *en tout nombre premier* p *ne divisant pas* D_K *est paire, égale à* $2\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$ *où* $\mathfrak{p}$ *est un premier de* $\mathcal{O}_K$ *au-dessus de* p.

Démonstration. Soit p ne divisant pas D_K tel que $\mathrm{ord}_p(M) > 0$. Lorsque p est inerte dans K, avec $p\mathcal{O}_K = \mathfrak{p}$, le résultat est immédiat car alors $\mathrm{ord}_p(M) = 2\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$. On suppose donc à présent p décomposé dans K, disons $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. On note que p est nécessairement différent de ℓ car lorsque ℓ est décomposé dans K, alors, grâce à (3.5), on a $MD_K = N(\rho)$ qui est premier à ℓ. D'après (3.3) et la proposition 2.1 on a $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{N}(\varphi))$, et de même pour $\bar{\mathfrak{p}}$. Soit $I_{\mathfrak{p}}$ un groupe d'inertie en $\mathfrak{p}$ dans G_K. D'après l'hypothèse $\det\rho = \chi^{k-1}$ et avec les notations du paragraphe 3.1, on a $\varphi_{|I_{\mathfrak{p}}} = \widehat{\varphi}^{-1}_{|I_{\mathfrak{p}}}$ parce que $\chi_{|I_{\mathfrak{p}}} = 1$. D'où il vient

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{N}(\varphi)) = \mathrm{ord}_{\mathfrak{p}}\left(\mathfrak{N}\left(\widehat{\varphi}^{-1}\right)\right) = \mathrm{ord}_{\mathfrak{p}}\left(\mathfrak{N}\left(\widehat{\varphi}\right)\right) = \mathrm{ord}_{\bar{\mathfrak{p}}}\left(\mathfrak{N}\left(\varphi\right)\right)$$

puis $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta) = \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{f}_\delta)$ et $\mathrm{ord}_p(M) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta) + \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{f}_\delta) = 2\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$. □

On pose alors

$$M' = \prod_{p\nmid D_K} p^{\mathrm{ord}_p(M)/2} \times \prod_{p\mid D_K} p^{x_p},$$

où pour tout nombre premier p divisant D_K, on définit

$$x_p = \begin{cases} \mathrm{ord}_p(M)/2 & \text{si } \mathrm{ord}_p(M) \text{ est pair;} \\ (\mathrm{ord}_p(M)+1)/2 & \text{si } \mathrm{ord}_p(M) \text{ est impair.} \end{cases}$$

D'après le lemme précédent, M' est un entier naturel divisant M qui vérifie $\mathrm{ord}_{\mathfrak{p}}(M') \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$ pour tout $\mathfrak{p} \mid \mathfrak{f}_\delta$: cela suit du lemme 3.6 pour les $\mathfrak{p}$ premiers à D_K, et pour ceux qui divisent D_K du calcul $\mathrm{ord}_{\mathfrak{p}}(M') = 2\,\mathrm{ord}_p(M') \geq \mathrm{ord}_p(M) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$, où on a noté $p = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p})$.

Lemme 3.7. *Le caractère ε se factorise modulo M'.*

Démonstration. On reprend les notations du début de ce paragraphe et on commence par comparer $m^{k-1}\eta(m)$ avec $\delta_{\mathrm{f}}(m) = m^{k-1}$ pour un entier $m \equiv 1 \pmod{M'}$. Comme M' et M ont les mêmes diviseurs premiers, on a en particulier $\mathrm{pgcd}(m, M) = 1$. On remarque tout d'abord que la formule

$$\delta_{\mathrm{H}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} = \delta(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)}$$

est valable pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. En effet, lorsque $\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K) = 0$, elle est triviale et lorsque $\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K) > 0$, cela résulte du fait que cela entraîne $\mathfrak{p} \nmid M = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)$ et par suite la formule n'est autre chose que la définition de δ_{H}. Ainsi, on a

$$m^{k-1}\eta(m) = \delta_{\mathrm{H}}(m\mathcal{O}_K) = \prod_{\mathfrak{p}} \delta_{\mathrm{H}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} = \prod_{\mathfrak{p}} \delta(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)}$$

et grâce à $m^{k-1} = \delta_{\mathrm{f}}(m) = \prod_{\mathfrak{p}\mid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m)$

$$\begin{aligned} m^{k-1} &= \prod_{\mathfrak{p}\mid m\mathcal{O}_K} \delta_{\mathfrak{p}}(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) \\ &= \prod_{\mathfrak{p}} \delta_{\mathfrak{p}}(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) = m^{k-1}\eta(m) \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m). \end{aligned}$$

Notons $P(m) = \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) = \eta(m)^{-1}$ le produit apparaissant à la dernière ligne de la formule ci-dessus. Tout d'abord, on remarque que l'on a

$P(m) = \prod_{\mathfrak{p}|\mathfrak{f}_\delta} \delta_\mathfrak{p}(m)$ car d'une part $\mathrm{pgcd}(\mathfrak{f}_\delta, m\mathcal{O}_K) = 1$ et d'autre part, si $\mathfrak{p} \nmid m\mathcal{O}_K$ et $\mathfrak{p} \nmid \mathfrak{f}_\delta$, alors $m \in \mathcal{O}_\mathfrak{p}^\times$, puis $\delta_\mathfrak{p}(m) = 1$. Comme pour tout $\mathfrak{p} \mid \mathfrak{f}_\delta$ on a $\mathrm{ord}_\mathfrak{p}(m-1) \geq \mathrm{ord}_\mathfrak{p}(M') \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{f}_\delta)$, par définition du conducteur d'un Größencharakter, on en déduit $P(m) = 1$, puis $\eta(m) = 1$. Maintenant on remarque que l'on a

$$\varepsilon(m) = \eta(m)\left(\frac{-D_K}{m}\right) = \left(\frac{-D_K}{m}\right) = \pm 1$$

car η se factorise modulo M'. Or, $\varepsilon(m)$ se réduit sur 1 modulo ℓ par hypothèse. On a donc $\varepsilon(m) = 1$ et le résultat voulu. $\square$

Le caractère ε, se réduisant sur le caractère trivial, est nécessairement d'ordre une puissance de ℓ, disons ℓ^h. On pose alors $\mu = \varepsilon^{(\ell^h-1)/2}$. C'est un caractère de même ordre et de même conducteur que ε vérifiant $\mu^2 = \varepsilon^{-1}$. Pour $z \in \mathbf{C}$, de partie imaginaire $\Im(z) > 0$, on pose alors

$$g^\dagger(z) = (g_\delta \otimes \mu)(z) = \sum_{n\geq 1} \mu(n) c_n q^n, \quad \text{avec } q = e^{2i\pi z}.$$

D'après [19, Proposition 3.64], $g^\dagger$ est le développement de Fourier d'une forme propre de poids k, de caractère $\varepsilon\mu^2 = 1$ et de niveau $\mathrm{ppcm}(MD_K, r^2)$ où r est le conducteur de ε (ou de μ). Or, on vérifie que M'^2 divise le produit MD_K. Ainsi, $\mathrm{ppcm}(MD_K, r^2) = MD_K$ d'après le lemme 3.7. Soit g la newform associée à $g^\dagger$. Alors, g est de niveau divisant MD_K et à multiplication complexe par K. Comme μ se réduit sur le caractère trivial, la réduction de la représentation v-adique associée à g est isomorphe à celle de g_δ, puis à ρ. Ceci achève la démonstration du théorème 1.1.

4. Exemples numériques

Pour l'exemple ci-dessous nous avons utilisé le logiciel PARI/GP ([25]).

4.1. Soit $\Delta = \sum_{n\geq 1} \tau(n) q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots$ l'unique forme parabolique normalisée de poids 12 et de niveau 1. On note

$$\rho_{\Delta,23} : \mathrm{G}_\mathbf{Q} \longrightarrow \mathrm{GL}_2(\mathbf{F}_{23})$$

l'unique représentation semi-simple non ramifiée hors de 23 telle que

$$\det \rho_{\Delta,23}(\mathrm{Frob}_p) = \tau(p) \pmod{23} \quad \text{et} \quad \mathrm{tr}\, \rho_{\Delta,23}(\mathrm{Frob}_p) = p^{11} \pmod{23}$$

pour tout nombre premier $p \neq 23$. Elle est de poids $k(\rho_{\Delta,23}) = 12$ et de conducteur $N(\rho_{\Delta,23}) = 1$.

Il résulte des congruences de Wilton ([29, p. 2]) que la représentation $\rho_{\Delta,23}$ est diédrale. Soit, plus explicitement, H le corps de classes de Hilbert de $K = \mathbf{Q}(\sqrt{-23})$. C'est une extension de degré 6 de $\mathbf{Q}$ de groupe de Galois D_3. Alors, $\rho_{\Delta,23}$ est isomorphe à la représentation

$$\mathrm{G}_\mathbf{Q} \longrightarrow \mathrm{Gal}(H/\mathbf{Q}) \simeq D_3 \xrightarrow{\sigma} \mathrm{GL}_2(\mathbf{Z}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_{23}),$$

où $\sigma : D_3 \to \mathrm{GL}_2(\mathbf{Z})$ est l'unique représentation irréductible de degré 2 du groupe D_3 (voir [15, §3.4]) et où la dernière flèche est l'application de réduction modulo 23.

On explicite à présent la forme à multiplication complexe dont l'existence est garantie par le théorème 1.1. Soit δ un Größencharakter de K de type à l'infini $(11, 0)$ et conducteur $\sqrt{-23}\mathcal{O}_K$ tel que, avec les notations du paragraphe 3.4, $\eta = \left(\frac{-23}{\cdot}\right)$. La newform g_δ associée à δ est alors de poids 12, niveau 23^2, caractère trivial et de corps des coefficients l'extension totalement réelle L de degré 3 de $\mathbf{Q}$ engendrée par une racine α du polynôme $X^3 - 6X - 3$ (pour les détails, voir le fichier `DeltaMod23.gp`, disponible sur le site de la revue [1]). On a

$$g_\delta = \sum_{n \geq 1} c_n q^n = q + (-21\alpha^2 - 4\alpha + 84)q^2 + (53\alpha^2 + 251\alpha - 212)q^3 + \cdots$$

On pose

$$\Delta^\dagger = \sum_{\substack{n \geq 1 \\ 23 \nmid n}} \tau(n) q^n = \sum_{n \geq 1} \tau'(n) q^n$$

de sorte que $\Delta^\dagger(z) = \Delta(z) - U_{23}(\Delta)(23z)$ où U_{23} est l'opérateur de Hecke en 23 agissant sur les formes de poids 12 et de niveau divisible par 23. Ainsi, $\Delta^\dagger$ et g_δ sont des formes normalisées de poids 12, niveau 23^2 et caractère trivial qui sont propres pour l'algèbre de Hecke engendrée par les opérateurs $\{T_p,\ p \text{ premier},\ p \neq 23\}$.

Soit $\lambda_{23} = (\alpha - 5)\mathcal{O}_L$ l'unique idéal premier de l'anneau $\mathcal{O}_L$ des entiers de L ramifié au-dessus de 23. Vérifions que l'on a

$$\tau'(n) \equiv c_n \pmod{\lambda_{23}}, \quad \text{pour tout entier } n \leq m,$$

où $m = \left[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0\left(23^2\right)\right] = 552$. Pour les entiers n divisibles par 23, cela résulte immédiatement des égalités $\tau'(n) = 0$ et $c_n = 0$. Lorsque $23 \nmid n$, on se ramène par multiplicativité des coefficients de Fourier au cas où n est premier et on utilise la commande `CoefficientFormeCM` du fichier `DeltaMod23.gp` (l'ensemble des calculs prend quelques secondes sur un ordinateur de bureau). D'après [22, Theorem 1], il vient donc $\tau'(n) \equiv c_n \pmod{\lambda_{23}}$, pour tout entier $n \geq 1$, puis

$$\tau(p) \equiv c_p \pmod{\lambda_{23}}, \quad \text{pour tout nombre premier } p \neq 23.$$

On conclut avec [6, lemme 3.2] que $\rho_{\Delta,23}$ est isomorphe à la réduction modulo λ_{23} de la représentation galoisienne 23-adique associée à g_δ. En particulier, comme l'affirme le théorème 1.1, $\rho_{\Delta,23}$ provient bien d'une forme à multiplication complexe de poids $k(\rho_{\Delta,23}) = 12$ et de niveau $N' = 23^2 N(\rho_{\Delta,23}) = 23^2$.

Remarque 4.1. On constate ici que le niveau 23^2 est optimal. En effet, il n'existe pas de forme à multiplication complexe de poids 12 et de niveau 1 ou 23 congrue à Δ modulo 23.

4.2. Le corollaire 1.3 s'applique également à la représentation modulo 7 attachée à la courbe elliptique d'équation

$$Y^2 + Y = X^3 - X^2 - 18507X - 989382$$

notée 65533.a1 dans LMFDB ([24]). La détermination de la forme à multiplication complexe (de niveau 71^2) dont l'existence est garantie par le corollaire 1.3 s'effectue par une méthode analogue à celle utilisée précédemment. Les détails sont accessibles dans le fichier `EMod7.gp` (disponible sur le site de la revue [1]).

Bibliographie

[1] N. Billerey & F. A. E. Nuccio, « Représentations galoisiennes diédrales et formes à multiplication complexe », *J. Théor. Nombres Bordx* **30** (2018), nº 2, p. 651-670, http://jtnb.cedram.org/jtnb-bin/fitem?id=JTNB_2018__30_2_651_0.

[2] D. M. Bloom, « The subgroups of $\mathrm{PSL}(3, q)$ for odd q », *Trans. Am. Math. Soc.* **127** (1967), p. 150-178.

[3] H. Carayol, « Sur les représentations l-adiques associées aux formes modulaires de Hilbert », *Ann. Sci. Éc. Norm. Supér.* **19** (1986), nº 3, p. 409-468.

[4] ———, « Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires », *Duke Math. J.* **59** (1989), nº 3, p. 785-801.

[5] I. Chen, « Surjectivity of mod ℓ representations attached to elliptic curves and congruence primes », *Can. Math. Bull.* **45** (2002), nº 3, p. 337-348.

[6] P. Deligne & J.-P. Serre, « Formes modulaires de poids 1 », *Ann. Sci. Éc. Norm. Supér.* **7** (1974), p. 507-530.

[7] E. Ghate & P. Parent, « On uniform large Galois images for modular abelian varieties », *Bull. Lond. Math. Soc.* **44** (2012), nº 6, p. 1169-1181.

[8] E. Hecke, *Mathematische Werke*, Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen, Vandenhoeck & Ruprecht, 1959, 955 pages.

[9] S. Lang, *Introduction to modular forms*, Grundlehren der Mathematischen Wissenschaften, vol. 222, Springer, 1976, ix+261 pages.

[10] J. Nualart, « Minimal lifts of dihedral 2-dimensional Galois representations », *Bull. Braz. Math. Soc. (N.S.)* **42** (2011), nº 3, p. 359-371.

[11] M. Raynaud, « Schémas en groupes de type $(p, \ldots, p)$ », *Bull. Soc. Math. Fr.* **102** (1974), p. 241-280.

[12] K. A. Ribet, « Galois action on division points of Abelian varieties with real multiplications », *Am. J. Math.* **98** (1976), nº 3, p. 751-804.

[13] ———, « Abelian varieties over $\mathbf{Q}$ and modular forms », in *Algebra and topology 1992 (Taejŏn)*, Korea Advanced Institute of Science and Technology, Mathematics Research Center, 1992, p. 53-79.

[14] J.-P. Serre, *Corps locaux*, 2ème éd., Publications de l'Institut de Mathématique de l'Université de Nancago, vol. 8, Hermann, 1968, 243 pages.

[15] ———, « Une interprétation des congruences relatives à la fonction τ de Ramanujan », in *Séminaire Delange-Pisot-Poitou : 1967/68*, Théorie des Nombres, vol. 1, Faculté des Sciences de Paris. Secrétariat Mathématique, 1969, Exp. 14, 17 p.

[16] ———, « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », *Invent. Math.* **15** (1972), nº 4, p. 259-331.

[17] ———, *Représentations linéaires des groupes finis*, Hermann, 1978, 184 pages.

[18] ———, « Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) », *Duke Math. J.* **54** (1987), n° 1, p. 179-230.

[19] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Iwanami Shoten ; Princeton University Press, 1971, xiii+267 pages.

[20] ———, « On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields », *Nagoya Math. J.* **43** (1971), p. 199-208.

[21] ———, « Class fields over real quadratic fields and Hecke operators », *Ann. Math.* **95** (1972), p. 130-190.

[22] J. Sturm, « On the congruence of modular forms », in *Number theory (New York, 1984-85)*, Lecture Notes in Mathematics, vol. 1240, Springer, 1984, p. 1984-1985.

[23] Y. Taguchi, « Induction formula for the Artin conductors of mod ℓ Galois representations », *Proc. Am. Math. Soc.* **130** (2002), n° 10, p. 2865-2869.

[24] The LMFDB Collaboration, « The L-functions and Modular Forms Database », 2013, http://www.lmfdb.org.

[25] The PARI Group, « PARI/GP version 2.9.2 », 2014, available from http://pari.math.u-bordeaux.fr/.

[26] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer, 1997, xiv+487 pages.

[27] A. Weil, « On a certain type of characters of the idèle-class group of an algebraic number-field », in *Proceedings of the international symposium on algebraic number theory (Tokyo & Nikko, 1955)*, Science Council of Japan, 1956, p. 1-7.

[28] G. Wiese, « Dihedral Galois representations and Katz modular forms », *Doc. Math.* **9** (2004), p. 123-133.

[29] J. R. Wilton, « Congruence Properties of Ramanujan's Function tau(n) », *Proc. Lond. Math. Soc.* **31** (1930), n° 1, p. 1-10.

Nicolas Billerey
Université Clermont Auvergne
LMBP UMR 6620 – CNRS
Campus des Cézeaux
3, place Vasarely
F-63178 Aubière, France
E-mail: nicolas.billerey@uca.fr
URL: http://math.univ-bpclermont.fr/~billerey/

Filippo A. E. Nuccio Mortarino Majno di Capriglio
Université de Lyon
Institut Camille Jordan
UMR 5208 – CNRS
Université Jean Monnet
23, rue du Docteur Paul Michelon
F-42023 Saint-Étienne, France
E-mail: filippo.nuccio@univ-st-etienne.fr
URL: http://perso.univ-st-etienne.fr/nf51454h/