UNE REPRÉSENTATION GALOISIENNE UNIVERSELLE ATTACHÉE AUX FORMES MODULAIRES MODULO 2

JOËL BELLAÏCHE

Résumé : Soit A l'algèbre des opérateurs de Hecke agissant sur les formes modulaires paraboliques modulo 2 de niveau 1 et de tous poids. Nicolas et Serre ont déterminé la structure de A : on a $A \simeq \mathbb{F}_2[[x,y]]$. Soit $G_{\mathbb{Q},2}$ le groupe de Galois de l'extension maximale de $\mathbb{Q}$ non-ramifiée hors de 2 et l'infini, et G son plus grand pro-2-quotient. On construit une représentation galoisienne continue $r : G \to \mathrm{SL}_2(A)$ telle que $\mathrm{tr}\, r(\mathrm{Frob}_p) = T_p$ pour tout p premier impair. On montre aussi son unicité et on étudie ses propriétés de réductibilité.

English Title : A universal Galois representation attached to modular forms modulo 2.

Abstract : Let A be the algebra of Hecke operators acting on mod 2 cusp forms of level 1 and any weight. Nicolas and Serre have determined the structure of A : one has $A \simeq \mathbb{F}_2[[x,y]]$. Let $G_{\mathbb{Q},2}$ be the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside 2 and ∞, and let G be its maximal pro-2-quotient. One constructs a continuous Galois representation $r : G \to \mathrm{SL}_2(A)$ such that $\mathrm{tr}\, r(\mathrm{Frob}_p) = T_p$ for all odd prime p. One also proves its uniqueness and one studies its irreducibility properties.

Abridged english version. Let $\Delta = \sum_{n=0}^{\infty} q^{(2n+1)^2} \in \mathbb{F}_2[[q]]$ be the reduction modulo 2 of the classical Δ function, and let $\mathcal{F}(n)$ be the space generated by $\Delta, \Delta^3, \ldots, \Delta^{2n-1}$. Let $A(n)$ be the algebra generated by the actions of Hecke operators T_p (for p odd prime) on $\mathcal{F}(n)$, and $A = \varprojlim A(n)$. Nicolas and Serre have proved ([5]) the existence of an isomorphism $\mathbb{F}_2[[x,y]] \simeq A$ sending x to T_3 and y to T_5, and Serre has asked whether there existed a continuous Galois representation $r : G \to \mathrm{GL}_2(A)$ such that $\mathrm{tr}\,(\mathrm{Frob}_p) = T_p$.

Theorem 1. *There exists a unique such representation r and its determinant is 1.*

The main tool in the proof of the existence is the notion of determinant, a generalization of the notion of pseudo-character, due to Chenevier ([2]). The uniqueness is equivalent to the first assertion (which is due to Serre) of (iii) of Theorem 2 below,

Theorem 2. *(i) The representation $r : G \to \mathrm{GL}_2(\mathrm{Frac}(A))$ is absolutely irreducible.*

(ii) The residual representation $\bar{r} : G \to \mathrm{GL}_2(\mathbb{F}_2)$ *is the extension of the trivial character by itself corresponding to* $\mathbb{Q}(\sqrt{2})$.

(iii) If $\mathfrak{p}$ *is a prime ideal of* A *of height one, calling* $k(\mathfrak{p})$ *the fraction field of* $A/\mathfrak{p}$*, the representation* $r_{\mathfrak{p}} : G \to \mathrm{GL}_2(k(\mathfrak{p}))$ *deduced from* r *is irreducible for every* $\mathfrak{p}$ *and absolutely irreducible for every* $\mathfrak{p}$ *except for one prime* $\mathfrak{p} = \mathfrak{p}_0$*, described in (1) below, in which case it is irreducible but becomes reducible after a quadratic ramified extension of the field of coefficients* $k(\mathfrak{p}_0) = \mathbb{F}_2((x))$*. Moreover, when* $\mathfrak{p} \neq \mathfrak{p}_0$*,* $r_{\mathfrak{p}}$ *remains absolutely irreducible after replacing* G *by any open subgroup, except in the two cases* $\mathfrak{p} = (x)$ *and* $\mathfrak{p} = (y)$ *; in those cases the image of* $r_{\mathfrak{p}}$ *is dihedral.*

Finally, one also proves that the T_p's are algebraically independent over $\mathbb{F}_2$ in A.

1. Énoncé des résultats

Le but de cette note est de répondre à une question que Serre avait posée lors d'un séminaire à Harvard sur ses travaux avec Nicolas ([4], [5]) concernant l'algèbre de Hecke des formes modulaires de niveau 1 modulo 2, et de donner la preuve de quelques résultats connexes. Cette note fait donc suite à [4] et [5], dont nous reprenons les notations :

On pose $\Delta = \sum_{n=0}^{\infty} q^{(2n+1)^2} \in \mathbb{F}_2[[q]]$: c'est la réduction modulo 2 de la fonction classique Δ. On note $\mathcal{F}(n)$ l'espace engendré par $\Delta, \Delta^3, \ldots, \Delta^{2n-1}$. Les opérateurs de Hecke T_p agissent sur les espaces $\mathcal{F}(n)$. On note $A(n)$ la sous-algèbre de $\mathrm{End}_{\mathbb{F}_2}(\mathcal{F}(n))$ engendrée par les T_p pour p impair, et $A = \varprojlim A(n)$. Nicolas et Serre ont montré l'existence d'un isomorphisme (évidemment unique) d'algèbres $\psi : \mathbb{F}_2[[x, y]] \to A$ tel que $\psi(x) = T_3$ et $\psi(y) = T_5$ (cf. [5]). Nous l'utiliserons pour identifier $\mathbb{F}_2[[x, y]]$ et A.

Soit $G_{\mathbb{Q},2}$ le groupe de Galois de l'extension maximale de $\mathbb{Q}$ non ramifiée hors de 2 et l'infini, et G le plus grand quotient de $G_{\mathbb{Q},2}$ qui est un pro-2-groupe. Serre a posé la question suivante : *existe-t-il une représentation continue* $r : G \to \mathrm{GL}_2(A)$ *telle que pour tout* p *premier impair, on ait* $\mathrm{tr}\, r(\mathrm{Frob}_p) = T_p$ *? Si oui, peut-on choisir son déterminant égal à* 1 *?*

Théorème 1. *Il existe une unique représentation continue* $r : G \to \mathrm{GL}_2(A)$ *telle que* $\mathrm{tr}\, r(\mathrm{Frob}_p) = T_p$ *pour tout* p *premier impair. Son déterminant est* 1.

On prouvera d'abord l'existence, et le fait que toute telle représentation est de déterminant 1, dans le §2 : c'est la réponse à la question de Serre. L'unicité est équivalente au point (3) du théorème 2 ci-dessous, qui sera prouvé au §3.

Pour $\mathfrak{p}$ un idéal premier de A, on note $k(\mathfrak{p})$ le corps des fractions de $A/\mathfrak{p}$. La représentation r définit naturellement des représentations $r_{\mathfrak{p}} : G \to \mathrm{GL}_2(k(\mathfrak{p}))$. Quand $\mathfrak{p}$ est l'idéal maximal (x, y), on a $k(\mathfrak{p}) = \mathbb{F}_2$ et on note simplement $\bar{r} : G \to \mathrm{GL}_2(\mathbb{F}_p)$ la représentation $r_{(x,y)}$; quand $\mathfrak{p}$

est l'idéal nul, $k_{(0)}$ est le corps des fractions $K = \mathbb{F}_2((x,y))$ de A, et nous noterons simplement $r : G \to \mathrm{GL}_2(K)$ la représentation $r_{(0)}$.

Théorème 2.

(i) *Cas $\mathfrak{p} = (0)$: la représentation $r : G \to \mathrm{GL}_2(K)$ est absolument irréductible.*

(ii) *Cas $\mathfrak{p} = (x,y)$: la représentation résiduelle $\bar{r} : G \to \mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe à la représentation $g \mapsto \begin{pmatrix} 1 & \eta(g) \\ 0 & 1 \end{pmatrix}$ où $\eta : G \to \mathbb{F}_2$ est l'homomorphisme correspondant à l'extension $\mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$.*

(iii) *Cas $\mathfrak{p}$ de hauteur un : la représentation $r_{\mathfrak{p}}$ est irréductible.*

Le théorème suivant précise le point (iii). Pour $a \in \mathbb{Z}_2$, soit $\tau_a(x) \in \mathbb{F}_2[[x]]$ l'unique série formelle satisfaisant la propriété suivante : pour toute $\mathbb{F}_2$-algèbre locale complète B d'idéal maximal m, et tout $u \in m$, on a $(1+u)^a + (1+u)^{-a} = \tau_a((1+u) + (1+u)^{-1})$. On a $\tau_{\log_2(5)/\log_2(-3)}(x) = x + x^3 + x^5 + x^9 + x^{11} + x^{129} + \cdots \in A$, où $\log_2 : 1 + 4\mathbb{Z}_2 \to \mathbb{Z}_2$ est le logarithme 2-adique, et on pose

$$\mathfrak{p}_0 = (y + \tau_{\log_2(5)/\log_2(-3)}(x)) = (y + x + x^3 + x^5 + x^9 + x^{11} + x^{129} + \dots). \tag{1}$$

L'idéal $\mathfrak{p}_0$ de A est premier, de hauteur 1.

Théorème 3. *Soit $\mathfrak{p}$ un idéal premier de hauteur 1 de A.*

(i) Si $\mathfrak{p}$ est l'idéal $\mathfrak{p}_0$, $r_{\mathfrak{p}}$ n'est pas absolument irréductible. Cette représentation devient réductible sur une extension quadratique ramifiée de $k(\mathfrak{p}_0)$.

(ii) Si $\mathfrak{p} = (x)$ ou $\mathfrak{p} = (y)$, les deux représentations $r_{\mathfrak{p}}$ sont absolument irréductibles, et les images de $r_{\mathfrak{p}}$ sont isomorphes à un groupe diédral D, produit semi-direct de $\mathbb{Z}/2$ par $\mathbb{Z}_2$.

(iii) Dans tous les autres cas, $r_{\mathfrak{p}}$ est fortement absolument irréductible (i.e. la restriction de $r_{\mathfrak{p}}$ à tous les sous-groupes d'indice fini de G est absolument irréductible).

Le théorème suivant répond à une question posée dans [5].

Théorème 4. *Les éléments T_p (pour $p > 2$ premier) de A sont algébriquement indépendants sur $\mathbb{F}_2$.*

Remerciements : Je tiens à remercier Jean-Pierre Serre, pour avoir posé la question qui est à l'origine de ce travail, puis d'autres qui ont inspiré certains énoncés ; pour m'avoir donné l'argument sur l'absolue irréductibilité en codimension 1 de r, m'en avoir suggéré d'autres, et m'avoir permis de les utiliser ici ; pour m'avoir, avec Jean-Louis Nicolas que je remercie également, donné une version préliminaire de leurs notes [4] et [5] ; et finalement pour ses encouragements lors de ce travail. Je tiens aussi à remercier Mark Kisin et Barry Mazur avec qui j'ai eu de très nombreuses discussions concernant sur le sujet de cet article, Gaëtan Chenevier

qui a répondu à mes questions sur les déterminants, et Paul Monsky dont les exposés à Brandeis ont développé mon goût pour les séries formelles en caractéristique 2.

2. Preuve de l'existence de la représentation r

La preuve de l'existence de r repose sur la théorie des déterminants de Chenevier (cf. [2]) qui généralise à toutes caractéristiques les théories antérieures des pseudo-représentations et pseudo-caractères de Wiles, Taylor et Rouquier. Rappelons (loc. cit. [2, Exemple 1.8]) qu'un déterminant de Chenevier de dimension 2 d'un groupe G dans un anneau commutatif S est la donnée de deux applications $t : G \to S$, $d : G \to S^*$ satisfaisant certaines relations algébriques pour lesquelles nous renvoyons à *loc. cit.*. Si G est un groupe topologique et S un anneau topologique, et si t et d sont continues, on dira que le déterminant de Chenevier (t, d) est continu. Si $r : G \to \mathrm{GL}_2(S)$ est une représentation, $(\mathrm{tr}\, r, \det r)$ est un déterminant de Chenevier.

Première étape : *il existe un unique déterminant de Chenevier continu (t, d) de G dans A tel que $t(\mathrm{Frob}_p) = T_p$ pour tout nombre premier impair p. On a $d = 1$.*

Soit $n \geq 1$ un entier, et $k = 12(2n-1)$. Soit $S_k(\mathbb{Z}_2)$ l'espace des formes modulaires paraboliques à coefficients dans $\mathbb{Z}_2$ de niveau 1 et de poids k, et $\mathbb{T}_k$ la sous-algèbre de $\mathrm{End}_{\mathbb{Z}_2}(S_k(\mathbb{Z}_2))$ engendré par les T_p, $p > 2$. Soit L une extension finie de $\mathbb{Q}_2$ contenant les coefficients des formes paraboliques propres normalisées f de poids k et de niveau 1. Notons N_k l'ensemble de ces formes. Soit $\psi : \mathbb{T}_k \to \prod_{f \in N_k} L$ le morphisme de $\mathbb{Z}_2$-algèbres qui envoie T_p sur $(a_p(f))_{f \in N_k}$ où $a_p(f)$ est le p-ième coefficient de f. Ce morphisme est injectif car les formes propres forment une base de $S_k(L)$. Pour $f \in N_k$, le théorème de Deligne fournit une représentation continue $\rho_f : G_{\mathbb{Q},2} \to \mathrm{GL}_2(L)$ satisfaisant les relations d'Eichler-Shimura, et qui se factorise d'ailleurs par G puisque la représentation résiduelle de ρ_f (pour n'importe quel réseau stable) est une extension du caractère trivial par lui-même, donc d'image d'ordre 1 ou 2. On obtient donc une représentation continue $\rho = (\rho_f)_{f \in N_f} : G \to \mathrm{GL}_2(\prod_{f \in N_k} L)$ dont la trace t_ρ envoie Frob_p sur $(a_p(f))_{f \in N_k}$, i.e. sur $\psi(T_p)$, et le déterminant d_ρ envoie Frob_p sur p^{k-1}. Par [2, Corollary 1.14], on en déduit que le déterminant de Chenevier continu (t_ρ, d_ρ) dans $\prod_{f \in N_k} L$ provient par extension des scalaires d'un déterminant de Chenevier (t_ρ, d_ρ) de G dans $\mathbb{T}_k$, évidemment continu.

Par ailleurs, $\mathcal{F}(n)$ est un sous espace stable par les opérateurs de Hecke de $S_k(\mathbb{Z}_2) \otimes \mathbb{F}_2$ (qu'on voit comme un sous-espace de $\mathbb{F}_2[[q]]$ par l'application "développement de Fourier"). On dispose donc d'un morphisme naturel surjectif $\mathbb{T}_k \otimes \mathbb{F}_2 \to A(n)$ (envoyant $T_p \in \mathbb{T}_k$ sur $T_p \in A(n)$), continu si $A(n)$ est muni de la topologie discrète, et la composition de (t_ρ, d_ρ) avec ce morphisme fournit un déterminant de Chenevier continu (t_n, d_n) de G sur $A(n)$. On a $d_n = 1$ puisque p^{k-1} est impair pour $p \geq 3$, et $t_n(\mathrm{Frob}_p) = T_p$ par construction. Les déterminants (t_n, d_n) pour

$n = 1, 2, 3, \ldots$ sont donc compatibles et fournissent un déterminant de Chenevier continu (t, d) de G dans A satisfaisant les conditions requises, ce qui prouve l'assertion d'existence.

La condition de continuité et la densité des éléments de Frobenius montrent l'unicité de la fonction t satisfaisant les conditions requises ; comme un déterminant de Chenevier (t, d) à valeurs dans un anneau intègre est déterminé par t pour peu que $t \neq 0$ (cela résulte de la formule (ii) de [2, Exemple 1.8]), on obtient l'unicité de (t, d).

Deuxième étape : *Soit $\bar{K}$ une clôture algébrique de $K = \mathrm{Frac}(A)$. Il existe une représentation irréductible $r : G \to \mathrm{GL}_2(\bar{K})$ dont la trace est t et le déterminant* 1.

L'existence de r découle immédiatement de [2, Theorem 2.12]. Si r était réductible, l'application $t : G \to A$ serait la somme de deux caractères $G \to \bar{K}^*$, et serait donc constante sur les classes à gauche sous le groupe dérivé (algébrique) $D(G)$. Comme t est continue, elle serait aussi constante sur les classes à gauche sous $\overline{D}(G)$, autrement dit elle se factoriserait par l'abélianisé G^{ab} de G, et il en serait de même des applications composées $t_n : G \to A \to A(n) \to \mathrm{End}_{\mathbb{F}_2}\mathcal{F}(n)$ pour tout n. Par le théorème de Kronecker-Weber, cela signifierait que l'endomorphisme $t_n(\mathrm{Frob}_p) = T_p$ de $\mathcal{F}(n)$ ne dépendrait de p que par l'intermédiaire du résidu de p modulo N pour un certain entier N (dépendant de n). Faisons $n = 5$, si bien que $\Delta^9 \in \mathcal{F}(n)$. Pour $p \equiv 1 \pmod 8$, on voit (cf [4]) que $T_p\Delta^9 = c(p)\Delta$ avec $c(p) = 1$ si p ne s'écrit pas $a^2 + 32b^2$ avec a, b entiers, $c(p) = 0$ sinon. Comme 32 n'est pas un nombre idonéal, cette condition sur p ne dépend pas que du résidu de p modulo un entier (cf. [3, Corollary 34]). Cette contradiction prouve l'irréductibilité de r.

Troisième étape : *La représentation r est définie sur K.*

Si elle ne l'était pas, il existerait un corps de quaternions H sur K tel que $r(G) \subset H^* \subset \mathrm{GL}_2(\bar{K})$. Pour c la conjugaison complexe dans G, on aurait alors $r(c^2) = 1$, donc $(r(c) - 1)^2 = 0$ et comme H est un corps, $r(c) = 1$. Donc r se factoriserait par le quotient G^{tr} de G correspondant à la pro-2-extension totalement réelle non ramifiée hors de 2 et l'infini. Il n'y a qu'une extension quadratique réelle de $\mathbb{Q}$ non ramifiée hors de 2 et l'infini : c'est $\mathbb{Q}(\sqrt{2})$. On en déduit en utilisant le sous-groupe de Frattini que G^{tr} est abélien. Mais ceci contredit le fait que r n'est pas abélienne.

Fin de la preuve : Considérons la représentation $r : G \to \mathrm{GL}_2(K)$ construite ci-dessus ; elle est absolument irréductible et sa trace est à valeurs dans A. Comme A est noethérien, on en déduit par un argument standard qu'il existe un A-réseau [1] Λ dans K^2 stable par $r(G)$. Le réseau bidual (cf. [1, §4.2])) $(\Lambda^*)^* \subset K^2$ est alors stable par $r(G)$ lui aussi, mais comme il est

1. i.e. un sous-A-module de type fini Λ de K^2 tel que $\Lambda K = K^2$, cf. [1, §4.1].

réflexif sur un anneau local régulier de dimension 2. il est libre. L'action de $r(G)$ sur $\Lambda = A^2$ définit la représentation cherchée. Sa continuité découle de celle de sa trace.

3. Preuve du théorème 2 et de l'unicité de r.

On fixe r une représentation continue $G \to \mathrm{GL}_2(A)$ telle que $\mathrm{tr}\, r(\mathrm{Frob}_p) = T_p$ pour tout p premier impair. On a déjà vu que $r : G \to \mathrm{GL}_2(K)$ est absolument irréductible. Considérons $\bar{r} : G \to \mathrm{GL}_2(k)$. Comme $\mathrm{tr}\, \bar{r} = 0$, on a dans une certaine base $\bar{r}(g) = \begin{pmatrix} 1 & \eta(g) \\ 0 & 1 \end{pmatrix}$, où $\eta : G \to \mathbb{F}_2$ est un morphisme continu. Il y a quatre tels morphismes : 0 et ceux correspondant à $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$. Soit $\mathbb{F}_2[\epsilon]$ l'algèbre des nombres duaux sur $\mathbb{F}_2$ ($\epsilon^2 = 0$), et considérons maintenant le morphisme $\nu : A \to \mathbb{F}_2[\epsilon]$ qui envoie x et y sur ϵ. La composition de r avec ce morphisme définit une représentation $\tilde{r} : G \to \mathrm{GL}_2(\mathbb{F}_2[\epsilon])$ qui est une déformation de $\bar{r}$. On peut donc écrire, dans une base de $\mathbb{F}_2[\epsilon]^2$ relevant celle de $\mathbb{F}_2^2$ choisie plus haut, $\tilde{r} = \begin{pmatrix} 1+\epsilon\alpha & \eta+\epsilon\beta \\ \epsilon\gamma & 1+\epsilon\delta \end{pmatrix}$, où $\alpha, \beta, \gamma, \delta$ sont des applications continues de G dans $\mathbb{F}_2$. Le fait que $\tilde{r}$ est un homomorphisme entraîne que $\gamma : G \to \mathbb{F}_2$ en est un. Comme $\det \tilde{r} = 1$, on voit que $\mathrm{tr}\, \tilde{r} = (\alpha + \delta)\epsilon = \eta\gamma\epsilon$. Mais par définition, $\mathrm{tr}\, \tilde{r}(\mathrm{Frob}_3) = \nu(T_3) = \nu(x) = \epsilon$ et de même $\mathrm{tr}\, \tilde{r}(\mathrm{Frob}_5) = \epsilon$. On a donc $\eta(\mathrm{Frob}_3)\gamma(\mathrm{Frob}_3) = \eta(\mathrm{Frob}_5)\gamma(\mathrm{Frob}_5) = 1$ dans $\mathbb{F}_2$, et donc $\eta(\mathrm{Frob}_3) = \eta(\mathrm{Frob}_5) = 1$, ce qui montre (puisque 3 est décomposé dans $\mathbb{Q}(\sqrt{-2})$ et 5 est décomposé dans $\mathbb{Q}(i)$) que η correspond bien à $\mathbb{Q}(\sqrt{2})$. Ceci prouve le point (ii) du théorème 2.

Remarque 1. La preuve ci-dessus montre aussi que $\gamma = \eta \neq 0$. Autrement dit, la représentation $\tilde{r}$ est irréductible, au sens où il n'y a pas de $\mathbb{F}_2[\epsilon]$-sous-module libre de rang un de $\mathbb{F}_2[\epsilon]^2$ qui soit stable par $\tilde{r}(G)$. On en déduit facilement que pour $\mathfrak{p} = (f)$ un idéal premier de hauteur 1 où f est de la forme $x + y +$ termes de plus hauts degrés, la représentation $r_{\mathfrak{p}}$ est irréductible. En effet, le morphisme $\nu : A \to \mathbb{F}_2[\epsilon]$ se factorise sous cette condition sur $\mathfrak{p}$ par $A \to A/\mathfrak{p}$, et la réductibilité de $r_{\mathfrak{p}}$ sur $k(\mathfrak{p})$ entrainerait celle de $r_{\mathfrak{p}}$ sur $A/\mathfrak{p}$ (qui est un anneau de valuation discrète dans ce cas), donc celle de $\tilde{r}$ sur $\mathbb{F}_2[\epsilon]$. Cela s'applique en particulier à l'idéal $\mathfrak{p}_0$ (voir (1)).

Nous allons maintenant donner un argument de Serre prouvant que *pour tout idéal premier de hauteur un $\mathfrak{p} \neq \mathfrak{p}_0$, la représentation $r_{\mathfrak{p}}$ est absolument irréductible.* Supposons que $r_{\mathfrak{p}}$ est réductible dans une extension finie L de $k(\mathfrak{p})$, et soit B la fermeture intégrale de $A/\mathfrak{p}$ dans L. Notons X et Y les images de x et y dans B. L'anneau B est de valuation discrète, isomorphe à $\mathbb{F}_2[[t]]$, et l'on a $\mathrm{tr}\, r_{\mathfrak{p}} = \chi + \chi^{-1}$ où $\chi : G \to B^*$ est un caractère continu. Le charactère χ se factorise donc par un caractère $\tilde{\chi} : G^{\mathrm{ab}} = \mathbb{Z}_2^* \to B^*$. Écrivons $\tilde{\chi}(3) = \chi(\mathrm{Frob}_3) = 1 + u$ avec u dans l'idéal maximal de B. On a $X = \mathrm{tr}\, r_{\mathfrak{p}}(\mathrm{Frob}_3) = (1+u) + (1+u)^{-1}$. Comme B^* n'a pas d'élément d'ordre 2, $\tilde{\chi}(-1) = 1$. Comme $5 \equiv -3 \equiv 1 \pmod 4$, on peut poser $a =$

$\log_2(5)/\log_2(-3) \in \mathbb{Z}_2$ et on a $5 = (-3)^a$ dans $\mathbb{Z}_2$, et donc $\tilde{\chi}(5) = \tilde{\chi}((-3)^a) = \tilde{\chi}(3)^a = (1+u)^a$, et de même $\tilde{\chi}^{-1}(5) = (1+u)^{-a}$, si bien que $Y = \operatorname{tr} r_{\mathfrak{p}}(\mathrm{Frob}_5) = (1+u)^a + (1+u)^{-a} = \tau_a(X)$ (τ_a est définie juste après l'énoncé du théorème 2). On a donc $y + \tau_a(x) \in \mathfrak{p}$, i.e. avec les notations de l'introduction $\mathfrak{p}_0 \subset \mathfrak{p}$ et comme ce sont tous deux des idéaux premiers de hauteur 1, $\mathfrak{p}_0 = \mathfrak{p}$.

On a fini de prouver le théorème 2 pour toute représentation r satisfaisant les conditions requises : (i) a été prouvé dans la deuxième étape de la section précédente, (ii) au début de celle-ci, et nous venons de prouver (iii) pour $\mathfrak{p} \neq \mathfrak{p}_0$, tandis que la remarque 1 traite le cas $\mathfrak{p} = \mathfrak{p}_0$.

Comme nous l'avons dit, l'unicité de r découle de (iii) par un argument standard que nous rappelons brièvement. Soit M et M' deux A-réseaux réflexifs de K^2 stables par $r(G) \subset \mathrm{GL}_2(K)$; il s'agit de montrer que M et M' sont homothétiques. Pour tout idéal premier $\mathfrak{p}$ de hauteur 1, l'anneau localisé $A_{(\mathfrak{p})}$ est de valuation discrète, de corps de fraction K et corps résiduel $k(\mathfrak{p})$, et les $A_{(\mathfrak{p})}$-réseaux $A_{(\mathfrak{p})}M$ et $A_{(\mathfrak{p})}M'$, nécessairement libres, sont des représentations de dimension 2 de G, résiduellement irréductibles puisque leur représentation résiduelle est $r_{\mathfrak{p}}$. On a donc $A_{(\mathfrak{p})}M = x_{\mathfrak{p}}A_{(\mathfrak{p})}M'$ pour des éléments $x_{\mathfrak{p}} \in K^*$ qu'on peut choisir presque tous égaux à 1. Comme A est factoriel, il existe $x \in K^*$ tel que $xA_{(\mathfrak{p})} = x_{\mathfrak{p}}A_{(\mathfrak{p})}$ pour tout $\mathfrak{p}$. Comme $M = \cap_{\mathfrak{p}} A_{\mathfrak{p}}M$ puisque A est intégralement clos et M est réflexif ([1, §4.2, th. 2]), et de même pour M', on a $M = xM'$, CQFD.

4. Universalité de r et preuve des théorèmes 3 et 4

Commençons par montrer le caractère universel de la représentation r, ou plutôt de sa trace. Soit $\mathcal{C}$ la catégorie des $\mathbb{F}_2$-algèbres locales noethériennes, les morphismes étant les morphismes d'anneaux locaux. Soit D le foncteur de $\mathcal{C}$ dans la catégorie des ensembles qui, à un objet S de C, d'idéal maximal m, associe l'ensemble des déterminants de Chenevier continus (t, d) de G dans S tels que $d = 1$, $t(c) = 0$, et $t \equiv 0 \pmod{m}$.

Proposition 1 (Chenevier)**.** *Le foncteur D est représentable. L'espace tangent de D est de dimension* 2.

Preuve : La représentabilité du foncteur D sans les conditions $d = 1$, $t(c) = 0$ est [2, Prop 3.3], et celle de D s'en déduit immédiatement.

Soit G' le plus grand quotient de G abélien de 2-torsion. D'après [2, lemma 5.3] l'espace tangent de D est naturellement isomorphe à l'espace des applications $\tau : G' \to \mathbb{F}_2$ satisfaisant $\tau(1) = \tau(c) = 0$ (cet isomorphisme fait correspondre à une telle application τ le déterminant de Chenevier $(\epsilon\tau, 1)$ à valeurs dans $\mathbb{F}_2[\epsilon]$). Comme $G' = \mathrm{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$ est de cardinal 4, on voit que l'espace tangent est de dimension 2.

On déduit presque immédiatement de la proposition :

Corollaire 1. *Le foncteur D est représentable par A. Le déterminant universel sur A est* $(\operatorname{tr} r, 1)$.

En effet, soit R est l'objet de $\mathcal{C}$ représentant D, et $(t_{\text{univ}}, 1)$ le déterminant de Chenevier universel de G dans R. Le déterminant de Chenevier $(\operatorname{tr} r, 1)$ est un élément de $D(A)$ (on a bien $\operatorname{tr} r(c) = 0$ puisque les valeurs propres dans $\bar{K}$ de $r(c)$ sont de carré 1, donc égales à 1) et définit donc un morphisme $R \to A$, qui est surjectif car son image contient l'image $T_p = \operatorname{tr} r(\text{Frob}_p)$ de $t_{\text{univ}}(\text{Frob}_p)$ et est compacte, et donc un isomorphisme vue l'assertion sur l'espace tangent.

Démontrons le point (i) du théorème 3. Posons $B = \mathbb{F}_2[[u]]$, où u est une indéterminée, et soit $\chi : G \to B^*$ l'unique caractère continu tel que $\chi(\text{Frob}_3) = 1 + u$. Le déterminant de Chenevier $(\chi + \chi^{-1}, 1)$ est un élément de $D(B)$ et détermine donc, d'après le corollaire, un morphisme $\phi : A \to B$ tel que $\phi \circ \operatorname{tr} r = \chi + \chi^{-1}$. On montre comme dans la preuve du point (iii) du théorème 2 que $\ker \phi = \mathfrak{p}_0$. Posons $x = \phi(X) = \chi(\text{Frob}_3) + \chi(\text{Frob}_3)^{-1} = (1+u) + (1+u)^{-1} \in B$. L'image de ϕ est la sous-algèbre $\mathbb{F}_2[[x]]$ de B ; en effet, cet image contient x et est fermée, donc contient $\mathbb{F}_2[[x]]$; et pour tout p impair, l'image de T_p dans B est la série $\tau_{a(p)}(x) \in \mathbb{F}_2[[x]]$ où

$$a(p) = \log_2(p^*)/\log_2(-3) \in \mathbb{Z}_2, \text{ avec } p^* = p \text{ si } p \equiv 1 \pmod 4,\ p^* = -p \text{ sinon},$$

si bien que l'image de A est contenue dans $\mathbb{F}_2[[x]]$. On a donc $A/\mathfrak{p}_0 = \mathbb{F}_2[[x]]$ et $k(\mathfrak{p}_0) = \mathbb{F}_2((x))$, et $\text{Frac}(B)$ est une extension quadratique ramifiée de $k(\mathfrak{p}_0)$. Comme sur $\text{Frac}(B)$ on a $\operatorname{tr} r_{\mathfrak{p}_0} = \chi + \chi^{-1}$, on a prouvé (i).

Prouvons le théorème 4. Il suffit de montrer que les images t_p des T_p dans B sont algébriquement indépendantes sur $\mathbb{F}_2$. Comme $t_p = (1+u)^{a(p)} + (1+u)^{-a(p)}$, il suffit de montrer que les éléments $(1+u)^{a(p)}$ de B sont algébriquement indépendants. Les entiers 2-adiques $a(p) = \log_2(p^*)/\log_2(-3)$ sont linéairement indépendants sur $\mathbb{Z}$ par l'unicité de la factorisation d'un entier en nombres premiers. Nous sommes donc ramenés à prouver le lemme suivant :

Lemme 1. *Si (a_i) une une famille d'éléments de $\mathbb{Z}_2$ linéairement indépendants sur $\mathbb{Z}$, les séries formelles $(1+u)^{a_i}$ de $\mathbb{F}_2[[u]]$ sont algébriquement indépendantes sur $\mathbb{F}_2$.*

En effet, une relation algébrique sur $\mathbb{F}_2$ entre les séries formelles $(1+u)^{a_i}$ est une relation linéaire sur $\mathbb{F}_2$ entre séries formelles de la forme $(1+u)^{\sum n_i a_i}$, où les n_i sont des entiers positifs presque tous nuls, et ces exposants $\sum n_i a_i$ sont deux à deux distincts puisque les a_i sont linéairement indépendants sur $\mathbb{Z}$. Mais une famille finie de séries formelles $(1+u)^{b_i}$ où les b_i sont des entiers 2-adiques deux à deux distincts est linéairement indépendante sur $\mathbb{F}_2$. En effet, soit n un entier tel que $b_i \neq b_j \pmod{2^n}$ pour tout $i \neq j$, et soit $\bar{b}_i$ l'entier naturel compris entre 0 et $2^n - 1$ et congru à b_i modulo 2^n. On a alors $(1+u)^{b_i} \equiv (1+u)^{\bar{b}_i} \pmod{u^{2^n}}$. Les polynômes $(1+u)^{\bar{b}_i}$ sont linéairement indépendants puisque de degrés deux à deux distincts, et comme ils

sont tous de degrés $< 2^n$, l'indépendance linéaire des $(1+u)^{b_i}$ en résulte. Ceci termine la preuve du lemme et du théorème 4.

Pour finir la preuve du théorème 3, considérons un idéal premier $\mathfrak{p}$ de hauteur 1 différent de $\mathfrak{p}_0$. On sait donc que $r_{\mathfrak{p}}$ est absolument irréductible. Si la restriction de $r_{\mathfrak{p}}$ à un sous-groupe ouvert H de G est absolument réductible, et si L est une extension finie de $k(\mathfrak{p})$ sur laquelle $r_{\mathfrak{p}}$ se réduit, le sous-groupe H est d'indice 2 et il existe un caractère $\chi : H \to L^*$ tel que $r_{\mathfrak{p}} \simeq \mathrm{Ind}_H^G \chi$. L'extension quadratique de $\mathbb{Q}$ fixée par H ne peut pas être $\mathbb{Q}(\sqrt{2})$, car χ se factoriserait par le groupe de Galois de l'extension cyclotomique de $\mathbb{Q}(\sqrt{2})$ et $r_{\mathfrak{p}}$ serait absolument réductible, contrairement à notre hypothèse $\mathfrak{p} \neq \mathfrak{p}_0$. C'est donc $\mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{-2})$. Dans le premier cas, on a $\mathrm{Frob}_3 \in G - H$ puisque 3 est inerte dans $\mathbb{Q}(i)$, donc $\mathrm{tr}\, r_p(\mathrm{Frob}_3) = 0$ ce qui montre que x est dans $\mathfrak{p}$, et donc que $\mathfrak{p} = (x)$. On voit de même dans le second cas que $\mathfrak{p} = (y)$.

Réciproquement, il faut montrer que si $\mathfrak{p} = (x)$ ou $\mathfrak{p} = (y)$ l'image de G est diédrale. Il y a deux manières de le faire : la première, due à Serre, repose sur les propriétés des séries θ associées à $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{-2})$ respectivement, cf. [5, §§8 et 9]. La seconde est la suivante : soit $B = \mathbb{F}_2[[t]]$, H le sous-groupe d'indice 2 de G correspondant à $\mathbb{Q}(i)$, χ un caractère continu de H à valeur dans B^* dont le noyau correspond à la $\mathbb{Z}_2$-extension anti-cyclotomique de $\mathbb{Q}(i)$, et $\rho : G \to \mathrm{GL}_2(B)$ la représentation $\mathrm{Ind}_H^G \chi$. Comme χ est anti-cyclotomique, on voit que $\det \rho = 1$, et on en déduit que le déterminant de Chenevier $(\mathrm{tr}\, \rho, 1)$ de G dans B, est un élément de $D(B)$. On conclut dans le cas $\mathfrak{p} = (x)$ en appliquant le corollaire 1, comme dans la preuve du point (i) du théorème 3. Le même méthode avec $\mathbb{Q}(\sqrt{-2})$ s'applique au cas $\mathfrak{p} = (y)$.

Références

[1] N. Bourbaki, Éléments de mathématique. Fasc. XXXI. Algèbre commutative. Chapitre 7 : Diviseurs. Actualités Scientifiques et Industrielles, No. 1314, Hermann, Paris 1965

[2] G. Chenevier, The p-adic analytic space of pseudocharacters of a profinite groups and pseudorepresentations over arbitrary rings,
disponible sur http://www.math.polytechnique.fr/~chenevier/articles/determinants.pdf

[3] E. Kani, Idoneal Numbers and some generalizations, preprint 2009, 34 pp., à paraître aux Ann. Sci. Math. Quebec, disponible sur http ://www.mast.queensu.ca/~kani

[4] J.-L. Nicolas & J.-P. Serre, L'ordre de nilpotence des opérateurs de Hecke modulo 2, C.R.A.S. 350 (2012)

[5] J.-L. Nicolas & J.-P. Serre, Formes modulaires modulo 2 : structure de l'algèbre de Hecke, C.R.A.S. 350 (2012)

Joël Bellaïche, Brandeis University, 415 South Street, Waltham, MA 02454-9110, U.S.A
E-mail address: jbellaic@brandeis.edu