Astérisque

HENRI CARAYOL

La conjecture de Sato-Tate [d'après Clozel, Harris, Shepherd-Barron, Taylor]

Astérisque, tome 317 (2008), Séminaire Bourbaki,
exp. n° 977, p. 345-391

<http://www.numdam.org/item?id=AST_2008__317__345_0>

Séminaire BOURBAKI Juin 2007
59e année, 2006-2007, no 977, p. 345 à 392

LA CONJECTURE DE SATO-TATE
[d'après Clozel, Harris, Shepherd-Barron, Taylor]

par **Henri CARAYOL**

INTRODUCTION

0.1. — Soit $\mathcal{E}$ une courbe elliptique définie sur $\mathbb{Q}$. Pour p un nombre premier de bonne réduction, autrement dit lorsque p ne divise pas le conducteur N de la courbe, écrivons comme d'habitude $1+p-a_p$ le cardinal de $\mathcal{E}(\mathbb{F}_p)$. On sait depuis Hasse que a_p est de valeur absolue inférieure où égale à $2\sqrt{p}$, de sorte que l'on peut définir un angle θ_p par :

$$a_p = 2\sqrt{p}\cos\theta_p \quad ; \quad \theta_p \in [0,\pi].$$

Les valeurs propres de l'endomorphisme de Frobenius géométrique F_p (agissant sur la cohomologie ℓ-adique de notre courbe) sont alors $\sqrt{p}\,e^{i\theta_p}$ et $\sqrt{p}\,e^{-i\theta_p}$.

La conjecture de Sato-Tate, qui remonte à la première moitié des années 60, prédit comment doivent être répartis les θ_p dans l'intervalle $[0,\pi]$, dans le cas où $\mathcal{E}$ n'a pas de « multiplication complexe » : c'est-à-dire que $\mathcal{E}$ n'a pas d'autres endomorphismes sur $\mathbb{C}$ que ceux, évidents, qui constituent un anneau isomorphe à $\mathbb{Z}$.

CONJECTURE 0.1. — *On suppose $\mathcal{E}$ sans multiplication complexe. Alors les θ_p sont équirépartis sur $[0,\pi]$ relativement à la mesure $\mu = \frac{2}{\pi}\sin^2\theta\, d\theta$.*

Par définition, l'équirépartition prédite par cette conjecture consiste en la propriété suivante : notant $\mathcal{P}_n$ l'ensemble des nombres premiers $\leq n$ et non diviseurs de N, la moyenne $\frac{1}{\sharp\,\mathcal{P}_n}\sum_{p\in\mathcal{P}_n}\delta_{\theta_p}$ des mesures de Dirac aux points θ_p converge vaguement vers μ, autrement dit pour chaque fonction continue f sur $[0,\pi]$, on doit avoir :

$$\lim_{n\to+\infty}\frac{1}{\sharp\,\mathcal{P}_n}\sum_{p\in\mathcal{P}_n} f(\theta_p) \;=\; \mu(f)\ .$$

Lorsque $\mathcal{E}$ a de la multiplication complexe, ses endomorphismes constituent un ordre dans l'anneau des entiers d'un corps quadratique imaginaire. Il n'est pas difficile

alors de voir que les θ_p sont équirépartis relativement à la mesure $\frac{1}{2}\delta_{\frac{\pi}{2}} + \frac{1}{2\pi}\,d\theta$. Plus précisément, pour les p inertes, on a $a_p = 0$ et donc $\theta_p = \pi/2$, tandis que, pour les p décomposés, les valeurs propres de Frobenius sont égales (ou conjuguées) à celles données par un Grössencharakter du corps quadratique ; or on sait depuis Hecke que les angles associés sont équirépartis sur le cercle (pour la mesure habituelle).

On formule de façon évidente une généralisation de la conjecture au cas d'une courbe elliptique (sans multiplication complexe) définie sur un quelconque corps de nombres F : en chaque place finie (idéal premier) v de bonne réduction, notant q_v le cardinal du corps résiduel correspondant, on pose :

$$a_v = 1 + q_v - \sharp\,\mathcal{E}(\mathbb{F}_{q_v}) = 2\sqrt{q}_v \cos\theta_v \quad (\theta_v \in [0,\pi])$$

et l'on définit l'équirépartition des θ_v comme ci-dessus, en considérant la moyenne des δ_{θ_v} sur l'ensemble des v de norme $\leq n$.

L'objet de cet exposé est d'expliquer comment cette conjecture est maintenant démontrée sous certaines hypothèses additionnelles :

THÉORÈME 0.2. — *Soit $\mathcal{E}$ une courbe elliptique définie sur un corps totalement réel F. On suppose que $\mathcal{E}$ admet une réduction multiplicative en au moins une place finie. Alors les nombres θ_v sont équirépartis sur $[0,\pi]$ relativement à la mesure μ définie ci-dessus (dite « de Sato-Tate »).*

Remarque 0.3. — L'hypothèse que $\mathcal{E}$ admette quelque part une réduction multiplicative équivaut à dire que son invariant $j(\mathcal{E})$ n'est pas un entier de F, et elle entraîne que $\mathcal{E}$ ne possède pas de multiplication complexe. C'est une hypothèse qui pourra être levée le jour où l'on disposera de résultats suffisants sur la stabilisation de la formule des traces d'Arthur-Selberg, résultats qui semblent accessibles dans l'état d'avancement actuel de la théorie automorphe. Mentionnons également que Harris ([**14**]) a récemment prouvé, en admettant de telles avancées, des résultats conditionnels : en particulier un analogue de la conjecture de Sato-Tate pour le produit de deux courbes elliptiques (non isogènes).

0.2. — L'application de SU(2) dans $[0,\pi]$ qui, à une matrice unitaire u, associe $\arccos\left(\frac{1}{2}\mathrm{tr}(u)\right)$ est surjective $\left(\text{de section } \theta \to \begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix}\right)$ et elle identifie l'intervalle $[0,\pi]$ à l'ensemble des classes de conjugaison de SU(2). Il est facile de voir que la mesure de Sato-Tate n'est autre que l'image directe par cette application de la mesure de Haar normalisée de SU(2). Par suite la conjecture revient à prédire que les classes de conjugaison des $\begin{pmatrix} e^{i\theta_p} & \\ & e^{-i\theta_p} \end{pmatrix}$ sont équiréparties dans SU(2).

Dès la fin des années 60, Serre savait ramener cette conjecture à une question sur les fonctions L, ainsi qu'il l'a expliqué précisément dans son livre [**26**]. Noter que vers la même époque Tate avait également conscience de cette relation. Serre généralise

la méthode de Hadamard–de la Vallée Poussin afin d'énoncer un résultat qui couvre de nombreux cas connus ou conjecturaux d'équirépartition, et dont le prototype est l'équirépartition des nombres premiers dans les différentes classes de congruence de $(\mathbb{Z}/N\mathbb{Z})^*$:

Soient K un groupe compact, F un corps de nombres et supposons donnée, pour chaque place finie v (à l'exception d'un nombre fini) de F, une classe de conjugaison Θ_v dans K. Notant q_v le cardinal du corps résiduel correspondant, on forme, pour chaque représentation irréductible (unitaire) non triviale r de K, la fonction L suivante, qui converge pour $\Re s > 1$:

$$L^*(r,s) = \prod_v \det(1 - q_v^{-s} r(\Theta_v))^{-1}.$$

PROPOSITION 0.4 ([**26**]). — *On suppose que, pour chaque r irréductible non triviale, cette fonction se prolonge analytiquement à un ouvert contenant le demi-plan fermé $\Re s \geq 1$ et que le prolongement ne s'annule pas sur la droite $\Re s = 1$. Alors les classes de conjugaison Θ_v sont équiréparties dans K.*

Revenons au cas, qui nous intéresse ici, d'une courbe elliptique $\mathcal{E}/F$, et notons $\beta_v = e^{i\theta_v}$ et $\beta_v^{-1} = e^{-i\theta_v}$ les valeurs propres de Frobenius divisées par $\sqrt{q_v}$. Les représentations irréductibles non triviales de SU(2) sont les puissances symétriques $\mathrm{Sym}^{\mathrm{n}}\mathrm{r}_1$ ($n > 0$) de la représentation naturelle de dimension 2. La fonction L correspondante écrit alors

$$L^*(\mathrm{Sym}^{\mathrm{n}}\mathcal{E}, \mathrm{s}) = \prod_{\mathrm{v}} (1-\beta_{\mathrm{v}}^{-\mathrm{n}}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}(1-\beta_{\mathrm{v}}^{-\mathrm{n}+2}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1} \cdots (1-\beta_{\mathrm{v}}^{\mathrm{n}-2}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}(1-\beta_{\mathrm{v}}^{\mathrm{n}}\mathrm{q}_{\mathrm{v}}^{-\mathrm{s}})^{-1}.$$

On prendra garde au fait qu'il s'agit d'une fonction L incomplète (manquent les facteurs aux mauvaises places et en l'infini) et qu'elle est normalisée de façon inhabituelle (à la manière automorphe, ce qui se traduit par un décalage de $n/2$ par rapport à la normalisation habituelle). Pour prouver la conjecture de Sato-Tate, il « suffit » donc de montrer que ces fonctions se prolongent analytiquement et n'ont pas de zéro sur la droite $\Re s = 1$.

0.3. — Du moins lorsque le corps de base est $\mathbb{Q}$, on sait depuis les travaux de Wiles et Taylor-Wiles, complétés par ceux de Diamond, Breuil, Conrad et Taylor (cf. [**10**]), que notre courbe elliptique est associée à une forme modulaire parabolique (ou, dans un langage un peu différent, à une représentation automorphe parabolique du groupe $\mathrm{GL}_2(\mathbb{A})$), pour laquelle on sait par ailleurs que la fonction L admet un prolongement qui ne s'annule pas sur $\Re s = 1$. Les conjectures générales de Langlands prédisent d'autre part que doit exister une « fonctorialité puissance symétrique », qui à une représentation automorphe de $\mathrm{GL}_2(\mathbb{A})$ en associe une autre, cette fois-ci du groupe $\mathrm{GL}_{n+1}(\mathbb{A})$. Or on sait que les fonctions L associées aux représentations

automorphes paraboliques du groupe linéaire GL_n ($n > 1$) vérifient les propriétés voulues de prolongement (holomorphe) et de non-annulation sur la droite $\Re s = 1$. Si on savait prouver l'existence de ces fonctorialités, a priori de nature « analytique », la conjecture en découlerait donc aussitôt. Malheureusement, on ne sait faire cela à l'heure actuelle que pour des petites valeurs de n (Shahidi). La stratégie utilisée par Clozel, Harris, Shepherd–Barron, Taylor met en jeu plus d'arithmétique. L'idée est en gros de généraliser aux groupes de dimension supérieure la méthode de Taylor-Wiles afin de prouver directement la « modularité » des puissances symétriques, c'est-à-dire le fait qu'elles correspondent à des représentations automorphes des groupes linéaires. Formulé ainsi, il s'agit encore d'un résultat inaccessible à l'heure actuelle, mais les auteurs en prouvent une version affaiblie dans laquelle on doit se restreindre au groupe de Galois absolu d'une extension assez grande F'/F (ce que Taylor nomme l'automorphie « potentielle ») et supposer n *impair*. Cette dernière restriction est d'ailleurs conditionnellement levée dans le récent article de Harris [**14**] mentionné plus haut, qui établit un résultat analogue pour n pair.

THÉORÈME 0.5. — *Soit $\mathcal{E}$ une courbe elliptique comme ci-dessus (admettant quelque part une réduction multiplicative) ; supposons n impair. Il existe alors une extension galoisienne totalement réelle F'/F sur laquelle* $\mathrm{Sym}^n\mathcal{E}$ *devient automorphe (parabolique) : cela signifie que la puissance symétrique n-ième de la représentation ℓ-adique associée à $\mathcal{E}$, restreinte au groupe de Galois* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathrm{F}')$, *a même fonction L (convenablement normalisée) qu'une représentation automorphe parabolique de* $\mathrm{GL}_{n+1}(\mathbb{A}_{F'})$.

Remarque 0.6. — À vrai dire, on a besoin d'une version légèrement plus forte de ce théorème qui assure que l'on peut choisir, lorsque n varie dans un ensemble fini $\mathcal{N}$ de nombres impairs, F' fixe ; utilisant les propriétés du changement de base construit par Arthur et Clozel [**1**], on peut contrôler la « descente » (idée due originellement à Harris) et voir aussi que l'automorphie est alors assurée pour toute extension intermédiaire $F \subset F'' \subset F'$ avec F'/F'' résoluble.

Le théorème (0.2) résulte alors de ce qui précède par des arguments assez simples qui seront expliqués au paragraphe suivant.

0.4. — Le principe de la méthode utilisée avec succès depuis les travaux fondateurs de Wiles pour établir la modularité (nous parlerons plutôt ici d'automorphie) d'une représentation ℓ–adique ρ consiste à partir de la modularité de sa réduction $\overline{\rho}$ et d'un résultat de « relèvement de la modularité » affirmant que tout relèvement convenable de $\overline{\rho}$ est encore modulaire. Ici « convenable » est une abréviation imprécise pour un ensemble d'hypothèses, dont certaines sont naturelles (en particulier la nature de ρ aux places divisant ℓ, qui doit être au minimum « potentiellement semi-stable », mais

pour lesquelles on demande en général plus) et dont d'autres sont beaucoup plus compliquées et parfois artificielles, tenant à nos limitations techniques. Dans le cas originel des représentations associées aux courbes elliptiques sur $\mathbb{Q}$, on pouvait dans certains cas partir de la représentation modulo 3 (l'image correspondante étant résoluble) et sinon s'y ramener par un argument de compatibilité entre divers systèmes de représentations ℓ–adiques. La modularité de la représentation résiduelle $\overline{\rho}$ ne constituait donc pas un réel problème. Il y va tout autrement dès que l'on sort de ce cadre et Taylor a été le premier à prouver des résultats de modularité potentielle, dans le cas de représentations de dimension 2 plus générales. Le point crucial est que l'on ne sait pas alors montrer la modularité de $\overline{\rho}$; pour la prouver après restriction à un corps de nombres convenable, on utilise un théorème de Moret-Bailly (voir le paragraphe 9) affirmant (en gros) qu'un schéma irréductible a un point sur un corps de nombres (vérifiant certaines propriétés) s'il en est de même localement, i.e. sur les divers complétés. Ceci permettait à Taylor (en dimension 2) de montrer qu'une restriction convenable de $\overline{\rho}$ peut se réaliser à partir de la ℓ-torsion d'une certaine variété abélienne à multiplication réelle A. Par ailleurs on s'est assuré que la v-torsion de A, pour une place v de caractéristique différente de ℓ, est modulaire. Taylor en déduisait alors la modularité potentielle de la représentation résiduelle $\overline{\rho}$, par un argument de compatibilité entre systèmes ℓ–adiques qui faisait usage d'un résultat de relèvement de la modularité (un argument tout à fait semblable à celui de Wiles mentionné plus haut).

La situation est analogue dans le cas que nous considérons ici. Il s'agit tout d'abord d'établir des résultats de relèvement de l'automorphie. L'article [**8**], en réalité disponible depuis plusieurs années, réalisait ce programme modulo un important grain de sel. Rappelons en quelques mots que la stratégie inventée par Wiles et Taylor se décomposait en deux étapes : on prouve tout d'abord le relèvement de la modularité de $\overline{\rho}$ à ρ dans le cas « minimal », c'est-à-dire lorsque ρ est aussi peu ramifiée qu'il est permis par $\overline{\rho}$. Puis on passe au cas général en contrôlant comment varient, lorsque la ramification augmente, les algèbres de Hecke et de déformation galoisienne, et ceci repose sur un lemme, dû à Ihara, qui permet de générer des congruences entre formes de différents niveaux.

Le manuscrit [**8**] met en œuvre cette stratégie en dimension supérieure. On compare une certaine algèbre de Hecke $\mathbb{T}$, associée à un groupe unitaire sur un corps totalement réel, à un anneau universel $\mathcal{R}$ de déformations de représentations galoisiennes anti-autoduales. On utilise des techniques analogues à celles de Wiles et Taylor-Wiles, en y incorporant d'importantes améliorations conceptuelles dues à Diamond, Fujiwara, Skinner-Wiles. On utilise aussi bien sûr la construction de représentations galoisiennes associées aux représentations automorphes autoduales de $\mathrm{GL}(n)$ (Kottwitz, Clozel) ainsi que la conjecture de Langlands locale et la compatibilité entre cette dernière et les constructions globales (Harris, Taylor). Utilisant tous ces ingrédients, les auteurs

parviennent au bout de ce travail à établir l'égalité cherchée $\mathcal{R} = \mathbb{T}$ *dans le cas minimal*. Ils énoncent aussi une généralisation conjecturale du lemme d'Ihara au cas de $\mathrm{GL}(n)$ et montrent que cela impliquerait le résultat de relèvement cherché dans le cas général.

Cependant personne n'a pu jusqu'à présent prouver ce lemme, de sorte que les résultats contenus dans [**8**] sont restés pour l'essentiel conjecturaux jusqu'à une date récente. Ce n'est que le dernier travail de Taylor [**28**] qui a débloqué la situation en contournant l'obstacle du lemme d'Ihara et en le remplaçant par une idée entièrement nouvelle qui permet de rendre valides inconditionnellement les résultats de [**8**]. Au lieu de distinguer les cas minimal/non minimal, il s'attaque directement à ce dernier (supposant même, après changement de base, que la situation est « la pire » possible). L'idée fondamentale est de comparer la situation qui nous intéresse $\mathcal{R}, \mathbb{T}$ à une autre $\tilde{\mathcal{R}}, \tilde{\mathbb{T}}$ à laquelle s'appliquent les méthodes de Taylor-Wiles-Diamond-Fujiwara et Skinner-Wiles, enrichies d'idées essentielles dues à Kisin. Le résultat souhaité (à savoir l'égalité entre $\mathbb{T}$ et *l'anneau réduit* $\mathcal{R}^{\mathrm{red}}$) se déduit alors de l'égalité entre les réductions modulo ℓ (ou plutôt une place au-dessus de ℓ) de nos divers anneaux et le fait que les composantes irréductibles de $\mathcal{R}$ et $\tilde{\mathcal{R}}$ peuvent se comparer à celles de leurs réductions modulo ℓ.

Par ailleurs les résultats voulus sur l'automorphie potentielle de certaines représentations galoisiennes sont développés par Harris, Shepherd-Barron et Taylor dans [**15**]. Ici et contrairement au cas des représentations de degré 2, les familles de variétés abéliennes à multiplication réelle ne constituent plus une source suffisante de représentations galoisiennes modulo ℓ. L'ingrédient nouveau de [**15**] consiste à considérer la famille, paramétrée par $t \in \mathbb{P}^1$, d'hypersurfaces $Y_t \subset \mathbb{P}^n$ d'équations

$$X_0^{n+1} + X_1^{n+1} + X_2^{n+1} + \cdots + X_n^{n+1} = (n+1)\, t\, X_0 X_1 X_2 \cdots X_n\,.$$

Sur chacune agit le sous-groupe H_0 de la puissance cartésienne μ_{n+1}^{n+1} du groupe des racines $(n+1)$-ièmes de l'unité constitué des $(\eta_0, \eta_1, \ldots, \eta_n)$ vérifiant $\prod \eta_i = 1$. L'idée est que les invariants sous H_0 dans la cohomologie en degré $n-1$ de ces variétés fournissent, pour n pair, une famille assez vaste de représentations galoisiennes symplectiques de dimension n et de poids de Hodge-Tate $\{0, 1, \ldots, n-1\}$. C'est pour mettre en œuvre cette idée que l'on fait usage du résultat de Moret-Bailly ([**23**]), de façon analogue à ce qui a déjà été évoqué plus haut.

Je voudrais remercier ici Laurent Clozel et Jean-Pierre Wintenberger d'avoir bien voulu lire une version préliminaire de cet exposé, et de m'avoir fait part d'utiles remarques et suggestions.

1. PREMIÈRES RÉDUCTIONS

Dans ce paragraphe, j'explique pourquoi la conjecture de Sato-Tate se ramène au théorème (0.5) (enrichi comme expliqué dans la remarque (0.6)). Supposons ce théorème établi ; il nous faut donc prouver que $L^*(\mathrm{Sym}^n\mathcal{E}, s)$ admet un prolongement holomorphe sur un ouvert contenant la droite $\{\Re s = 1\}$ et que ce prolongement ne s'annule pas sur cette dernière.

Commençons par le cas où n est impair. Le théorème (0.5) nous fournit une extension F'. On applique alors le théorème d'induction de Brauer à la représentation triviale $\mathbf{1}_{\mathrm{Gal}(F'/F)}$ du groupe $\mathrm{Gal}(F'/F)$. Cette représentation apparaît ainsi comme une combinaison virtuelle d'induites de caractères de dimension 1 :

$$\mathbf{1}_{\mathrm{Gal}(F'/F)} = \sum m_i \,\mathrm{Ind}_{\mathrm{Gal}(F'/F_i'')}^{\mathrm{Gal}(F'/F)} \chi_i$$

avec F'/F_i'' des extensions *résolubles*. On en déduit une égalité de $\overline{\mathbb{Q}}_\ell$-représentations virtuelles de $\mathrm{Gal}(\overline{F}/F)$:

$$\begin{aligned} R(n) = R(n) \otimes \mathbf{1}_{\mathrm{Gal}(\overline{F}/F)} &= \sum m_i \, R(n) \otimes \mathrm{Ind}_{\mathrm{Gal}(\overline{F}/F_i'')}^{\mathrm{Gal}(\overline{F}/F)} \chi_i \\ &= \sum m_i \,\mathrm{Ind}_{\mathrm{Gal}(\overline{F}/F_i'')}^{\mathrm{Gal}(\overline{F}/F)} \left(R(n)_{|\mathrm{Gal}(\overline{F}/F_i'')} \otimes \chi_i\right), \end{aligned}$$

avec $R(n)$ la puissance symétrique n-ième de la représentation ℓ-adique de degré 2 associée à $\mathcal{E}$.

Les propriétés des fonctions L relativement à la somme et l'induction nous permettent alors d'écrire :

$$\begin{aligned} L^*(\mathrm{Sym}^n\mathcal{E}, s) &= \prod L^*\left(\mathrm{Ind}_{\mathrm{Gal}(\overline{F}/F_i'')}^{\mathrm{Gal}(\overline{F}/F)} \left(R(n)_{|\mathrm{Gal}(\overline{F}/F_i'')} \otimes \chi_i\right), s\right)^{m_i} \\ &= \prod L_{F_i''}^*\left(R(n)_{|\mathrm{Gal}(\overline{F}/F_i'')} \otimes \chi_i, s\right)^{m_i}. \end{aligned}$$

Or le théorème (0.5) (joint à la remarque (0.6)) affirme que les représentations considérées dans la seconde ligne de l'égalité ci-dessus sont automorphes (paraboliques) : par conséquent les fonctions L correspondantes ont des prolongements analytiques sans zéro sur $\Re s \geq 1$. La formule précédente implique donc que $L^*(\mathrm{Sym}^n\mathcal{E}, s)$ admet un prolongement méromorphe à $\mathbb{C}$ sans zéro ni pôle sur ce demi-plan.

Reste à voir ce qui se passe pour les puissances symétriques paires. On utilise pour cela la décomposition suivante (qui résulte de la décomposition analogue dans la catégorie des représentations de SL_2)

$$R(n) \otimes R(1) \simeq R(n+1) \oplus R(n-1).$$

D'où

$$L^*(\mathrm{Sym}^{n+1}\mathcal{E}, s) = \frac{L^*(R(n) \otimes R(1), s)}{L^*(\mathrm{Sym}^{n-1}\mathcal{E}, s)}.$$

Or pour n *impair* on sait que $R(n)$ et $R(1)$ deviennent automorphes sur la même extension F' (appliquer le théorème (0.5) et la remarque qui suit, avec $\mathcal{N} = \{1\,,\, n\}$). Un raisonnement identique à celui expliqué ci-dessus permet alors d'exprimer $L^*(R(n) \otimes R(1)\,, s)$ comme un quotient de produits de fonctions L à la Rankin, associées à des couples de formes automorphes (respectivement sur $\mathrm{GL}(n+1)$ et sur $\mathrm{GL}(2)$) ; or on sait (d'après Shahidi [**27**]) que ces fonctions L de paires ont un prolongement analytique et qui ne s'annule pas sur $\Re s = 1$. On voit donc qu'une récurrence sur les valeurs paires de la puissance (ici $n+1$ et $n-1$) permet de conclure.

Par ailleurs le théorème (0.5) est une conséquence du résultat légèrement plus général suivant (en réalité, l'énoncé dont on a besoin (cf. la remarque (0.6)) devrait être valide uniformément pour n variant dans un ensemble fini d'entiers pairs, mais je néglige cette difficulté non essentielle afin de ne pas compliquer inutilement cet exposé).

THÉORÈME 1.1 ([**15**]). — *Soient F un corps totalement réel, n un entier pair et ℓ un nombre premier non ramifié dans F que l'on suppose de plus « grand » par rapport à n (i.e. $\ell > \max(C(n)\,,\, 2n+1)$) où $C(n)$ est une constante ne dépendant que de n et qui sera définie dans la suite de cet exposé (cf. théorème 8.3). Soient $q \neq \ell$ un autre nombre premier, v_q une place de F au-dessus de q. On fait l'hypothèse que le cardinal du corps résiduel correspondant $k(v_q)$ est tel que $(\sharp k(v_q))^j \not\equiv 1 \bmod \ell$ pour $j = 1, \ldots, n$.*

Supposons alors donnée une représentation continue

$$r\colon \mathrm{Gal}(\overline{F}\,/\,F) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

vérifiant les propriétés suivantes :

(1) $\det r$ *est l'inverse du caractère cyclotomique* ;

(2) r *n'est ramifiée qu'en un nombre fini de places de* F ;

(3) *la réduction modulo* ℓ *de* r *est une surjection* $\mathrm{Gal}(\overline{F}\,/\,F) \to \mathrm{GL}_2(\mathbb{F}_\ell)$;

(4) *pour chaque place* w *de* F *au-dessus de* ℓ, *la restriction de* r *au groupe de Galois local est cristalline de poids* 0 *et* 1 ;

(5) *la semi-simplifiée de la restriction* r *au groupe de Galois local en* v_q *est non ramifiée et les valeurs propres correspondantes du Frobenius sont* 1 *et* $\sharp k(v_q)$.

Alors il existe une extension galoisienne F' de F sur laquelle $\mathrm{Sym}^{n-1} r$ devient automorphe (parabolique).

Pour obtenir le théorème (0.5), il suffit alors d'appliquer ce résultat (avec n remplacé par $n+1$) à r donnée par la cohomologie ℓ-adique de $\mathcal{E}$; en prenant ℓ assez grand (d'après un résultat bien connu de Serre, (3) est alors satisfaite), et pour v_q la place où notre courbe admet une réduction multiplicative (que l'on peut supposer déployée, quitte à tordre par un caractère).

Remarque 1.2. — En réalité la conclusion du théorème de [**15**] est plus précise : il existe une place v'_q de F' au-dessus de v_q telle que la restriction de Sym^{n-1} r au groupe de Galois $\mathrm{Gal}(\overline{F}\,/\,F')$ soit automorphe de poids 0 et de type $\{Sp_n(1)\}_{v'_q}$, au sens qui sera défini dans le paragraphe qui va suivre.

Remarque 1.3. — La généralisation qui fait passer du théorème (0.5) au précédent n'est pas « gratuite ». En fait, on utilise dans la preuve du théorème (1.1) l'existence d'une courbe elliptique $\mathcal{E}''$ sur un corps F'', vérifiant de nombreuses propriétés, en particulier le fait que la réduction $\bar{r}$ de r restreinte au groupe $\mathrm{Gal}(\overline{F}\,/\,F'')$ coïncide avec la représentation sur $H^1(\mathcal{E}_{\overline{F}}, \mathbb{F}_\ell)$. Il convient de remarquer toutefois que, dans l'application à notre cas de la représentation r associée à une courbe elliptique $\mathcal{E}$, en général $\mathcal{E}''$ est différente de $\mathcal{E}$, et qu'en réalité le fait que r provienne de $\mathcal{E}$ n'est donc d'aucune utilité (cf. ci-dessous (9.2), où $\mathcal{E}''$ est notée $\mathcal{E}$).

2. REPRÉSENTATIONS AUTOMORPHES ET ALGÈBRES DE HECKE

Dans les paragraphes précédents, je supposais de façon plus ou moins implicite que les représentations automorphes considérées étaient des représentations du groupe linéaire sur les adèles, mais en réalité, pour démontrer ces résultats, on travaille sur des formes intérieures de groupes unitaires. En effet la méthode de Taylor-Wiles pour GL_2 repose sur certaines coïncidences numériques dans des calculs de groupes de cohomologie galoisienne aux places archimédiennes ; ces coïncidences se produisent aussi pour des groupes unitaires ou symplectiques par exemple, auquel cas on peut espérer généraliser la méthode (voir [**13**] dans le cas du groupe GSp_4). Ce n'est jamais le cas pour GL_n avec $n > 2$. Nous allons donc dans la suite travailler avec des groupes unitaires sur F ; toutefois on a le « changement de base » qui, à une représentation automorphe sur un tel groupe, en associe une autre sur le groupe linéaire de l'extension quadratique totalement imaginaire E de F où le groupe unitaire devient isomorphe à une forme de GL_n. Les représentations automorphes de $\mathrm{GL}_n(\mathbb{A}_E)$ ainsi obtenues sont « anti-autoduales », i.e. invariantes par le passage à la contragrédiente suivie de l'application de la conjugaison par rapport à F. Réciproquement, une forme automorphe anti-autoduale vérifiant des propriétés locales convenables se descend en une représentation du groupe unitaire. En ce qui concerne le corps totalement réel F, les représentations automorphes de $\mathrm{GL}_n(\mathbb{A}_F)$ qui sont autoduales se relèvent par « changement de base » en des représentations automorphes de $\mathrm{GL}_n(\mathbb{A}_E)$, stables à la fois par passage à la contragrédiente et par conjugaison, et qui se descendent donc à des groupes unitaires convenables.

2.1. — Plus précisément, les groupes utilisés dans [**8**] et [**28**] sont des formes de groupes unitaires sur notre corps totalement réel F, qui sont compactes à toutes les places réelles. On notera G un tel groupe, obtenu comme suit : fixons un entier n , un nombre premier $\ell > n$ non ramifié dans F et notons E un corps CM obtenu comme le composé de F et d'un corps quadratique imaginaire dans lequel ℓ est décomposé ; fixons un ensemble fini non vide $S(B)$ de places finies de F, qui se décomposent dans E et dont aucune n'est au-dessus de ℓ ; on suppose que, si n est pair, $\sharp S(B)$ a la même parité que $n\,[F : \mathbb{Q}]/2$.

Il existe alors une algèbre à division B de centre E et de dimension n^2 qui est déployée à toutes les places non au-dessus de $S(B)$ et telle qu'au contraire $B_{\tilde{v}}$ soit une algèbre à division si $\tilde{v}$ se trouve au-dessus d'une place de $S(B)$. On peut de plus supposer que B est munie d'une involution de seconde espèce $b \to b^*$ de telle sorte que le groupe algébrique G sur F défini par

$$G(R) = \{g \in B \otimes_F R\,;\, gg^* = 1\}$$

soit compact (isomorphe à $U(n)$) en chaque place archimédienne et quasi-déployé en chaque place finie non dans $S(B)$.

On choisit un ordre $\mathcal{O}_B$ de B qui est stable par l'involution $*$ et maximal à toutes les places divisant les places décomposées de F, ce qui détermine un modèle entier de G. Si v est une place décomposée non dans $S(B)$, on peut fixer un relèvement $\tilde{v}$ de v en une place de E. On peut ensuite choisir un isomorphisme entre $\mathcal{O}_{B,v}$ et $M_n(\mathcal{O}_{F,v})$ et cela définit un isomorphisme entre $G(F_v)$ et $\mathrm{GL}_n(F_v)$, qui associe $G(\mathcal{O}_{F,v})$ et $\mathrm{GL}_n(\mathcal{O}_{F,v})$. Un tel isomorphisme est fixé modulo un automorphisme intérieur de $\mathrm{GL}_n(F_v)$ par le choix de $\tilde{v}$, l'autre choix conduisant à la composition par un automorphisme extérieur.

Pour $v \in S(B)$, le groupe $G(F_v)$ est le groupe multiplicatif d'un corps gauche ($B_{\tilde{v}}$, pour $\tilde{v}$ l'une des places au-dessus de v). Enfin, pour v non décomposée, $G(F_v)$ est un groupe unitaire quasi-déployé.

2.2. — Notons $\mathbb{A}_F$ l'anneau des adèles de F et $\mathbb{A}_F^\infty$ l'anneau des adèles privé de sa composante archimédienne. Soit $U \subset G(\mathbb{A}_F^\infty)$ un sous-groupe compact ouvert. L'espace des doubles classes $G(F) \setminus G(\mathbb{A}_F^\infty) / U$ est *fini* et c'est à partir de celui-ci, et donc de façon combinatoire, que sont définis dans [**8**] et [**28**] les espaces de formes automorphes. L'avantage est qu'on obtient ainsi à peu de frais une définition qui a un sens pour toute $\mathcal{O}$-algèbre, $\mathcal{O}$ désignant l'anneau des entiers d'un corps ℓ–adique K choisi assez gros pour contenir l'image de chaque plongement $E \to \overline{K}$.

Plus précisément, cette définition va dépendre du choix d'une représentation algébrique de $G(F_\ell)$ (produit des $G(F_v)$ aux places divisant ℓ), associée à un certain « poids », et aussi du choix de représentations ρ_v (cette fois-ci à noyau ouvert) des $G(F_v)$ pour $v \in S(B)$.

Le *poids* a est la donnée pour chaque plongement $\tau : E \to K$ de n entiers $a_{\tau,1} \geq a_{\tau,2} \geq \cdots \geq a_{\tau,n}$ vérifiant $a_{\tau c,i} = -a_{\tau,n+1-i}$ (où c désigne la conjugaison de E/F). Cela définit une représentation, notée ξ_a, de $G(F_\ell) = \prod_{v|\ell} G(F_v)$ sur un K-espace vectoriel W_a : on choisit pour chaque v un plongement τ correspondant ; cela donne un plongement de $G(F_v)$ dans le groupe $\mathrm{GL}_n(E_\tau)$ pour lequel le poids (a_τ) définit une représentation ; puis l'on fait le produit tensoriel des représentations ainsi obtenues. On peut fixer dans W_a un $\mathcal{O}$-réseau $G(\mathcal{O}_{F,\ell})$-invariant M_a.

Donnons-nous également, pour chaque $v \in S(B)$, une K–représentation absolument irréductible à noyau ouvert ρ_v de $G(F_v)$, laquelle admet également un réseau invariant M_{ρ_v}. On note $M_{a,\{\rho_v\}}$ le produit tensoriel de M_a et des M_{ρ_v}, sur lequel opère le produit de $G(\mathcal{O}_{F,\ell})$ et des $G(F_v)$ pour $v \in S(B)$.

2.3. — Si A est une $\mathcal{O}$-algèbre et U un sous-groupe compact ouvert assez petit de $G(\mathbb{A}_F^\infty)$, on définit l'espace $\mathcal{A}_{a,\{\rho_v\}}(U\,,\,A)$ des *formes automorphes de poids a et de type* $\{\rho_v\}_{v\in S(B)}$, à valeurs dans A, comme l'ensemble des applications :

$$f\,:\,G(F)\setminus G(\mathbb{A}_F^\infty) \to M_{a,\{\rho_v\}} \otimes_{\mathcal{O}} A$$

vérifiant l'identité, pour $u \in U$:

$$f(gu) = (u_{S(B),\ell})^{-1}\, f(g)$$

où l'on a noté $u_{S(B),\ell}$ la projection de u sur $G(F_\ell) \times \prod_{v\in S(B)} G(F_v)$.

Même notation $\mathcal{A}_{a,\{\rho_v\}}(V\,,\,A)$, lorsque V n'est pas nécessairement ouvert, pour désigner la réunion des $\mathcal{A}_{a,\{\rho_v\}}(U\,,\,A)$ avec $U \supset V$.

2.4. Lien avec les représentations automorphes des groupes linéaires

Lorsque A est un corps de caractéristique 0, il est facile d'identifier les espaces précédents à des espaces de formes automorphes, au sens habituel, sur le groupe $G(\mathbb{A}_F)$. À vrai dire, en vue de ce que nous allons faire ensuite, nous avons défini ci-dessus nos objets sur le corps ℓ-adique K de sorte que, si nous voulons comparer cela à la théorie habituelle, nous devons choisir un plongement $K \subset \mathbb{C}$.

Vues sur $\mathbb{C}$, les formes définies ci-dessus correspondent alors à des représentations automorphes du groupe G. On a alors le « changement de base » (Labesse-Clozel, [**21**]), déjà évoqué plus haut et qui associe à une telle représentation d'une forme de groupe unitaire une représentation automorphe du groupe $G(\mathbb{A}_E)$. Ce dernier n'est rien d'autre que le groupe adélique associé au groupe multiplicatif de l'algèbre B ; on applique ensuite la « correspondance de Jacquet-Langlands » (généralisée) qui produit finalement une représentation automorphe du groupe $\mathrm{GL}_n(\mathbb{A}_E)$.

Soit $\pi = \otimes \pi_w$ une telle représentation automorphe parabolique du groupe $\mathrm{GL}_n(\mathbb{A}_E)$. On dit que cette représentation est *de poids a* (avec a comme ci-dessus) si pour tout plongement $\tau : E \to \mathbb{C}$, qui définit une place archimédienne ∞_τ ainsi

qu'une identification entre E_{∞_τ} et $\mathbb{C}$, la représentation π_{∞_τ} a le même caractère infinitésimal que la représentation de plus haut poids a_τ.

Donnons-nous par ailleurs un ensemble fini S de places de E et pour chaque $v \in S$ une représentation de carré intégrable σ_v de $\mathrm{GL}_n(E_v)$. On dit que π est *de type* $\{\sigma_v\}_{v\in S}$ si, pour chaque $v \in S$, la composante locale π_v coïncide, à une torsion près par un caractère non ramifié, à la contragrédiente $\sigma_v^\vee$.

Dans le cas des représentations automorphes du groupe $\mathrm{GL}_n(\mathbb{A}_F)$, on définit les choses de façon semblable : un poids est la donnée pour chaque plongement réel τ de n entiers relatifs $a_{\tau,1} \geq a_{\tau,2} \geq \cdots \geq a_{\tau,n}$; on dit alors qu'une représentation $\pi = \otimes\pi_w$ est de poids a si, pour chaque τ, la représentation π_{∞_τ} a le même caractère infinitésimal que la représentation de plus haut poids a_τ.

Étant donnés un ensemble fini S de places de F et, pour chaque $v \in S$, une représentation de carré intégrable σ_v de $\mathrm{GL}_n(F_v)$, on définit comme ci-dessus ce qu'est une représentation automorphe de type $\{\sigma_v\}_{v\in S}$.

Les représentations automorphes du groupe G associées aux formes de poids a et de type $\{\rho_v\}_{v\in S(B)}$ définies précédemment correspondent par le changement de base suivi de la correspondance de Jacquet-Langlands à des représentations automorphes paraboliques du groupe $\mathrm{GL}_n(\mathbb{A}_E)$ qui sont anti-autoduales, de poids a et de type $\{\sigma_{\tilde{v}}\}_{\tilde{v}\in\tilde{S}(B)}$: l'anti-autodualité signifie que la contragrédiente $\pi^\vee$ coïncide avec π^c, obtenue en composant π et l'automorphisme défini par c. Quant à $\sigma_{\tilde{v}}$ pour $\tilde{v} \in \tilde{S}(B)$ (ensemble des places relevant une place de $S(B)$) c'est la représentation de la série discrète de $\mathrm{GL}_n(E_{\tilde{v}}) = \mathrm{GL}_n(F_v)$ qui correspond à ρ_v (une représentation de $G(F_v)$, identifié à $B_{\tilde{v}}^*$) par la correspondance de Jacquet-Langlands locale.

Les représentations automorphes paraboliques du groupe $\mathrm{GL}_n(\mathbb{A}_F)$ qui sont autoduales, de poids a et de type $\{\sigma_v\}_{v\in S(B)}$ s'envoient par changement de base sur un sous-ensemble des précédentes : on obtient des représentations automorphes paraboliques π de $\mathrm{GL}_n(\mathbb{A}_E)$ telles que $\pi^\vee \simeq \pi \simeq \pi^c$.

2.5. — Dans [**28**], on introduit de plus un ensemble fini R de places décomposées de F, disjoint de $S(B)$ et ne contenant aucune place divisant ℓ. On fixe pour chaque $v \in S$ une place $\tilde{v}$ de E qui la relève, ainsi qu'un isomorphisme entre $G(F_v)$ et $\mathrm{GL}_n(F_v)$. On considère alors le sous-groupe d'Iwahori $\mathrm{Iw}(v)$, constitué des matrices de $\mathrm{GL}_n(\mathcal{O}_{F,v})$ dont la réduction est triangulaire supérieure. On a un homomorphisme $\mathrm{Iw}(v) \to (k(v)^*)^n$ (avec $k(v)$ le corps résiduel) qui envoie une matrice de $\mathrm{Iw}(v)$ sur la réduction de ses termes diagonaux.

On se donnera pour chaque $v \in R$ un caractère χ_v de $\mathrm{Iw}(v)$ à valeurs dans $\mathcal{O}^*$, factorisé via cet homomorphisme. La donnée de χ_v équivaut donc à la donnée de n caractères $\chi_{v,1}, \chi_{v,2}, \ldots, \chi_{v,n}$ de $k(v)^*$.

On note

$$M_{a,\{\rho_v\},\{\chi_v\}} = M_{a,\{\rho_v\}} \otimes \bigotimes_{v\in R} \mathcal{O}(\chi_v)\,;$$

c'est une représentation du groupe produit $G(F_\ell) \times \prod_{v\in S(B)\cup R} G(F_v)$. Supposant U choisi tel que sa projection sur chacun des $G(F_v)$, pour $v \in R$, soit contenue dans $\mathrm{Iw}(v)$, on définit un espace de formes automorphes $\mathcal{A}_{a,\{\rho_v\},\{\chi_v\}}(U\,,\,A)$ constitué des fonctions

$$f\,:\,G(F)\setminus G(\mathbb{A}_F^\infty) \to M_{a,\{\rho_v\},\{\chi_v\}} \otimes_{\mathcal{O}} A$$

vérifiant une identité analogue à la précédente, avec cette fois la projection de u sur $G(F_\ell) \times \prod_{v\in S(B)\cup R} G(F_v)$.

2.6. Algèbres de Hecke

Fixons-nous un ensemble fini T de « mauvaises » places de F, décomposées dans E, et contenant $S(B)$ ainsi que toutes les places divisant ℓ. On suppose que notre sous-groupe U se décompose comme un produit de $U_v \subset G(F_v)$ et qu'à chaque place v non dans T, U_v est un sous-groupe maximal « hyperspécial » ; en particulier pour v décomposé non dans T, on a $U_v \simeq \mathrm{GL}_n(\mathcal{O}_{F,v})$.

Les opérateurs de Hecke, agissant sur $\mathcal{A}_{a,\{\rho_v\}}(U\,,\,\mathcal{O})$, sont définis (de façon habituelle) à partir des doubles classes, pour chaque place v décomposée non dans T :

$$T_v^{(j)} \;=\; \Big[\,\mathrm{GL}_n(\mathcal{O}_{F,v}) \begin{pmatrix} \varpi_v \mathbf{1}_j & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_{n-j} \end{pmatrix} \mathrm{GL}_n(\mathcal{O}_{F,v})\,\Big]$$

où ϖ_v désigne une uniformisante en la place v.

L'*algèbre de Hecke* $\mathbb{T}^T_{a,\{\rho_v\}}(U)$ est la sous–$\mathcal{O}$–algèbre de $\mathrm{End}\big(\mathcal{A}_{a,\{\rho_v\}}(U\,,\,\mathcal{O})\big)$ engendrée par ces opérateurs (aux « bonnes places » uniquement, donc), ainsi que par l'inverse de $T_v^{(n)}$.

Cette algèbre de Hecke est commutative, libre et de type fini comme $\mathcal{O}$–module.

Notations analogues et mêmes résultats lorsqu'on rajoute comme ci-dessus l'ensemble R de places v où U_v est contenu dans le sous-groupe d'Iwahori, lequel doit opérer via un caractère χ_v. Pour T contenant toutes les places décomposées ramifiées (et donc en particulier R) l'algèbre de Hecke correspondante, agissant sur $\mathcal{A}_{a,\{\rho_v\},\{\chi_v\}}(U\,,\,\mathcal{O})$, est notée $\mathbb{T}^T_{a,\{\rho_v\},\{\chi_v\}}(U)$.

2.7. Places de Taylor-Wiles

Enfin on verra apparaître dans la suite un ensemble fini supplémentaire Q de places de F décomposées dans E (les « places de Taylor-Wiles »). On fixera alors comme ci-dessus une place $\tilde{v}$ au-dessus de chaque $v \in Q$, ainsi qu'un isomorphisme entre $G(F_v)$ et le groupe $\mathrm{GL}_n(F_v)$. Puis on considérera le sous-groupe $U_0(v)$ (resp. $U_1(v) \subset U_0(v)$)

de $\mathrm{GL}_n(\mathcal{O}_{F,v})$ constitué des matrices dont la réduction a une dernière ligne de la forme $\begin{pmatrix} 0 & 0 & \cdots & 0 & \star \end{pmatrix}$ (resp. $\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$).

On prendra $U_v = U_1(v)$ comme composante du sous-groupe U en ces places . On aura alors sur l'ensemble des formes automorphes correspondantes un opérateur de Hecke V_α, défini pour chaque $\alpha \in F_v^*$ et associé à la double classe :

$$V_{\alpha,v} = \left[U_1(v) \begin{pmatrix} \mathbf{1}_{n-1} & \mathbf{0} \\ \mathbf{0} & \alpha \end{pmatrix} U_1(v) \right].$$

3. REPRÉSENTATIONS GALOISIENNES ASSOCIÉES AUX FORMES AUTOMORPHES

3.1. — Soit E un corps CM, et soit π une représentation automorphe parabolique du groupe $\mathrm{GL}_n(\mathbb{A}_E)$. On suppose qu'elle est anti-autoduale, que ses composantes archimédiennes ont de la cohomologie, et qu'il existe une place finie où la composante locale π_v appartient à la série discrète. Dans ces conditions, on sait associer à π un système de représentations ℓ-adiques de dimension n du groupe de Galois $\mathrm{Gal}(\overline{E}/E)$. Ceci a été démontré à la suite de divers travaux de Kottwitz, Clozel, Taylor, et utilise le yoga du changement de base entre groupe linéaire sur E et groupes unitaires sur F, mais pas exactement les mêmes groupes unitaires que ceux dont il a été question ci-dessus. La construction fait usage en effet de variétés de Shimura associées à des groupes unitaires de type $(n-1,1)$ en une place infinie et compacts aux autres (cf. par exemple [**4**]) ; il s'agit donc de redescendre notre représentation π à une forme de groupe unitaire de ce type. Il est important de remarquer que, dans l'état actuel de la théorie automorphe, on ne sait pas faire la construction de représentations galoisiennes à partir de groupes unitaires isotropes. C'est cette limitation qui nous impose de supposer qu'il existe une place discrète et cela conduit à l'hypothèse additionnelle dans la preuve de la conjecture de Sato-Tate : le fait que la courbe est supposée avoir réduction multiplicative en une place au moins. C'est aussi pour la même raison que l'on a supposé $S(B) \neq \varnothing$ dans le paragraphe précédent. Lorsqu'on disposera de résultats suffisants sur la stabilisation de la formule des traces d'Arthur-Selberg, cette limitation devrait devenir inutile. On prouverait ainsi la conjecture de Sato-Tate sur un corps totalement réel en toute généralité.

De même, pour F totalement réel, on associe une représentation ℓ-adique de $\mathrm{Gal}(\overline{F}/F)$ à toute représentation automorphe du groupe $\mathrm{GL}_n(\mathbb{A}_F)$ qui est cohomologique, essentiellement (i.e. à torsion près par un caractère) autoduale, et qui admet une composante discrète.

Par réduction modulo ℓ, on obtient aussi des représentations galoisiennes à valeurs dans $\overline{\mathbb{F}}_\ell$.

DÉFINITION 3.1. — *Une représentation ℓ-adique de $\mathrm{Gal}(\overline{E}/E)$ est dite automorphe de poids a et de type $\{\sigma_v\}_{v\in S}$ si elle provient d'une représentation automorphe parabolique du groupe $\mathrm{GL}_n(\mathbb{A}_E)$ qui est anti-autoduale, de poids a et de type $\{\sigma_v\}_{v\in S(B)}$. Même définition pour une représentation à valeurs dans $\overline{\mathbb{F}}_\ell$ (on demande que ce soit la réduction d'une telle représentation galoisienne).*

Définitions analogues pour des représentations de $\mathrm{Gal}(\overline{F}/F)$. On autorise dans ce cas la représentation automorphe π à être seulement essentiellement autoduale : $\pi^\vee \simeq \pi\otimes\chi$, avec χ un caractère factorisé, via le déterminant, en un caractère de Hecke de F.

Compte tenu de la correspondance entre représentations automorphes sur G et sur GL_n, on voit donc que l'on peut associer à nos formes automorphes sur G des représentations, ℓ-adiques et modulo ℓ, du groupe de Galois de E. D'une façon maintenant assez habituelle dans cette théorie, on exprime l'essence de cette construction en termes d'algèbres de Hecke.

On commence par associer à tout idéal maximal $\mathfrak{m}$ de $\mathbb{T}^T_{a,\{\rho_v\}}(U)$ une représentation sur le quotient $\mathbb{T}^T_{a,\{\rho_v\}}(U)/\mathfrak{m}$ (un corps fini de caractéristique ℓ)

$$\overline{r}_{\mathfrak{m}} : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\mathbb{T}^T_{a,\{\rho_v\}}(U)/\mathfrak{m})$$

qui est non ramifiée en chaque place décomposée $v\notin T$ et telle que le polynôme caractéristique de $\overline{r}_{\mathfrak{m}}(\mathrm{Frob}_v)$ soit égal à la réduction modulo $\mathfrak{m}$ de

$$X^n - T_v^{(1)}X^{n-1} + \cdots + (-1)^j(\mathbf{N}w)^{j(j-1)/2}T_v^{(j)}X^{n-j} + \cdots + (-1)^n(\mathbf{N}w)^{n(n-1)/2}T_v^{(n)}\,.$$

On obtient $\overline{r}_{\mathfrak{m}}$ par réduction à partir des représentations ℓ-adiques évoquées au numéro précédent.

Si on suppose que $\overline{r}_{\mathfrak{m}}$ est absolument irréductible, alors elle se relève en une représentation

$$r_{\mathfrak{m}} : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\mathbb{T}^T_{a,\{\rho_v\}}(U)_{\mathfrak{m}})$$

à valeurs dans la localisée de l'algèbre de Hecke en $\mathfrak{m}$ et telle que le polynôme caractéristique en une place décomposée $v\notin T$ soit égal au polynôme ci-dessus. Cela peut se voir en plongeant $\mathbb{T}^T_{a,\{\rho_v\}}(U)_{\mathfrak{m}}$ dans un produit de corps ℓ-adiques puis en appliquant un résultat de [**3**] afin de prouver que le produit des représentations galoisiennes obtenues sur ces différents corps peut en fait se réaliser sur le sous-anneau $\mathbb{T}^T_{a,\{\rho_v\}}(U)_{\mathfrak{m}}$.

3.2. — Les représentations ρ de $\mathrm{Gal}(\overline{E}/E)$, obtenues comme on vient de l'expliquer à partir de représentations de groupes unitaires, sont des représentations « essentiellement anti-autoduales » : ce qui signifie que la composée ρ^c avec la conjugaison complexe (agissant par conjugaison sur $\mathrm{Gal}(\overline{E}/E)$) coïncide avec la contragrédiente

$\rho^\vee$ à torsion près par un caractère, lequel correspond ici à la puissance d'ordre $1-n$ du caractère cyclotomique ϵ.

On prend en compte ce fait en introduisant un groupe $\mathcal{G}_n$ sur $\mathbb{Z}$, avatar du L-groupe associé par Langlands à G, et défini comme le produit semi-direct de $\mathrm{GL}_n \times \mathrm{GL}_1$ par un groupe à deux éléments $\{1\,,\,j\}$, agissant par

$$j(g\,,\,\mu)j \;=\; (\mu {}^t g^{-1}\,,\,\mu)\,.$$

On a un morphisme $\nu : \mathcal{G}_n \to \mathbb{G}_m$ qui envoie (g,μ) sur μ et j sur -1.

Utilisant l'anti-autodualité, on montre que les représentations considérées ci-dessus se prolongent en des homomorphismes de $\mathrm{Gal}(\overline{E}/F)$ à valeurs dans $\mathcal{G}_n$. Plus précisément il existe une extension (dépendant de certains choix auxiliaires) de la représentation résiduelle $\overline{r}_\mathfrak{m}$ en un homomorphisme

$$\overline{r}_\mathfrak{m} \;:\; \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(\mathbb{T}^T_{a,\{\rho_v\}}(U)/\mathfrak{m})$$

et, une fois ce dernier fixé, il se relève de façon unique en un homomorphisme

$$r_\mathfrak{m} \;:\; \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(\mathbb{T}^T_{a,\{\rho_v\}}(U)_\mathfrak{m})$$

(le sous-groupe $\mathrm{Gal}(\overline{E}/E)$ est alors l'image réciproque de $\mathrm{GL}_n(\mathbb{T}^T_{a,\{\rho_v\}}(U)_\mathfrak{m}) \times \mathrm{GL}_1(\mathbb{T}^T_{a,\{\rho_v\}}(U)_\mathfrak{m})$ et la composante sur le premier facteur coïncide avec la représentation construite précédemment – tandis que celle sur le second facteur est ϵ^{1-n}.)

3.3. Places particulières

Le but des numéros suivants est de décrire en certaines places particulières le comportement des représentations galoisiennes construites au numéro précédent : on regarde la restriction $\overline{r}_{\mathfrak{m},w}$ (resp. $r_{\mathfrak{m},w}$) de $\overline{r}_\mathfrak{m}$ (resp. $r_\mathfrak{m}$) au groupe de décomposition $\mathrm{Gal}(\overline{E}_w/E_w)$ en une place w de E relevant une place v de F. Cette représentation locale est non ramifiée, comme on l'a vu ci-dessus, pour v une place décomposée non dans T. Elle l'est aussi pour v inerte si U_v est un sous-groupe compact maximal « hyperspécial ».

Rappelons ici des résultats importants relatifs à la correspondance de Langlands (supposons pour simplifier qu'on a fixé un isomorphisme entre $\mathbb{C}$ et $\overline{\mathbb{Q}}_\ell$) : Harris et Taylor ont prouvé ([**16**]) l'existence de la correspondance de Langlands locale, qui à une représentation (admissible irréductible) π_v du groupe $\mathrm{GL}_n(F_v)$ associe une $\overline{\mathbb{Q}}_\ell$-représentation $R_\ell(\pi_v)$ de $\mathrm{Gal}(\overline{F}_v/F_v)$.

On montre alors la chose suivante : la correspondance qui associe aux représentations π de $\mathrm{GL}_n(\mathbb{A}_E)$ (vérifiant les conditions ci-dessus) des représentations galoisiennes $r_\ell(\pi)$ est *compatible à cette correspondance de Langands locale.* Cela signifie que pour v une place de caractéristique $\neq \ell$ la Frobenius-semi-simplifiée de la restriction de $r_\ell(\pi)$ au groupe de décomposition en v correspond par R_ℓ à $\pi_v^\vee(n-1)$ (torsion à

la Tate). Dans [**16**] cela était déjà prouvé à semi-simplification près, résultat complété depuis dans [**32**].

On en déduit la semi-simplifiée de la réduction modulo ℓ de $r_\ell(\pi)$.

Mêmes propriétés évidemment pour les représentations galoisiennes associées aux représentations automorphes de $\mathrm{GL}_n(\mathbb{A}_F)$.

Passons en revue les différentes places considérées au paragraphe précédent, en commençant par celles divisant ℓ qui, elles, relèvent de la théorie cristalline. On s'intéresse non seulement à $\overline{r}_{\mathfrak{m}}$, mais aussi aux représentations obtenues sur les quotients artiniens de l'algèbre de Hecke.

3.4. Places divisant ℓ

On supposera dans la suite qu'en chaque place v divisant ℓ, on a : $U_v = \mathrm{GL}_n(\mathcal{O}_{F,v})$. On fait d'autre part une hypothèse de « petitesse » du poids a : pour chaque plongement de F dans K, l'un des deux plongements τ de E qui le relève est tel que soient satisfaites les inégalités :

$$\ell - 1 - n \geq a_{\tau,1} \geq a_{\tau,2} \geq \cdots \geq a_{\tau,n} \geq 0\,.$$

On peut considérer alors les restrictions aux groupes de décomposition aux différentes places w divisant ℓ des représentations précédentes ; plus précisément, on regarde les quotients artiniens A des algèbres de Hecke considérées et les représentations

$$r_{\mathfrak{m},w} \otimes_{\mathbb{T}^T_{a,\{\rho_v\}}(U)_{\mathfrak{m}}} A \,:\, \mathrm{Gal}(\overline{E}_w/E_w) \to \mathrm{GL}_n(A)\,.$$

Sous les hypothèses précédentes, on montre alors que ces représentations sur des anneaux artiniens sont dans l'image essentielle d'un foncteur $\mathbb{G}$, qui est essentiellement celui défini par Fontaine et Laffaille [**11**]. Ce foncteur $\mathbb{G}$ va d'une catégorie de modules filtrés munis de données additionnelles vers la catégorie des $\mathcal{O}$-modules munis d'une action du groupe de Galois local : voir [**8**] pour plus de détails.

3.5. Places du type « série discrète »

Comme ci-dessus, on supposera par la suite qu'aux places de $v \in S(B)$ notre groupe U_v est maximal, égal à $G(\mathcal{O}_{F,v})$.

Partons d'une telle place v et de notre représentation donnée ρ_v. Par la correspondance de Langlands, il correspond à cette dernière une représentation de carré intégrable σ_v de $\mathrm{GL}_n(F_v)$. On sait décrire une telle représentation de la série discrète : c'est une représentation de Steinberg (ou spéciale) généralisée $\mathrm{Sp}_{m_v}(\sigma'_v)$, associée à une représentation cuspidale σ'_v de $\mathrm{GL}_{n/m_v}(F_v)$ pour m_v un diviseur de n. Alors $R_\ell(\sigma'_v)$ est une représentation galoisienne irréductible de degé n/m_v. La représentation galoisienne $R_\ell(\sigma_v)$ est indécomposable et admet une filtration stable dont le gradué associé est la somme des m_v représentations $R_\ell(\sigma'_v)\,\epsilon^i$, i variant entre 0

et $m_v - 1$. Dans le cas particulier où $m_v = n$, on a les représentations de Steinberg proprement dites.

On imposera dans la suite que les ρ_v soient choisies de telle sorte que les réductions $\overline{R}_\ell(\sigma'_v)$ des $R_\ell(\sigma'_v)$ soient irréductibles (et donc alors bien déterminées), et telles que les $\overline{R}_\ell(\sigma'_v)\,\overline{\epsilon}^i$ ($0 \leq i \leq m_v - 1$) soient deux à deux non équivalentes.

Nous fixerons $\tilde{r}'_v : \mathrm{Gal}(\overline{F}_v/F) \to \mathrm{GL}_{n/m_w}(\mathcal{O})$, un modèle entier de $R_\ell(\sigma'_v)$.

En une telle place $v \in S(B)$ il existe alors sur $\overline{r}_\mathfrak{m}$ une unique filtration invariante par le groupe de Galois local, dont les gradués respectifs $\mathrm{gr}^i \overline{r}_\mathfrak{m}$ sont isomorphes, après restriction à l'inertie, aux $\tilde{r}_v \otimes_\mathcal{O} k(\epsilon^i)$.

Il en est de même pour les représentations $r_\mathfrak{m}$: les filtrations et isomorphismes sur k définis ci-dessus se relèvent de façon unique à $T^T_{a,\{\rho_v\}}(U)_\mathfrak{m}$. On obtient donc en particulier un isomorphisme $\tilde{\kappa}_v$ entre $\mathrm{gr}^0 r_\mathfrak{m}$ et $\tilde{r}_v \otimes_\mathcal{O} \mathbb{T}^T_{a,\{\rho_v\}}(U)_\mathfrak{m}$. Même chose bien sûr pour les représentations obtenues sur les quotients artiniens A de l'algèbre de Hecke.

3.6. Places au-dessus de R

Plaçons-nous dans la situation de (2.5) où l'on considère un sous-groupe U qui a une composante égale à un sous-groupe d'Iwahori aux places $v \in R$, et les formes automorphes associées à des caractères $\chi_{v,j}$ des $k(v)^*$. On s'intéresse à la représentation galoisienne sur l'algèbre de Hecke (localisée) correspondante :

$$r_\mathfrak{m} \,:\, \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\mathbb{T}^T_{a,\{\rho_v\},\{\chi_v\}}(U)_\mathfrak{m})$$

et à sa restriction au groupe de décomposition en la place $\tilde{v}$ choisie au-dessus de $v \in R$ (2.5).

Les $\chi_{v,j}$ définissent des représentations de $\mathcal{O}^*_{F,v} \simeq \mathcal{O}^*_{E,\tilde{v}}$ et donc, via l'isomorphisme de la théorie du corps de classes, des caractères (que nous désignerons encore par la même notation) du groupe d'inertie $I_{E_{\tilde{v}}}$ en $\tilde{v}$.

On peut alors montrer que, pour tout $\sigma \in I_{E_{\tilde{v}}}$, le *polynôme caractéristique* de $r_\mathfrak{m}(\sigma)$ est égal à :

$$\prod_{j=1}^{n} \left(X - \chi_{v,j}(\sigma)\right).$$

3.7. Places de Taylor-Wiles

De même, on considère le cas où $v \in Q$ est une place de F telle que $U_v = U_1(v))$ (cf. (2.7)) et l'on s'intéresse à la restriction de nos représentations galoisiennes au groupe de décomposition en $\tilde{v}$. On se place sous les hypothèses supplémentaires suivantes : la norme $\mathbf{N}v$ est $\equiv 1 \bmod \ell$; pour $\phi_{\tilde{v}}$ un élément de Frobenius fixé et correspondant à une uniformisante $\varpi_{\tilde{v}}$, il existe une valeur propre *simple* a_v du polynôme caractéristique de $\overline{r}_\mathfrak{m}(\phi_{\tilde{v}})$.

Sous ces hypothèses, on montre que la représentation résiduelle $\overline{r}_{\mathfrak{m}}$ admet une décomposition (dépendant du choix de a_v)

$$\overline{r}_{\mathfrak{m}|\mathrm{Gal}(\overline{E}_{\tilde{v}}/E_{\tilde{v}})} = \overline{\psi}_v \oplus \overline{s}_v$$

avec $\overline{s}_v$ non ramifiée de dimension $n-1$ et $\overline{\psi}_v$ de dimension 1 telle que l'action galoisienne y soit donnée via l'isomorphisme de la théorie du corps de classes par un caractère $\overline{V}$ de $E_{\tilde{v}}^*$ tel que $\overline{V}(\varpi_{\tilde{v}}) = a_v$ et que $\overline{V}(\alpha)$, pour $\alpha \in \mathcal{O}_{E,\tilde{v}}^*$, coïncide avec l'action de l'opérateur de Hecke $V_{\alpha,v}$.

Cette décomposition se relève alors en une décomposition de $r_{\mathfrak{m}}$ vérifiant des propriétés analogues :

$$r_{\mathfrak{m}|\mathrm{Gal}(\overline{E}_{\tilde{v}}/E_{\tilde{v}})} = \psi_v \oplus s_v\,.$$

4. ÉNONCÉ DE THÉORÈMES DE RELÈVEMENT DE L'AUTOMORPHIE

4.1. La notion de représentation d'image assez grosse

Il s'agit d'une hypothèse technique qui sera utilisée dans les résultats qui vont suivre.

Soit $H \subset \mathrm{GL}_n(k)$ un sous-groupe du groupe linéaire sur le corps fini k. On dit que H est *assez gros* si les trois conditions suivantes sont remplies :

- $H^0\big(H, \mathfrak{g}_n^0(k)\big) = (0)$ (où $\mathfrak{g}_n^0(k)$ désigne l'ensemble des matrices de trace nulle, H agissant via l'action adjointe) ;
- $H^1\big(H, \mathfrak{g}_n^0(k)\big) = (0)$;
- pour tout sous-H-module irréductible $W \subset \mathfrak{g}_n(k)$ (ensemble de toutes les matrices), il existe $h \in H$ et $\alpha \in k$ vérifiant les propriétés suivantes : l'espace propre généralisé $V_{h,\alpha}$ de h dans k^n relatif à α est de dimension 1 ; si on note $\pi_{h,\alpha}$ (resp. $\iota_{h,\alpha}$) la projection h-équivariante $k^n \to V_{h,\alpha}$ (resp. l'injection h-équivariante $V_{h,\alpha} \to k^n$), alors on a : $\pi_{h,\alpha} \circ W \circ \iota_{h,\alpha} \neq (0)$.

On vérifie par exemple que cette condition est satisfaite pour H contenant $\mathrm{Sp}_n(k)$ (cf. [**8**], preuve du cor. (4.5.4)) ; elle l'est aussi pour l'image d'un groupe contenant $SL_2(\mathbb{F}_\ell)$ par la représentation de degré n donnée par la puissance symétrique $(n-1)$-ième ([**15**], lemme (3.2)).

Notion analogue pour $H \subset \mathcal{G}_n(k)$. On dit que H est assez gros si :

- $H^0\big(H, \mathfrak{g}_n(k)\big) = (0)$;
- $H^1\big(H, \mathfrak{g}_n(k)\big) = (0)$;
- pour tout sous-H-module irréductible $W \subset \mathfrak{g}_n(k)$, il existe $h \in H \cap \mathcal{G}_n^0(k)$ et $\alpha \in k$ vérifiant les mêmes propriétés que ci-dessus.

4.2. Cas des corps CM

THÉORÈME 4.1 ([**28**], théorème 5.1 ou bien, modulo la conjecture expliquée en 5.3 ci-dessous, [**8**], théorème 4.3.4)

Soit E un corps CM, extension quadratique d'un corps totalement réel F. Soient deux entiers $\ell > n \geq 2$, avec ℓ premier non ramifié dans E. Soit enfin

$$r : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

une représentation continue irréductible. On note $\overline{r}$ la semi-simplifiée de la réduction de r et $\overline{r}'$ une extension de $\overline{r}$ en un homomorphisme de $\mathrm{Gal}(\overline{E}/F)$ dans $\mathcal{G}_n(\overline{\mathbb{F}}_\ell)$.

On suppose que sont vérifiées les propriétés suivantes :

(1) $r^c \simeq r^\vee \epsilon^{1-n}$.

(2) *r n'est ramifiée qu'en un nombre fini de places.*

(3) *La restriction de r au groupe de décomposition en chaque place v divisant ℓ est cristalline.*

(4) *Plus précisément, il existe un poids $a = (a_{\tau,i})$ qui est petit au sens expliqué en (3.4) et qui donne les sauts de la filtration de Hodge en une place v correspondant à τ : ces sauts sont les $a_{\tau,j} + n - j$, tous avec multiplicité* 1.

(5) *Il existe un ensemble* non vide *S de places finies de E ne divisant pas ℓ tel que, pour chaque $v \in S$, la restriction de r au groupe de décomposition corresponde à semi-simplification près à une représentation de carré intégrable σ_v de $\mathrm{GL}_n(E_v)$:*

$$r\,|^{\mathrm{ss}}_{\mathrm{Gal}(\overline{E}_v/E_v)} \simeq R_\ell(\sigma_v)^\vee(1-n)^{\mathrm{ss}}\,.$$

Une telle σ_v est donc une représentation de Steinberg généralisée $\mathrm{Sp}_{m_v}(\sigma'_v)$ associée à une représentation cuspidale de $\mathrm{GL}_{n/m_v}(E_v)$. Soit $R_v = R_\ell(\sigma'_v)^\vee$: c'est une représentation de dimension n/m_v (telle que $r\,|^{\mathrm{ss}}_{\mathrm{Gal}(\overline{E}_v/E_v)}$ soit la somme de m_v tordues de R_v).

On demande de plus que la réduction $\overline{R}_v$ soit irréductible et que l'on ait $\overline{R}_v \not\simeq \overline{R}_v\overline{\epsilon}^j$ pour $j = 1, \ldots, m_v$.

(6) *Le corps fixe $\overline{E}^{\mathrm{Ker\,ad}\,\overline{r}}$ ne contient pas $E(\zeta_\ell)$ (avec ζ_ℓ une racine ℓ-ième primitive de* 1*).*

(7) *L'image $\overline{r}'\big(\mathrm{Gal}(\overline{E}/F(\zeta_\ell))\big)$ est assez grosse.*

(8) *La représentation résiduelle $\overline{r}$ est irréductible et automorphe de poids a et de type $\{\sigma_v\}_{v\in S}$.*

Alors r est automorphe de poids a, de type $\{\sigma_v\}_{v\in S}$, et de niveau premier à ℓ (i.e. le facteur du groupe U au-dessus de ℓ est un sous-groupe compact maximal).

4.3. Cas des corps totalement réels

THÉORÈME 4.2 ([**28**], théorème 5.2 ou bien, modulo la conjecture expliquée en 5.3 ci-dessous, [**8**], théorème 4.5.3)

Soit F un corps totalement réel. Soient deux entiers $\ell > n \geq 2$ avec ℓ premier non ramifié dans F. Soit

$$r : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

une représentation continue irréductible vérifiant les propriétés ci-dessous (on note $\overline{r}$ la semi-simplifiée de la réduction de r).

(1) *$r^\vee \simeq r\epsilon^{n-1}\chi$ où χ est un caractère $\mathrm{Gal}(\overline{F}/F) \to \overline{\mathbb{Q}}_\ell^*$ tel que $\chi(c_v)$ soit indépendant de $v \mid \infty$ (avec c_v la conjugaison complexe correspondante).*

(2) *r n'est ramifiée qu'en un nombre fini de places.*

(3) *La restriction de r au groupe de décomposition en chaque place v divisant ℓ est cristalline.*

(4) *Plus précisément il existe un poids $a = (a_{\tau,i})$ (avec τ décrivant ici seulement l'ensemble des plongements de F dans K), vérifiant une condition de « petitesse » analogue à la précédente, i.e :*

$$\ell - 1 - n + a_{\tau,n} \geq a_{\tau,1} \geq a_{\tau,2} \geq \cdots \geq a_{\tau,n}\,,$$

et ce poids donne les sauts de la filtration de Hodge en une place v correspondant à τ : ce sont les $a_{\tau,j} + n - j$, tous avec multiplicité 1.

(5) *Il existe un ensemble* non vide *S de places finies de F ne divisant pas ℓ tel que, pour chaque $v \in S$, la restriction de r au groupe de décomposition corresponde à semi-simplification près à une représentation de carré intégrable σ_v de $\mathrm{GL}_n(E_v)$:*

$$r\,|^{\mathrm{ss}}_{\mathrm{Gal}(\overline{F}_v/F_v)} \simeq R_\ell(\sigma_v)^\vee(1-n)^{\mathrm{ss}}\,.$$

Une telle σ_v est une représentation de Steinberg généralisée $\mathrm{Sp}_{m_v}(\sigma'_v)$ associée à une représentation cuspidale de $\mathrm{GL}_{n/m_v}(F_v)$. Soit $R_v = r_\ell(\sigma'_v)^\vee$; c'est une représentation de dimension n/m_v (telle que $r\,|^{\mathrm{ss}}_{\mathrm{Gal}(\overline{F}_v/F_v)}$ soit la somme de m_v tordues de R_v).

On demande de plus que la réduction $\overline{R}_v$ soit irréductible et que l'on ait $\overline{R}_v \not\simeq \overline{R}_v\overline{\epsilon}^j$ pour $j = 1, \ldots, m_v$.

(6) *Le corps fixe $\overline{F}^{\mathrm{Ker\,ad}\,\overline{r}}$ ne contient pas $F(\zeta_\ell)$.*

(7) *L'image $\overline{r}\big(\mathrm{Gal}(\overline{F}/F(\zeta_\ell))\big)$ est assez grosse.*

(8) *La représentation résiduelle $\overline{r}$ est irréductible et automorphe de poids a et de type $\{\sigma_v\}_{v\in S}$.*

Alors *r est automorphe de poids a, de type $\{\sigma_v\}_{v\in S}$ et de niveau premier à ℓ.*

5. ESPACES DE DÉFORMATIONS : [28] VERSUS [8]

5.1. — On se donne un corps ℓ-adique K comme dans le paragraphe précédent, donc supposé au moins assez gros pour contenir tous les plongements possibles de E ; nous notons également $\mathcal{O}$ son anneau d'entiers, λ une uniformisante et k le corps résiduel.

On part d'un homomorphisme continu $\overline{r} : \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(k)$, ainsi que d'un caractère $\chi : \mathrm{Gal}(\overline{E}/F) \to \mathcal{O}^*$ et l'on cherche à déformer $\overline{r}$. Nous appliquerons ensuite cette théorie avec, pour k, le corps résiduel d'une algèbre de Hecke en un idéal $\mathfrak{m}$ et $\overline{r} = \overline{r}_{\mathfrak{m}}$, afin de comparer des anneaux de déformations galoisiennes à des algèbres de Hecke localisées.

Plus précisément (cf. 3.2), $\overline{r}$ est tel que $\overline{r}^{-1}(\mathrm{GL}_n(k) \times \mathrm{GL}_1(k))$ soit le sous-groupe $\mathrm{Gal}(\overline{E}/E)$; on suppose aussi que $\overline{r}_{|\mathrm{Gal}(\overline{E}/E)}$ est absolument irréductible et que $\nu \circ \overline{r} = (\chi \bmod \lambda)$.

Ces données étant fixées, on s'intéresse au problème de relever $\overline{r}$ à une $\mathcal{O}$-algèbre artinienne locale A de corps résiduel k ; un tel relèvement est par définition la donnée d'un homomorphisme continu :

$$r : \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(A)$$

de réduction $\overline{r}$ et tel que $\nu \circ r = \chi$. Une *déformation* consiste en une classe de conjugaison, sous $\ker\big(\mathcal{G}_n(A) \to \mathcal{G}_n(k)\big)$, de tels relèvements.

On peut vérifier, de façon maintenant assez habituelle dans cette théorie, que l'espace des telles déformations est (pro-)représentable par une $\mathcal{O}$-algèbre locale noethérienne complète $\mathcal{R}^{\mathrm{univ}}$. Mais cette algèbre est beaucoup trop grosse pour pouvoir être comparée à une algèbre de Hecke. C'est pourquoi on introduit des restrictions locales supplémentaires aux différentes places : on se limite à ne considérer que des déformations vérifiant des propriétés qui sont imposées (comme expliqué brièvement aux paragraphes 3.3–3.7 précédents) par le fait de provenir des algèbres de Hecke considérées. Cela définit certains quotients de $\mathcal{R}^{\mathrm{univ}}$ que l'on comparera ensuite à des algèbres de Hecke localisées. Ici l'approche diverge sensiblement entre les articles [**8**] et [**28**].

5.2. — Je vais me contenter ici de décrire de façon extrêmement rapide et schématique la méthode utilisée dans [**8**] pour me concentrer ensuite de façon plus détaillée sur celle de [**28**]. Supposons donnée une représentation galoisienne résiduelle $\overline{r}_{\mathfrak{m}}$ associée à un idéal maximal $\mathfrak{m}$ de l'algèbre de Hecke $\mathbb{T}^T_{a,\{\rho_v\}}(U)$. On se donne un ensemble fini Z de places (de caractéristique résiduelle $\neq \ell$) où $\overline{r}_{\mathfrak{m}}$ est non ramifiée mais où l'on va progressivement autoriser les déformations à se ramifier.

Plus précisément, soit $S \subset Z$. On considère les déformations de $\overline{r}_{\mathfrak{m}}$ dont les restrictions aux groupes de Galois locaux $\mathrm{Gal}(\overline{E}_w/E_w)$ sont des représentations vérifiant des propriétés du type suivant :

a) En une place divisant ℓ : la représentation est « cristalline » au sens suivant : elle est dans l'image essentielle du foncteur $\mathbb{G}$ (cf. (3.4)). Dans [**8**] apparaît aussi la possibilité qu'en certaines places divisant ℓ la situation puisse être ramifiée ou que U_v soit plus petit que $\mathrm{GL}_n(\mathcal{O}_{F,v})$, avec une représentation galoisienne associée *ordinaire* ; on étudie alors les déformations du même type. Cette étude ne joue plus de rôle dans la nouvelle approche de Taylor [**28**] et je n'en parlerai pas dans la suite de cet exposé.

b) En une place de S(B) : la déformation est du type « série discrète » (i.e. vérifiant les propriétés décrites en (3.5)).

c) Pour w une place au-dessus de $v \in Z - S$, la représentation est non ramifiée.

(Dans [**8**] d'autres types de places apparaissent aussi dont je ne dirai rien ici.)

Les déformations vérifiant les conditions imposées sont représentées par un anneau universel $\mathcal{R}_S$. On construit également une algèbre de Hecke localisée correspondante $\mathbb{T}_{\mathfrak{m},S}$, sur laquelle on a une représentation galoisienne :

$$r_{\mathfrak{m}} : \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(\mathbb{T}_{\mathfrak{m},S}) .$$

Par universalité de $\mathcal{R}_S$, on obtient ainsi un homomorphisme (dont il est facile de voir qu'il est surjectif) :

$$\mathcal{R}_S \to \mathbb{T}_{\mathfrak{m},S} .$$

Les théorèmes de relèvement de l'automorphie démontrés conjecturalement dans [**8**] résultent du théorème suivant (cas minimal), prouvé inconditionnellement :

THÉORÈME 5.1. — *L'homomorphisme $\mathcal{R}_\varnothing \to \mathbb{T}_{\mathfrak{m},\varnothing}$ est un isomorphisme.*

De ce théorème, si l'on admet une généralisation conjecturale (énoncée ci-dessous) du lemme d'Ihara, on déduit le résultat suivant, qui permet d'obtenir les résultats de relèvement voulus.

THÉORÈME 5.2. — *Admettons la conjecture (5.3) ci-dessous. Alors pour tout $S \subset Z$, l'homomorphisme $\mathcal{R}_S \to \mathbb{T}_{\mathfrak{m},S}$ est un isomorphisme.*

Formellement du moins, cela fonctionne donc comme dans le cas originel de Taylor-Wiles : on prouve tout d'abord le résultat dans le cas de ramification minimale (utilisant la lisseté de limites convenables des anneaux considérés), puis on augmente la ramification.

5.3. Un « lemme d'Ihara » conjectural

Reprenons les notations de (2.3) et (2.6) concernant les espaces de formes automorphes sur G et les algèbres de Hecke correspondantes. On se donne donc un ensemble T de mauvaises places comme en (2.6), et U un sous-groupe compact-ouvert dont les composantes sont toutes maximales hyperspéciales hors de T. On fixe aussi $v \in T$ non dans $S(B)$ et ne divisant pas ℓ ainsi qu'un isomorphisme entre $G(F_v)$ et $\mathrm{GL}_n(F_v)$ (cf. (2.1)).

On s'intéresse à l'espace $\mathcal{A}_{0,\{1\}}(U\,,\,\overline{k})$ des formes automorphes de poids 0 et de type trivial à valeurs dans $\overline{k}$ (clôture algébrique du corps fini k). Sur cet espace agit l'algèbre de Hecke correspondante $\mathbb{T}^T_{0,\{1\}}(U)$.

Supposons donnés un caractère $\lambda : \mathbb{T}^T_{0,\{1\}}(U) \to \overline{k}$ et $f \in \mathcal{A}_{0,\{1\}}(U\,,\,\overline{k})^\lambda$ une forme automorphe vecteur propre pour l'action de l'algèbre de Hecke, correspondant au caractère λ.

Notons $V \subset U$ le sous-groupe dont les composantes aux différentes places sont les mêmes que celles de U, sauf la composante en v qui est triviale.

$\mathcal{A}_{0,\{1\}}(U\,,\,\overline{k})$ est contenu dans l'espace $\mathcal{A}_{0,\{1\}}(V\,,\,\overline{k})$ constitué des applications :

$$h \,:\, G(F) \setminus G(\mathbb{A}_F^\infty) \to \overline{k}$$

qui sont invariantes à droite par V et par un sous-groupe ouvert (dépendant de h) de $G(F_v)$. Sur cet espace on a une action, par translation à droite, du groupe $G(F_v) \simeq \mathrm{GL}_n(F_v)$.

Notons $\langle G(F_v).f\rangle$ le sous-espace de $\mathcal{A}_{0,\{1\}}(V\,,\,\overline{k})$ engendré par les translatés de f.

D'autre part, au caractère λ correspond, comme expliqué au paragraphe 3, une représentation galoisienne

$$\overline{r}_\lambda \,:\, \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\overline{k})$$

(si on préfère c'est, à des identifications près, la représentation $\overline{r}_{\mathfrak{m}}$ associée à $\mathfrak{m} = \mathrm{Ker}\lambda$).

Nous dirons que f (ou λ) *n'est pas d'Eisenstein* si cette représentation est irréductible.

CONJECTURE 5.3. — *On se place sous les hypothèses précédentes. On suppose que f n'est pas d'Eisenstein. Soit $W \subset \langle G(F_v).f\rangle$ un sous-espace stable sous l'action de $G(F_v)$ et irréductible comme représentation de $G(F_v)$. Alors c'est une représentation **générique** de $\mathrm{GL}_n(F_v)$.*

Il me reste à expliquer ce qu'est une représentation générique définie sur $\overline{k}$. La définition est essentiellement la même que sur $\mathbb{C}$. Supposons fixé un caractère modulo ℓ non trivial $\psi : F_v \to \overline{k}$ du groupe additif F_v.

Soit $H \subset \mathrm{GL}_n(F_v)$ le sous-groupe constitué des matrices triangulaires supérieures à termes diagonaux tous égaux à 1. On définit un caractère $\Theta : H \to \overline{k}$ en associant à une matrice $(u_{i,j}) \in H$ l'élément $\Theta(u_{i,j}) = \psi(\sum u_{i-1,i})$.

Une représentation W de GL_n (définie sur $\overline{k}$) est dite *générique* s'il existe une forme linéaire L sur W qui vérifie l'identité pour $u \in H$ et $w \in W$:

$$L(u.w) = \Theta(u)\, L(w)\,.$$

Il est facile de voir que cette notion est indépendante du choix de Ψ. Si la condition est satisfaite, alors W est isomorphe à un sous-espace de l'induite $\mathrm{Ind}_H^{\mathrm{GL}_n(F_v)} \Theta$: cette réalisation constitue le *modèle de Whittaker* de W.

Remarque 5.4. — La conjecture porte uniquement sur les *sous-modules* irréductibles de $\langle G(F_v).f \rangle$. L'énoncé analogue pour les sous-quotients est faux.

Remarque 5.5. — Dans l'énoncé ci-dessus, on s'est limité à ne considérer que les formes de poids 0 et de type trivial. Si on suppose la conjecture vraie dans ce cadre, alors on peut prouver que le même énoncé est aussi valide pour des poids et des types plus généraux.

Remarque 5.6. — Sur $\mathbb{C}$, le résultat est vrai et résulte des propriétés du changement de base entre groupes unitaires et groupes linéaires, et de ce que les composantes de toute représentation automorphe cuspidale de GL_n sont génériques.

On peut démontrer assez simplement la conjecture pour $n = 2$ à partir du théorème d'approximation forte. Au-delà cela semble être une question très difficile.

5.4. L'approche de [28]

L'approche de [**28**] est, dans son principe, à l'opposé de celle de [**8**] : elle consiste à se placer au contraire d'emblée dans le cas où la différence enre la ramification de la représentation résiduelle et celle du relèvement considéré est la « pire » possible. En fait toute la ramification de $\overline{r}_{\mathfrak{m}}$ disparaît après une restriction convenable au groupe de Galois d'une extension résoluble (ce qui correspond du point de vue automorphe à un « changement de base »). De même on peut ainsi tuer la ramification d'un relèvement ℓ-adique, *sauf* la ramification unipotente et c'est dans ce cas que se place Taylor : on regarde les relèvements unipotents d'une représentation non ramifiée. Utilisant la « descente » dans la théorie du changement de base, il n'est pas difficile d'en déduire ensuite les résultats voulus de relèvement de l'automorphie.

5.5. — On conservera dans la suite les notations précédemment introduites, en particulier en ce qui concerne le groupe G. Désignant comme plus haut par $S(B)$ l'ensemble des places ramifiées de l'algèbre B, et par S_ℓ l'ensemble des places de F divisant ℓ, on notera $S_1 \neq \varnothing$ et R deux autres ensembles finis de places qui se décomposent dans E, disjoints entre eux et disjoints de la réunion $S(B) \cup S_1$. On notera T la réunion $S(B) \bigsqcup S_\ell \bigsqcup S_1 \bigsqcup R$. Pour chaque $v \in T$, on choisira $\tilde{v}$, l'une des deux places de E qui divisent v.

On notera U un sous-groupe compact comme ci-dessus, décomposé en produit de facteurs U_v ; on suppose que U_v est maximal hyperspécial pour chaque place non décomposée, et égal à $G(\mathcal{O}_{F,v})$ (donc aussi maximal) en chaque place décomposée $v \notin S_1 \bigsqcup R$. Finalement, pour $v \in R$, le groupe U_v coïncide avec le sous-groupe d'Iwahori $\mathrm{Iw}(\tilde{v})$ tandis que, pour $v \in S_1$, c'est le sous-groupe de congruence principal de niveau 1

$$U_v \;=\; \ker\bigl(\mathrm{GL}_n(\mathcal{O}_{E,\tilde{v}}) \to \mathrm{GL}_n(k(\tilde{v}))\bigr)\,.$$

Les éléments de S_1 jouent un rôle technique auxiliaire, en particulier pour assurer que le groupe U est « assez petit » (on suppose que, si p désigne la caractéristique résiduelle associée à une telle place, on a $[E(\zeta_p) : E] > n$).

On se donne un poids a supposé « petit » au sens de (3.4). On se donne également, en chaque place $v \in S(B)$, un diviseur m_v de n et une représentation $\tilde{r}_v$ de dimension n/m_w, en supposant que les réductions des $\tilde{r} \otimes \epsilon^i$ (avec $0 \leq i \leq m_v - 1$) sont absolument irréductibles et deux à deux non équivalentes.

On fixe enfin un idéal maximal $\mathfrak{m}$ de l'algèbre de Hecke $\mathbb{T}^T_{a,\{\rho_v\},\{1\}}(U)$, d'où comme en (3.1) une représentation de $\mathrm{Gal}(\overline{E}/E)$ sur le corps résiduel k, que l'on suppose absolument irréductible. Elle se prolonge donc en $\overline{r}_\mathfrak{m} : \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(k)$. Le caractère $\nu \circ \overline{r}_\mathfrak{m}$ coïncide avec $\bar{\epsilon}^{1-n}$ sur $\mathrm{Gal}(\overline{E}/E)$ et donc il est égal à $\epsilon^{1-n}\,\delta^{\mu_\mathfrak{m}}$ avec δ le caractère non trivial de $\mathrm{Gal}(E/F)$ et $\mu_\mathfrak{m} = 0$ ou 1.

On se ramène à supposer que sont satisfaites les hypothèses suivantes :

a) l'image par $\overline{r}_\mathfrak{m}$ de $\mathrm{Gal}(\overline{E}/F(\zeta_\ell))$ (pour ζ_ℓ une racine ℓ-ième primitive de 1) est assez grosse ;

b) pour tout $v \in R$, on a $\mathrm{N}v \equiv 1 \bmod \ell$ et la restriction de $\overline{r}_\mathfrak{m}$ au groupe de décomposition en $\tilde{v}$ est triviale ;

c) pour tout $v \in S_1$, $\overline{r}_\mathfrak{m}$ est non ramifiée en v et

$$H^0\left(\mathrm{Gal}\,(\overline{E}_{\tilde{v}}/E_{\tilde{v}})\,,\,(\mathrm{ad}\,\overline{r}_\mathfrak{m})(1)\right) \;=\; 0\,.$$

5.6. — Notons $\mathbb{T}$ la localisée en $\mathfrak{m}$ de l'algèbre $\mathbb{T}^T_{a,\{\rho_v\},\{1\}}(U)$. On considère les déformations de $\overline{r}_\mathfrak{m}$ en un homomorphisme $r_A : \mathrm{Gal}(\overline{E}/F) \to \mathcal{G}_n(A)$ telles que $\nu \circ r_A = \epsilon^{1-n}\delta^{\mu_\mathfrak{m}}$ et qui sont

i) « cristallines » en les places divisant ℓ ;

ii) comme expliqué en (3.5) pour les places de $S(B)$;

iii) telles qu'en chaque place $v \in R$ et σ dans le groupe d'inertie $I_{\tilde{v}}$, le polynôme caractéristique de $r_A(\sigma)$ soit égal à $(X-1)^n$.

L'espace de ces déformations est représenté par un anneau local complet $\mathcal{R}$. D'autre part, l'algèbre de Hecke $\mathbb{T}$ fournit une telle déformation et cela nous définit donc un homomorphisme surjectif :

$$\mathcal{R} \to \mathbb{T}\,.$$

Le résultat central de [**28**], dont résultent ensuite assez facilement les propriétés voulues de relèvement de l'automorphie, est le suivant :

THÉORÈME 5.7 ([**28**]). — *L'homomorphisme précédent induit un isomorphisme entre l'anneau réduit* $\mathcal{R}^{\mathrm{red}}$ *et* $\mathbb{T}$. *De plus, on a* $\mu_{\mathfrak{m}} \equiv n \bmod 2$.

6. LA MÉTHODE DE TAYLOR : PRÉLIMINAIRES

Le théorème (5.7) n'est pas accessible directement aux méthodes issues de celle de Taylor-Wiles, même en y incorporant l'ensemble des perfectionnements apportés depuis par plusieurs mathématiciens. L'idée fondamentale de [**28**] est de comparer la situation du théorème (5.7) à une autre qui, elle, relève de ces méthodes (à condition de faire intervenir des idées de Kisin), et telle que le problème de déformation considéré soit représentable par un anneau $\tilde{\mathcal{R}}$ qui coïncide avec $\mathcal{R}$ en réduction modulo λ.

L'idée de Kisin reprise ici par Taylor consiste à faire intervenir des anneaux de relèvements locaux (en certaines places données). Relèvements et non pas déformations, une nuance qui tient à des problèmes de représentabilité et qui nous oblige en retour à « repérer » (« framing ») nos anneaux globaux. On s'attend, du moins est-ce la philosophie sous-jacente, à ce que ces anneaux définis localement capturent l'essentiel de la singularité des anneaux globaux ; cette philosophie se trouvera confirmée ici, du moins sur une limite projective convenable des anneaux globaux considérés.

6.1. Les anneaux $\tilde{T}$ et $\tilde{\mathcal{R}}$

Supposons fixés, pour chaque $v \in R$, n caractères $\chi_{v,1}, \chi_{v,2}, \ldots, \chi_{v,n}$ de $k(v)^*$ (cf. (2.5)) à valeurs dans $\mathcal{O}^*$, tous d'ordre ℓ et deux à deux distincts (ce qui est possible puisque $\mathbf{N}v \equiv 1 \bmod \ell$ et que $\ell > n$). Les réductions modulo λ de ces caractères sont donc triviales. Il en résulte donc que les espaces associés de formes automorphes sur k coïncident avec ceux qui correspondent au caractère trivial :

$$\mathcal{A}_{a,\{\rho_v\},\{\chi_v\}}(U\,,\,k) = \mathcal{A}_{a,\{\rho_v\},\{1\}}(U\,,\,k)\,.$$

On a aussi une égalité analogue au niveau des algèbres de Hecke tensorisées par k. En particulier à l'idéal $\mathfrak{m}$ correspond un idéal maximal $\mathfrak{m}'$ de l'algèbre $\mathbb{T}^T_{a,\{\rho_v\},\{\chi_v\}}(U)$,

de telle sorte que le quotient soit égal à k et que la représentation galoisienne associée coïncide avec $\overline{r}_{\mathfrak{m}}$. Le localisé en $\mathfrak{m}'$ de $\mathbb{T}^T_{a,\{\rho_v\},\{\chi_v\}}(U)$ est noté $\tilde{\mathbb{T}}$.

On considère alors, comme en (5.6), les déformations $\tilde{r}_A$ de $\overline{r}_{\mathfrak{m}}$ sur des anneaux artiniens A, en remplaçant la condition (iii) par la suivante :

(iii′) en chaque place $v \in R$ et pour σ dans le groupe d'inertie, le polynôme caractéristique de $\tilde{r}_A(\sigma)$ est égal à $\prod_{j=1}^{n} \big(X - \chi_{v,j}(\sigma)\big)$ (où l'on a bien sûr noté $\chi_{v,j}$ le caractère du groupe d'inertie qui correpond à $\chi_{v,j}$ par l'isomorphisme de la théorie du corps de classes).

Comme plus haut, on peut vérifier qu'il existe un anneau local complet $\tilde{\mathcal{R}}$ universel pour ce problème de déformations. Par ailleurs, il est clair (cf. (3.4)) que l'on a une telle déformation sur l'algèbre de Hecke $\tilde{\mathbb{T}}$ d'où un homomorphisme surjectif :

$$\tilde{\mathcal{R}} \to \tilde{\mathbb{T}}\,.$$

Une remarque essentielle pour la suite est que, pour A une k-algèbre, les conditions (iii) et (iii′) sont équivalentes et donc que l'on peut identifier les réductions modulo λ de $\mathcal{R}$ et $\tilde{\mathcal{R}}$ (de façon compatible avec leurs projections sur les réductions de $\mathbb{T}$ et $\tilde{\mathbb{T}}$).

6.2. Anneaux de relèvements locaux et repérages globaux

Partons d'un corps local, qui sera ici le complété $E_{\tilde{v}} \simeq F_v$ pour $v \in R$, et d'une représentation à valeurs dans k du groupe de Galois de ce corps : ce sera ici la restriction (en fait *triviale* par hypothèse) $\overline{r}_{\mathfrak{m},\tilde{v}}$ de $\overline{r}_{\mathfrak{m}}$ au groupe de décomposition en $\tilde{v}$. Le problème de déformer cette représentation à une conjugaison près n'est pas représentable en général parce que nous avons trop d'automorphismes. C'est pourquoi l'on est conduit à considérer, de façon d'ailleurs plus élémentaire, le problème de relever tout simplement cette représentation : pour $\mathcal{A}$ un anneau local artinien de corps résiduel k, un tel relèvement consiste en la donnée d'un homomorphisme $\mathrm{Gal}(\overline{E}_{\tilde{v}}/E_{\tilde{v}}) \to \mathrm{GL}_n(\mathcal{A})$ de réduction $\overline{r}_{\mathfrak{m},\tilde{v}}$.

On vérifie que ce problème de relèvement est (pro-)représentable par un anneau local $\mathcal{L}_v^{\mathrm{univ}}$. Si on ne considère que les relèvements astreints à vérifier la condition (iii) de (5.6) (respectivement (iii′)) ci-dessus), alors on obtient deux anneaux locaux quotients de $\mathcal{L}_v^{\mathrm{univ}}$ et notés $\mathcal{L}_v$ (resp. $\tilde{\mathcal{L}}_v$).

Techniquement on n'a toutefois pas de foncteur associant un relèvement local à une déformation globale (puisque cette dernière n'est définie qu'à conjugaison près). On remédie à cela au moyen de la

DÉFINITION 6.1. — *Un relèvement de $\overline{r}_{\mathfrak{m}}$ (sur un anneau A de corps résiduel k), repéré (« framed ») aux places de R, consiste en la donnée* :

a) *d'un relèvement r de $\overline{r}_{\mathfrak{m}}$* ;

b) *pour chaque $v \in R$, d'un relèvement r_v de la représentation locale $\overline{r}_{\mathfrak{m},\tilde{v}}$ (plus exactement, de sa projection sur le facteur GL_n)* ;

c) *d'isomorphismes* $\alpha_v : r_v \to r_{|\mathrm{Gal}(\overline{E}_{\tilde{v}}/E_{\tilde{v}})}$ *de réduction l'identité.*

Une déformation repérée est une classe de conjugaison, sous $\ker\big(\mathrm{GL}_n(A) \to \mathrm{GL}_n(k)\big)$*, de relèvements repérés (un élément* γ *envoyant* r *sur* $\gamma r \gamma^{-1}$ *et* α_v *sur* $\gamma\alpha_v$*, les* r_v *demeurant inchangés).*

On peut considérer les problèmes de déformation globaux précédents, et ajouter dans les données un repérage aux places de R. Il n'est pas très difficile de voir que l'on peut représenter ces nouveaux foncteurs par des anneaux $\mathcal{R}^{\square}$ et $\tilde{\mathcal{R}}^{\square}$.

On a des foncteurs d'oubli qui, à une déformation repérée $(r, \{r_v\}_{v\in R}, \{\alpha_v\}_{v\in R})$, associent la déformation r et les relèvements r_v. Notant $\mathcal{L}_R$ le produit tensoriel complété (sur $\mathcal{O}$) des $\mathcal{L}_v$ (pour $v \in R$), on obtient ainsi des homomorphismes

$$\mathcal{L}_R \to \mathcal{R}^{\square} \text{ et } \mathcal{R} \to \mathcal{R}^{\square}.$$

La différence entre $\mathcal{R}$ et $\mathcal{R}^{\square}$ est facile à comprendre : l'objet universel sur $\mathcal{R}$ étant représenté par une application :

$$r^{\mathrm{univ}} : \mathrm{Gal}(\dot{\overline{E}}/F) \to \mathcal{G}_n(\mathcal{R})$$

(qui n'est pas canonique, seule sa classe de conjugaison l'est), on peut prendre simplement pour r_v la restriction de r^{univ}. La donnée d'un repérage en v revient alors à la donnée de la matrice $(X_{i,j,v})$ qui représente $\alpha_v - \mathbf{1}$ et dont les coefficients doivent appartenir à l'idéal maximal de $\mathcal{R}$. Notant $\mathcal{T}_R$ l'anneau des séries formelles sur $\mathcal{O}$ en les $(n^2\,\sharp R)$ indéterminées $X_{i,j,v}$, on a donc un isomorphisme (non canonique) :

$$\mathcal{R}\hat{\otimes}_{\mathcal{O}}\mathcal{T}_R \simeq \mathcal{R}^{\square}.$$

De même en ce qui concerne $\tilde{\mathcal{R}}$, on a (en posant $\tilde{\mathcal{L}}_R = \hat{\otimes}_{v\in S}\tilde{\mathcal{L}}_v$) des homomorphismes $\tilde{\mathcal{L}}_R \to \tilde{\mathcal{R}}^{\square}$ et $\tilde{\mathcal{R}} \to \tilde{\mathcal{R}}^{\square}$, ainsi qu'un isomorphisme $\tilde{\mathcal{R}}\hat{\otimes}_{\mathcal{O}}\mathcal{T}_R \simeq \tilde{\mathcal{R}}^{\square}$.

6.3. Propriétés des anneaux de relèvements locaux

L'étude des anneaux de relèvements locaux introduits ci-dessus joue un rôle fondamental dans [**28**]. C'est un problème tout à fait concret : du fait que la représentation résiduelle dont on part est triviale et comme on déforme en caractéristique résiduelle ℓ différente de celle de $E_{\tilde{v}}$, un tel relèvement est *modérément ramifié*, et correspond donc à la donnée de deux matrices inversibles de taille n : Φ (image d'un élément de Frobenius fixé) et Σ (image d'un générateur fixé σ du groupe d'inertie modérée), toutes deux de réduction l'identité, et vérifiant la relation : $\Phi\,\Sigma\Phi^{-1} = \Sigma^q$ (avec q le cardinal du corps résiduel en $\tilde{v}$). Une condition supplémentaire porte sur le polynôme caractéristique de Σ, qui doit être égal à $(X-1)^n$ dans le cas de l'anneau $\mathcal{L}_v$ et à $\prod(X - \chi_{v,j}(\sigma))$ pour $\tilde{\mathcal{L}}_v$.

PROPOSITION 6.2 ([**28**]). — *On suppose $\ell > n$. Soit $v \in R$.*

(a) *Les schémas* $\operatorname{Spec} \mathcal{L}_v$ *et* $\operatorname{Spec} \tilde{\mathcal{L}}_v$ *sont de même dimension de Krull* $1 + n^2$ *et équidimensionnels : cette dimension est aussi celle de chaque composante irréductible. De plus aucune de ces composantes n'est contenue dans la fibre spéciale.*

(b) $\operatorname{Spec} \tilde{\mathcal{L}}_v$ *est irréductible.*

(c) *Chaque composante irréductible de la fibre spéciale* $\operatorname{Spec}(\mathcal{L}_v \otimes_{\mathcal{O}} k)$ *est contenue dans une unique composante irréductible de* $\operatorname{Spec} \mathcal{L}_v$ *et réciproquement toute composante irréductible de* $\operatorname{Spec} \mathcal{L}_v$ *contient une composante irréductible de la fibre spéciale.*

Ces résultats sont démontrés en étudiant les schémas analogues $\mathcal{M}$ et $\tilde{\mathcal{M}}$ représentant les couples de matrices (Σ, Φ) (avec Φ inversible) vérifiant les relations précédentes (mais sans la condition de se réduire sur l'identité) puis en localisant.

En ce qui concerne $\mathcal{M}$, en appliquant le logarithme à Σ (rappelons que $\ell > n$), on peut prouver que le schéma réduit $\mathcal{M}^{\mathrm{red}}$ est isomorphe au schéma réduit $\mathcal{N}^{\mathrm{red}}$, où $\mathcal{N}$ classifie les couples de matrices (Φ, N) avec Φ inversible, N de polynôme caractéristique X^n et vérifiant la relation $\Phi N \Phi^{-1} = qN$. On peut alors montrer que les composantes irréductibles de $\mathcal{N}^{\mathrm{red}}$ correspondent aux *partitions* σ de l'entier n et qu'il en est de même pour la fibre spéciale : on regarde en gros l'adhérence du sous-schéma constitué des couples (Φ, N) comme ci-dessus et tels que la taille des blocs de Jordan associés à N corresponde à σ (cela a une signification claire sur un corps et la difficulté consiste à donner encore un sens à ces notions au-dessus de $\mathcal{O}$).

Pour ce qui est de $\tilde{\mathcal{M}}$, on remarque que le polynôme caractéristique de Σ divise $X^\ell - 1$ et, comme on suppose que $q \equiv 1 \bmod \ell$, ce dernier divise $X^q - X$. On peut donc voir plus simplement $\tilde{\mathcal{M}}$ comme le schéma qui classifie les couples de matrices inversibles (Σ, Φ) vérifiant $\Sigma\Phi = \Phi\Sigma$ et tel que le polynôme caractéristique de Σ soit comme plus haut. Il n'est pas difficile alors de voir que la fibre générique est isomorphe à $\mathrm{GL}_n/T_n \times T_n$ (avec T_n le tore formé des matrices diagonales) par l'application :

$$\begin{aligned} \mathrm{GL}_n/T_n \times T_n &\longrightarrow \tilde{\mathcal{M}} \\ (gT_n, t) &\longmapsto (gtg^{-1}, gd_0g^{-1}), \end{aligned}$$

où d_0 désigne la matrice diagonale formée avec les $\chi_{v,j}(\sigma)$. Cette fibre générique est donc lisse et connexe de la dimension voulue.

D'autre part, la fibre spéciale est isomorphe au schéma $\tilde{N}_k$ sur k qui classifie les couples de matrices (Φ, N) avec Φ inversible, N de polynôme caractéristique X^n et vérifiant la relation $\Phi N = N\Phi$ (il suffit de prendre $N = \Sigma - 1$). Comme plus haut, les composantes irréductibles de $\tilde{N}_k$ correspondent aux partitions de n. Pour prouver que $\tilde{\mathcal{M}}$ est irréductible, on montre que chacune des composantes de la fibre spéciale admet un point qui n'appartient pas aux autres et qui accepte de se relever à la fibre générique.

Enfin, pour la localisation, on a besoin dans [**28**] d'autres résultats dont je ne parlerai pas ici, portant sur la normalisée de $\tilde{\mathcal{M}}^{\mathrm{red}}$.

De la proposition précédente, on déduit par produit l'analogue pour les anneaux $\mathcal{L}_R$ et $\tilde{\mathcal{L}}_R$:

PROPOSITION 6.3. — *On suppose toujours $\ell > n$.*

(a) *Les schémas* $\operatorname{Spec}\mathcal{L}_R$ *et* $\operatorname{Spec}\tilde{\mathcal{L}}_R$ *sont équidimensionnels de même dimension de Krull* $1 + n^2 \sharp R$. *De plus, aucune de leurs composantes irréductibles n'est contenue dans la fibre spéciale.*

(b) $\operatorname{Spec}\tilde{\mathcal{L}}_R$ *est irréductible.*

(c) *Chaque composante irréductible de la fibre spéciale* $\operatorname{Spec}(\mathcal{L}_R \otimes_{\mathcal{O}} k)$ *est contenue dans une unique composante irréductible de* $\operatorname{Spec}\mathcal{L}_R$ *et, réciproquement, toute composante irréductible de* $\operatorname{Spec}\mathcal{L}_R$ *contient une composante irréductible de la fibre spéciale.*

6.4. Modules quasi-fidèles

C'est une notion d'algèbre commutative introduite pour les besoins de [**28**].

Soient A une $\mathcal{O}$-algèbre locale noethérienne et M un A-module de type fini.

DÉFINITION 6.4. — *On dit que M est un module quasi-fidèle si l'une des trois conditions équivalentes suivantes est satisfaite* :

- *l'idéal annulateur de M est nilpotent*;
- *le point générique de chaque composante irréductible de* $\operatorname{Spec} A$ *appartient au support de M* ;
- *le support de M est égal à* $\operatorname{Spec} A$.

Pour A réduit, « quasi-fidèle » équivaut à « fidèle ». C'est une notion un peu plus maniable que la fidélité :

PROPOSITION 6.5. — (1) *Si M est quasi-fidèle et si I est un idéal de A, alors M/IM est quasi-fidèle sur A/I. Si J est un idéal contenant I et tel que l'action sur M/IM se factorise via A/J, alors J est contenu dans le radical $\sqrt{I}$ et M/IM est un module quasi-fidèle sur A/J.*

(2) *Supposons que chaque composante irréductible de la fibre spéciale* $\operatorname{Spec}(A \otimes_{\mathcal{O}} k)$ *est contenue dans une unique composante irréductible de* $\operatorname{Spec} A$ *et, réciproquement, que toute composante irréductible de* $\operatorname{Spec} A$ *contient une composante irréductible de la fibre spéciale. Supposons que M est un A-module qui est sans torsion sur $\mathcal{O}$ et tel que $M/\lambda M$ soit quasi-fidèle sur $A/\lambda A$. Alors M est un A-module quasi-fidèle.*

On utilisera (voir (7.5) ci-dessous) cette notion et ces résultats dans l'optique suivante : notons $\mathcal{A} = \mathcal{A}_{a,\{\rho_v\},\{1\}}(U, \mathcal{O})_{\mathfrak{m}}$ le localisé en $\mathfrak{m}$ de l'espace des formes automorphes. Via l'homomorphisme (surjectif) $\mathcal{R} \to \mathbb{T}$, on peut voir $\mathcal{A}$ comme un $\mathcal{R}$-module. On va, dans la suite, montrer qu'il est quasi-fidèle et le théorème 4.2 en résultera alors : en effet si $\mathcal{R}^{\mathrm{red}} \to \mathbb{T}$ n'était pas bijectif, il définirait un sous-schéma fermé strict de $\mathrm{Spec}\mathcal{R}$ qui supporterait $\mathcal{A}$.

7. L'IDÉE DE LA PREUVE DU THÉORÈME 4.2

7.1. Places de Taylor-Wiles

Une idée invariablement présente tant dans la méthode originelle de Taylor-Wiles que dans les développements ultérieurs consiste à ajouter un ensemble fini bien choisi (dépendant d'un entier N) de places où l'on va autoriser nos déformations à se ramifier d'une certaine façon. Ceci a pour effet de stabiliser, en un certain sens, le problème de déformation correspondant, en tuant des singularités parasites. Plus précisément, on crée de façon artificielle une limite projective (pour $N \to \infty$) des anneaux de déformation obtenus et cette limite est alors aussi peu ramifiée que possible.

Plaçons-nous sous les notations et les hypothèses de (5.5). Une proposition semblable à la suivante était déjà prouvée et utilisée dans [**8**]. Il s'agit de résultats d'un genre maintenant assez habituel et qui reposent sur des calculs de groupes de cohomologie galoisienne locaux et globaux, et de groupes de Selmer. L'idée sous-jacente est que le nombre minimal de générateurs des anneaux de déformations est donné par la dimension d'un H^1 (prenant en compte les structures aux places ramifiées) à valeurs dans l'adjointe de la représentation résiduelle que l'on déforme. La preuve utilise la dualité de Poitou-Tate et des formules de calcul de la caractéristique d'Euler-Poincaré, ainsi que le théorème de Čebotarev. Voir par exemple [**25**] où l'on explique les idées analogues dans le travail originel de Wiles et Taylor-Wiles.

PROPOSITION 7.1 ([**8**]). — *Il existe un entier u tel que les propriétés suivantes soient satisfaites. On pose $u' = u - n[F : \mathbb{Q}](1 - (-1)^{\mu_{\mathfrak{m}}-n})$ (cf. (5.5) pour la définition de $\mu_{\mathfrak{m}}$).*

Pour chaque entier $N \geq 1$ il existe :

• *un ensemble Q_N de cardinal u de places finies de F, disjoint de $S(B) \bigsqcup S_\ell \bigsqcup S_1 \bigsqcup R$. Chaque $v \in Q_N$ est décomposée dans E et vérifie $\mathbf{N}v \equiv 1 \bmod \ell^N$.*

• *Pour chaque $v \in Q_N$ et $\tilde{v}$ une place fixée de E au-dessus de v, il existe une décomposition comme en (3.7), associée à une racine simple $a_{\tilde{v}}$ du polynôme caractéristique de $\overline{r}_{\mathfrak{m}}(\phi_{\tilde{v}})$:*

$$(\overline{r}_{\mathfrak{m}})_{|\mathrm{Gal}(\overline{E}_{\tilde{v}}/E_{\tilde{v}})} = \overline{\psi}_v \oplus \overline{s}_v$$

et telle que $\overline{\psi}_v$ ne soit pas isomorphe à un sous-quotient de $\overline{s}_v$.

• *Soit $\mathcal{R}^{\square}_{Q_N}$ l'anneau universel de déformations repérées définies en rajoutant au problème de déformation considéré précédemment les places de Q_N : on autorise les relèvements à se ramifier en $v \in Q_N$, mais en imposant localement en ces places la condition mentionnée en (3.7), c'est-à-dire qu'il existe un relèvement local $\psi_v \oplus s_v$ en $\tilde{v}$ de la décomposition $\overline{\psi}_v \oplus \overline{s}_v$.*

Alors $\mathcal{R}^{\square}_{Q_N}$ peut être engendré comme algèbre sur $\mathcal{L}_R$ par u' éléments.

• *Soit $\tilde{\mathcal{R}}^{\square}_{Q_N}$ défini de façon analogue à partir de $\tilde{\mathcal{R}}^{\square}$. Alors $\tilde{\mathcal{R}}^{\square}_{Q_N}$ peut être engendré comme algèbre sur $\tilde{\mathcal{L}}_R$ par u' éléments.*

Remarquons que le théorème (5.7) que nous voulons prouver entraîne que $u' = u$ (puisque $\mu_{\mathfrak{m}}$ a la même parité que n). En réalité c'est cette égalité entre u et u' que l'on prouvera directement au cours de la démonstration, et l'égalité $\mu_{\mathfrak{m}} = (-1)^n$ en résultera.

7.2. — Supposons désormais choisi pour chaque N un tel ensemble Q_N ; on note $U_1(Q_N)$ le sous-groupe dont les composantes sont celles de U aux places $v \notin Q_N$, et égales à $U_1(v)$ pour $v \in Q_N$ (cf. (2.7)). On considère l'algèbre de Hecke $\mathbb{T}^T_{a,\{\rho_v\},\{1\}}(U_1(Q_N))_{\mathfrak{m}}$, sur laquelle on a une déformation $r_{\mathfrak{m},N}$ de $\overline{r}_{\mathfrak{m}}$. Le polynôme caractéristique $P_{\tilde{v}}$ de $r_{\mathfrak{m}}(\phi_{\tilde{v}})$ admet d'après le lemme de Hensel une unique racine simple $A_{\tilde{v}}$ qui relève $a_{\tilde{v}}$. Posons $P_{\tilde{v}}(X) = (X - A_{\tilde{v}})Q_{\tilde{v}}(X)$; on introduit alors un espace de formes automorphes

$$\mathcal{A}_N = \Big(\prod_{v \in Q_N} (Q_{\tilde{v}}(V_{\varpi_{\tilde{v}}})) \Big) \mathcal{A}_{a,\{\rho_v\},\{1\}}\big(U_1(Q_N)\,,\,\mathcal{O}\big)_{\mathfrak{m}}\,.$$

On montre que $\mathcal{A}_N$ est un facteur direct de $\mathcal{A}_{a,\{\rho_v\},\{1\}}\big(U_1(Q_N)\,,\,\mathcal{O}\big)_{\mathfrak{m}}$ sur lequel $V_{\varpi_{\tilde{v}}}$ agit via $A_{\tilde{v}}$. D'autre part, il existe pour chaque $v \in Q_N$ un homomorphisme

$$V_{\tilde{v}} : E^*_{\tilde{v}} \to \mathbb{T}^T(\mathcal{A}_N)^*$$

qui donne, via l'isomorphisme de la théorie du corps de classes, l'action du groupe de Galois local sur un facteur ψ_v relevant $\overline{\psi}_v$. Ici $\mathbb{T}^T(\mathcal{A}_N)$ désigne le quotient de l'algèbre de Hecke qui agit effectivement sur $\mathcal{A}_N$.

Notons Δ_N le produit des ℓ-sous-groupes de Sylow des groupes d'inertie $I_{\tilde{v}}$ pour les $v \in Q_N$. Ce groupe Δ_N s'identifie aussi au produit des ℓ-sous-groupes de Sylow des $k(\tilde{v})^*$ et l'on a un homomorphisme, donné par le déterminant de la représentation universelle :

$$\Delta_N \to \mathcal{R}^*_{Q_N}.$$

Comme ψ_v est le seul facteur éventuellement ramifié de $r_{\mathfrak{m},N}$, sa restriction au groupe d'inertie correspond au déterminant de $r_{\mathfrak{m},N}$; le produit des restrictions aux $\mathcal{O}_{E,\tilde{v}}^*$ des $V_{\tilde{v}}$ peut se factoriser comme le composé :

$$\prod_{v\in Q_N} \mathcal{O}_{E,\tilde{v}}^* \to \prod_{v\in Q_N} k(\tilde{v})^* \to \Delta_N \to \mathcal{R}_{Q_N}^* \to \mathbb{T}^T(\mathcal{A}_N)^* .$$

Enfin on vérifie ([**8**]) que $\mathcal{A}_N$ est un $\mathcal{O}[\Delta_N]$ module libre et qu'on a une identification entre le module des coïnvariants $(\mathcal{A}_N)_{\Delta_N}$ et $\mathcal{A} = \mathcal{A}_{a,\{\rho_v\},\{1\}}$.

De même on construit $\tilde{\mathcal{A}}_N$ à partir de $\tilde{\mathcal{A}}_{a,\{\rho_v\},\{\chi_v\}}\big(U_1(Q_N)\,,\,\mathcal{O}\big)_{\mathfrak{m}}$. L'analogue de tout ce qui vient d'être dit est vrai pour $\tilde{\mathcal{A}}_N$, $\tilde{\mathcal{R}}_{Q_N}$.

7.3. — Comme annoncé plus haut, on crée de façon artificielle des limites projectives des anneaux précédents lorsque N tend vers l'infini, ainsi également que des modules ; cette idée que les modules devaient être pris en compte aussi bien que les anneaux eux-mêmes est en substance l'amélioration conceptuelle apportée par Diamond et Fujiwara à la méthode originelle : voir [**9**] ou bien [**12**].

Je renvoie à [**28**] pour les détails de la construction, me bornant ici à expliquer quel est l'argument central de l'article.

On introduit des modules de formes automorphes « repérées » simplement par produit tensoriel

$$\mathcal{A}_N^{\square} = \mathcal{A}_N \otimes_{\mathcal{R}_{Q_N}} \mathcal{R}_{Q_N}^{\square} \qquad \tilde{\mathcal{A}}_N^{\square} = \tilde{\mathcal{A}}_N \otimes_{\tilde{\mathcal{R}}_{Q_N}} \tilde{\mathcal{R}}_{Q_N}^{\square} ,$$

où la structure de $\mathcal{R}_{Q_N}$ (resp. $\tilde{\mathcal{R}}_{Q_N}$)–module s'obtient via l'homomorphisme vers l'algèbre de Hecke correspondante.

Notons $\Delta_\infty = \mathbb{Z}_\ell^u$ et $S_\infty = \mathcal{T}_R[[\Delta_\infty]]$ (une algèbre de séries formelles en $u + n^2\sharp R$ indéterminées, dont u correspondent aux places de Taylor-Wiles et $n^2\sharp R$ aux repérages aux places de R).

Comme Δ_N est un produit de u groupes qui sont cycliques d'ordres des puissances de ℓ, on peut, pour chaque N, choisir une surjection $\Delta_\infty \to \Delta_N$, d'où un homomorphisme Δ_∞ dans $\mathcal{R}_{Q_N}^*$ et un homomorphisme d'algèbres $\mathcal{O}[[\Delta_\infty]] \to \mathcal{R}_{Q_N}$. De même avec l'anneau $\tilde{\mathcal{R}}_{Q_N}$.

D'autre part, on peut comme en (5.3) fixer des isomorphismes

$$\mathcal{R}_{Q_N}\hat{\otimes}_{\mathcal{O}}\mathcal{T}_R \simeq \mathcal{R}_{Q_N}^{\square} \text{ et } \tilde{\mathcal{R}}_{Q_N}\hat{\otimes}_{\mathcal{O}}\mathcal{T}_R \simeq \tilde{\mathcal{R}}_{Q_N}^{\square}.$$

D'où finalement des homomorphismes de S_∞ dans $\mathcal{R}_{Q_N}^{\square}$ et dans $\tilde{\mathcal{R}}_{Q_N}^{\square}$. Si $\mathfrak{a}$ est l'idéal d'augmentation de S_∞, le quotient de $\mathcal{R}_{Q_N}^{\square}$ par l'idéal engendré par $\mathfrak{a}$ s'identifie à $\mathcal{R}$ car on a successivement « tué » le repérage et pris les coïnvariants par Δ_N. De même, on récupère $\mathcal{R}_{Q_N}$ à partir du noyau $\mathfrak{a}_N$ de la surjection de S_∞ sur $\mathcal{T}_R[[\Delta_N]]$. Des propriétés analogues valent avec les anneaux $\tilde{\mathcal{R}}_{Q_N}^{\square}$.

7.4. — Puisqu'en vertu de la proposition (7.1) nos anneaux de déformations repérées $\mathcal{R}^{\square}_{Q_N}$ sont engendrés sur $\mathcal{L}_R$ par u' éléments, on peut créer une limite artificielle de ces anneaux en considérant l'anneau de séries formelles

$$\mathcal{R}^{\square}_{\infty} = \mathcal{L}_R[[Y_1, Y_2 \cdots Y_{u'}]]$$

et en choisissant des homomorphismes surjectifs

$$\mathcal{R}^{\square}_{\infty} \longrightarrow \mathcal{R}^{\square}_{Q_N}.$$

On définit de même un anneau $\tilde{\mathcal{R}}^{\square}_{\infty}$ de séries formelles sur $\tilde{\mathcal{L}}_R$ en u' indéterminées et l'on fixe des homomorphismes surjectifs $\tilde{\mathcal{R}}^{\square}_{\infty} \to \tilde{\mathcal{R}}^{\square}_{Q_N}$.

Je renvoie à [**28**] où l'on explique comment manufacturer une « limite » $\mathcal{A}^{\square}_{\infty}$ des $\mathcal{A}^{\square}_{N}$ de façon compatible avec les choix liés à S_∞ et $\mathcal{R}^{\square}_{\infty}$. On l'obtient plus précisément comme une limite projective de quotients $\mathcal{A}^{\square}_{M_i}/\mathfrak{b}_{N_i}$, associés à une famille d'idéaux $\mathfrak{b}_{N_i}$ de S_∞, et qui sont des $\mathcal{R}^{\square}_{\infty}\hat{\otimes}\big(S_\infty/\mathfrak{b}_{N_i}\big)$-modules, finis et libres sur $S_\infty/\mathfrak{b}_{N_i}$.

Le résultat obtenu $\mathcal{A}^{\square}_{\infty}$ est un module sur $\mathcal{R}^{\square}_{\infty}\hat{\otimes}S_\infty$, fini et libre sur S_∞, et tel que l'action de S_∞ se factorise par un homomorphisme vers $\mathcal{R}^{\square}_{\infty}$. La construction fournit de plus un homomorphisme surjectif

$$\mathcal{R}^{\square}_{\infty} \to \mathcal{R}$$

et un isomorphisme entre $\mathcal{A}^{\square}_{\infty} \otimes_{S_\infty} (S_\infty/\mathfrak{a})$ et $\mathcal{A}$ compatible avec l'homomorphisme composé $\mathcal{R}^{\square}_{\infty} \to \mathcal{R} \to \mathbb{T}$.

De même, on obtient $\tilde{\mathcal{A}}^{\square}_{\infty}$, un homomorphisme $\tilde{\mathcal{R}}^{\square}_{\infty} \to \tilde{\mathcal{R}}$ et $\tilde{\mathcal{A}}^{\square}_{\infty} \otimes_{S_\infty} (S_\infty/\mathfrak{a}) \simeq \tilde{\mathcal{A}}$ vérifiant des propriétés analogues.

Enfin il est possible d'effectuer toutes les constructions précédentes de telle sorte que les deux situations coïncident en réduction modulo λ.

Remarque 7.2. — Utilisant la proposition (6.3), on voit que les anneaux $\mathcal{R}^{\square}_{\infty}$ et $\tilde{\mathcal{R}}^{\square}_{\infty}$ sont équidimensionnels de même dimension $1 + n^2\sharp R + u'$. Remarquer aussi que la dimension de l'anneau S_∞ est, elle, égale à $1+n^2\sharp R+u$ avec $u' = u$ ou $u' < u$ suivant que $\mu_{\mathfrak{m}}$ a ou non la même parité que n.

7.5. Fin de la preuve du théorème 4.2

Comme expliqué en (6.4), notre but est de montrer que $\mathcal{A}$ est un $\mathcal{R}$-module quasi-fidèle. Il suffit de voir que $\mathcal{A}^{\square}_{\infty}$ est quasi-fidèle sur $\mathcal{R}^{\square}_{\infty}$ (on prend ensuite les quotients par l'idéal engendré par $\mathfrak{a}$ et on utilise la proposition (6.5)).

Montrons tout d'abord l'analogue de ce résultat pour le $\tilde{\mathcal{R}}^{\square}_{\infty}$-module $\tilde{\mathcal{A}}^{\square}_{\infty}$: étant libre sur S_∞, ce module est de profondeur au moins égale à $1 + n^2\sharp R + u$. Son support dans $\mathrm{Spec}\tilde{\mathcal{R}}^{\square}_{\infty}$ est donc de dimension $\geq 1 + n^2\sharp R + u$. Puisque la dimension de $\mathrm{Spec}(\tilde{\mathcal{R}}^{\square}_{\infty})$ est égale à $1+n^2\sharp R+u'$, il est donc impossible que u' soit $< u$ et on trouve donc l'égalité voulue entre u et u' (ce qui équivaut au résultat sur la parité de $\mu_{\mathfrak{m}}$).

Utilisant l'irréductibilité de $\mathrm{Spec}(\tilde{\mathcal{R}}_\infty^\square)$ donnée par la proposition (6.3), on voit aussi que le support de $\tilde{\mathcal{A}}_\infty^\square$ est égal à $\mathrm{Spec}(\tilde{\mathcal{R}}_\infty^\square)$ tout entier.

Le même argument ne s'applique pas directement à $\mathcal{A}_\infty^\square$ car $\mathrm{Spec}(\mathcal{R}_\infty^\square)$ n'est pas irréductible en général et rien ne s'opposerait donc a priori à ce que $\mathcal{A}_\infty^\square$ soit concentré sur une réunion de composantes irréductibles.

Mais la quasi-fidélité de $\tilde{\mathcal{A}}_\infty^\square$ sur $\tilde{\mathcal{R}}_\infty^\square$ entraîne, en vertu de la proposition (6.5), que $\tilde{\mathcal{A}}_\infty^\square/\lambda\tilde{\mathcal{A}}_\infty^\square$ est quasi-fidèle sur $\tilde{\mathcal{R}}_\infty^\square/\lambda\tilde{\mathcal{R}}_\infty^\square$.

Du fait que les deux situations coïncident modulo λ, on a donc la même propriété de quasi-fidélité de $\mathcal{A}_\infty^\square/\lambda\mathcal{A}_\infty^\square$ sur $\mathcal{R}_\infty^\square/\lambda\mathcal{R}_\infty^\square$. Une seconde application de la proposition (6.5), compte tenu de la proposition (6.3)(c), nous permet alors de conclure que $\mathcal{A}_\infty^\square$ est quasi-fidèle sur $\mathcal{R}_\infty^\square$. Cela prouve donc le résultat principal de [**28**].

8. UNE FAMILLE D'HYPERSURFACES

8.1. — Dans la suite, on suppose que n est un entier *pair*.

Soit Y l'hypersurface de $\mathbb{P}^n \times \mathbb{P}^1$ constituée des couples de points de coordonnées homogènes $(X_0, X_1, \ldots, X_{n+1})$, (s,t) vérifiant l'équation

$$s(X_0^{n+1} + X_1^{n+1} + X_2^{n+1} + \cdots + X_n^{n+1}) = (n+1)\, t\, X_0 X_1 X_2 \cdots X_n\,.$$

On notera π la projection de Y sur $\mathbb{P}^1$ et $Y_{(s,t)}$ la fibre au-dessus du point (s,t). Pour simplifier les notations, on notera dans la suite ∞ le point de $\mathbb{P}^1$ de coordonnées homogènes $(0,1)$, et on paramétrera la droite affine complémentaire par t en posant $s=1$. La fibre au-dessus de $(1,t)$ sera donc notée Y_t.

Cette famille d'hypersurfaces est définie sur $\mathbb{Q}$ et même sur les entiers (disons, sur $\mathbb{Z}[\frac{1}{n+1}]$ si on veut avoir des propriétés raisonnables). Elle a été étudiée depuis longtemps par différents mathématiciens, en particulier par Dwork. L'essentiel de son étude se fait sur $\mathbb{C}$.

On voit facilement que Y est lisse au-dessus de l'ouvert

$$T_0 = \mathbb{P}^1 - (\{\infty\} \cup \mu_{n+1})\,,$$

où μ_{n+1} désigne l'ensemble des racines de l'unité d'ordre $(n+1)$. Au-dessus des points ζ de μ_{n+1} la variété Y_ζ présente des singularités quadratiques ordinaires. Remarquer que Y_0 est une hypersurface de Fermat.

Notons $H_0 \subset \mu_{n+1}^{n+1}$ le sous-groupe constitué des $(\eta_0, \eta_1, \ldots, \eta_n)$ vérifiant $\prod \eta_i = 1$. Ce groupe H_0 agit sur chaque fibre Y_t par

$$(\eta_0, \eta_1, \ldots, \eta_n).(X_0, X_1, \ldots, X_{n+1}) = (\eta_0 X_0, \eta_1 X_1, \ldots, \eta_n X_n)$$

(action qui se factorise par le quotient de H_0 par le sous-groupe diagonal).

On s'intéresse aux invariants sous H_0 dans la cohomologie d'ordre $n-1$ des fibres Y_t. Suivant que l'on regarde la cohomologie entière, ou à valeurs dans $\mathbb{Z}/N\mathbb{Z}$ (N un entier premier à $n+1$), ou ℓ-adique ($\ell \nmid (n+1)$), ou enfin de de Rham, on notera les ensembles d'invariants correspondants par

$$V_t\,,\ \text{resp.}\ V[N]_t\,,\ \text{resp.}\ V_{\ell,t}\,,\ \text{resp.}\ V_{\mathrm{DR},t}\,.$$

Les trois premiers constituent des systèmes locaux sur T_0. Le quatrième est muni de la filtration de Hodge, qui varie holomorphiquement avec $t \in T_0$.

Remarquer que Y_0 admet une action du groupe plus gros $H = \mu_{n+1}^{n+1}$ et donc que le quotient $H/H_0 \simeq \mu_{n+1}$ agit sur les espaces correspondants, à $t = 0$. Cette action fournit un outil pour décomposer et étudier plus précisément les groupes de cohomologie précédents en $t = 0$ (Deligne).

On peut d'ailleurs utiliser cette fibre en 0 pour prouver la

PROPOSITION 8.1. — *Pour $t \in T_0$, les espaces $V_t \otimes \mathbb{Q}$, (resp. $V[N]_t$, $V_{\ell,t}$, $V_{\mathrm{DR},t}$) sont libres de rang n (respectivement sur $\mathbb{Q}$, $\mathbb{Z}/N\mathbb{Z}$, $\mathbb{Q}_\ell$, $\mathbb{C}$). Les poids qui interviennent dans la filtration de Hodge de $V_{\mathrm{DR},t}$ sont $0, 1, 2, \ldots, n-1$, chacun apparaissant avec multiplicité 1 (autrement dit les bidegrés de Hodge sont les $(p, n-1-p)$, avec p variant de 0 à $n-1$).*

8.2. — Comme $n-1$ est supposé impair le cup-produit induit sur les espaces précédents une forme bilinéaire alternée, qui est non dégénérée (et même parfaite en ce qui concerne les stuctures entières) :

$$\begin{aligned} V_t \times V_t &\to \mathbb{Z} \\ V[N]_t \times V[N]_t &\to (\mathbb{Z}/N\mathbb{Z})\,(1-n) \\ V_{\ell,t} \times V_{\ell,t} &\to \mathbb{Q}_\ell\,(1-n). \end{aligned}$$

Donnons-nous un point complexe $t \in T_0(\mathbb{C})$. Le groupe fondamental $\pi_1\,(T_0(\mathbb{C})\,,\,t)$ agit sur la fibre V_t (opération de monodromie) en respectant la forme alternée, d'où un homomorphisme dans le groupe symplectique sur $\mathbb{Z}$ correspondant

$$\pi_1\,(T_0(\mathbb{C})\,,\,t) \to \mathrm{Sp}\,(V_t)\,.$$

On a alors :

THÉORÈME 8.2. — *L'image de l'homomorphisme précédent est Zariski-dense dans le groupe symplectique* $\mathrm{Sp}\,(V_t \otimes \mathbb{C})$.

Ce théorème devrait être extractible des travaux de Katz ([**19**]) convenablement décryptés. Les auteurs de [**8**] en donnent une preuve directe, en calculant la monodromie autour des différents points au-dessus desquels le morphisme π n'est pas lisse ; ce calcul est facile au-dessus des points de μ_{n+1} car les singularités sont quadratiques

ordinaires et la théorie de Picard-Lefschetz s'applique. Il est plus compliqué autour de ∞ et nécessite d'étudier l'équation de Picard-Fuchs dans un voisinage. Une fois ces calculs effectués, on les transfère sur $\mathbb{P}^1 - \{0\,,\,1\,,\,\infty\}$ par descente via le morphisme $t \to t^{n+1}$ et on utilise alors des résultats de Beukers et Heckman ([**2**]) relatifs aux groupes hypergéométriques.

En partant du théorème ci-dessus, on peut ensuite prouver le suivant qui joue un rôle fondamental dans [**15**] :

THÉORÈME 8.3. — *Il existe une constante $C(n)$ (ne dépendant que de n) vérifiant la propriété suivante : si N est un entier dont tous les facteurs premiers sont $> C(n)$ et si $t \in T_0(\mathbb{C})$, l'homomorphisme*

$$\pi_1\,(T_0(\mathbb{C})\,,\,t) \to \mathrm{Sp}\,(V[N]_t)$$

est surjectif.

Le passage d'un théorème à l'autre utilise des résultats importants de Matthews, Vaserstein et Weisfeiler sur les propriétés de congruence des sous-groupes Zariski-denses : voir [**22**], lequel repose sur le théorème de classification des groupes finis simples ; voir aussi Nori ([**24**]), où une démonstration d'un tel résultat est esquissé, ou bien encore Hrushovski et Pillay ([**17**]) pour une approche alternative fondée sur la théorie des modèles. Du théorème (8.3), on déduit enfin le corollaire qui va suivre.

Donnons-nous W, un $(\mathbb{Z}/N\mathbb{Z})$-module libre de rang n, muni d'une forme alternée parfaite (un tel W est unique à isomorphisme près) et considérons le revêtement $T_W(\mathbb{C}) = \underline{\mathrm{IsomSp}}\,(W\,,\,V[N])$ de $T_0(\mathbb{C})$, dont la fibre au-dessus d'un point t est constituée des isomorphismes entre W et $V[N]_t$ compatibles aux formes symplectiques. C'est un revêtement étale galoisien de groupe $\mathrm{Sp}(W)$.

COROLLAIRE 8.4. — *$T_W(\mathbb{C})$ est connexe.*

8.3. — Soient $F \subset \mathbb{C}$ un corps de nombres, $\overline{F}$ sa clôture algébrique (dans $\mathbb{C}$). Supposons maintenant le module W muni d'une action du groupe de Galois $\mathrm{Gal}(\overline{F}/F)$ respectant sa forme symplectique (à une torsion à la Tate près) :

$$\langle\ ,\ \rangle_W\ :\ W \times W \to (\mathbb{Z}/N\mathbb{Z})\,(1-n)\,.$$

On regarde T_0 comme un schéma sur $\mathbb{Q}$ puis on étend les scalaires à F, en posant $T_{0,F} = T_0 \otimes F$. Via l'action de Galois, on peut voir W comme un revêtement étale fini (noté $\underline{W}$) de $\mathrm{Spec}\,F$. Au-dessus de $T_{0,F}$, on dispose donc des deux systèmes locaux $\underline{W}$ (image réciproque du précédent) et $V[N]$. On peut donc définir le F-schéma T_W des isomorphismes symplectiques entre $\underline{W}$ et $V[N]$. C'est un revêtement étale galoisien de $T_{0,F}$, qui est géométriquement connexe en vertu du corollaire précédent.

Concrètement, se donner un point de T_W sur une extension $F' \subset \overline{F}$ de F revient à se donner $t \in F' - \mu_{n+1}(F')$ et un isomorphisme symplectique entre $V[N]_t$ et W compatible à l'action du sous-groupe $\mathrm{Gal}(\overline{F}/F')$.

8.4. — D'autres résultats, de nature plus arithmétique, jouent un rôle important dans l'utilisation que l'on fait dans [**15**] de cette famille d'hypersurfaces. C'est tout particulièrement le cas du suivant, qui décrit dans certains cas la fibre $V[\ell]_0$:

PROPOSITION 8.5. — *Soit ℓ premier tel que $\ell \equiv 1 \bmod.(n+1)$. Alors $V[\ell]_0$, vu comme représentation du groupe d'inertie $I_{\mathbb{Q}_\ell}$, est isomorphe à la somme $1 \oplus \overline{\omega}_\ell^{-1} \oplus \overline{\omega}_\ell^{-2} \oplus \cdots \oplus \overline{\omega}_\ell^{1-n}$ (où $\overline{\omega}_\ell$ désigne la réduction modulo ℓ du caractère cyclotomique).*

Pour la représentation ℓ-adique $V_{\ell,0}$ le résultat analogue résulte de la décomposition sous l'action du groupe $H/H_0 \simeq \mu_{n+1}$ et de la connaissance des poids de Hodge-Tate. Du fait que les réductions $\overline{\omega}_\ell^{-i}$ (avec i variant de 0 à $n-1$) sont deux à deux distinctes, il est facile d'en déduire par réduction le résultat voulu : en effet, on a affaire à une représentation de $I_{\mathbb{Q}_\ell}^{\mathrm{ab}} \simeq \mathbb{Z}_\ell^*$; l'action du sous-groupe isomorphe à $\mathbb{F}_\ell^*$ admet alors pour espaces propres des droites, stables sous l'action du groupe entier.

On a enfin un résultat de bonne réduction ainsi que, pour t se réduisant sur ∞, un autre de mauvaise (analogue du type multiplicatif des courbes elliptiques).

Le premier résulte de théorèmes standard sur la cohomologie ℓ-adique :

PROPOSITION 8.6. — *Soient K une extension finie de $\mathbb{Q}_\ell$ et $t \in T_0(K)$. Alors $V_{\ell,t}$, vue comme représentation de $\mathrm{Gal}(\overline{K}/K)$, est de de Rham de poids de Hodge-Tate $\{0, 1, \ldots, n-1\}$. Si t est entier de réduction un point de T_0 à valeurs dans le corps résiduel (autrement dit, si $t^{n+1} - 1$ est inversible), alors $V_{\ell,t}$ est cristalline.*

Dans la proposition suivante, on se donne deux nombres premiers distincts q et ℓ, ce dernier ne divisant pas $n+1$. On se donne également un corps q-adique K et $t \in K$ non entier : c'est donc un élément de $T_0(K)$ de réduction ∞. Notons q_K le cardinal du corps résiduel et $v(t) < 0$ la valuation normalisée de t.

PROPOSITION 8.7. — (i) *Les représentations $V_{\ell,t}$ et $V[\ell]_t$ du groupe $\mathrm{Gal}(\overline{K}/K)$ ont des semi-simplifiées non ramifiées. Les valeurs propres correspondantes de Frobenius peuvent s'écrire α, $\alpha\, q_K$, $\alpha\,(q_K)^2, \ldots, \alpha\,(q_K)^{n-1}$ avec $\alpha \in \{\pm 1\}$.*

(ii) *Le groupe d'inertie agit sur $V_{\ell,t}$ par l'exponentielle d'un endomorphisme nilpotent $N_{t,K}$ d'ordre de nilpotence exactement n.*

(iii) *Le groupe d'inertie agit sur $V[\ell]_t$ par $\exp(v(t)\overline{N}_{t,K})$, où $\overline{N}_{t,K}$ est un endomorphisme nilpotent dont l'ordre, si ℓ est supérieur à une certaine constante $D(n)$, est exactement n.*

9. AUTOMORPHIE POTENTIELLE DE LA REPRÉSENTATION RÉSIDUELLE

9.1. — L'idée de base est d'appliquer le résultat qui va suivre aux espaces T_W définis ci-dessus. Il s'agit d'une légère amélioration d'un résultat de Moret-Bailly, lequel était lui-même parti de travaux de Rumely. Cela permet en gros, étant donné une variété lisse et géométriquement connexe définie sur un corps de nombres, de prédire l'existence d'un point défini sur une extension et vérifiant certaines propriétés locales, à condition qu'un tel point existe localement. Plus précisément :

PROPOSITION 9.1 ([**23**]). — *Soient F un corps de nombres, $S = S_1 \bigsqcup S_2$ un ensemble fini de places de F tel que S_2 ne contienne que des places finies. On se donne T/F une variété lisse et géométriquement connexe. On se donne également pour chaque $v \in S_1$ un sous-ensemble ouvert (pour la topologie v-adique) et non vide $\Omega_v \subset T(F_v)$ et pour chaque $v \in S_2$ un sous-ensemble ouvert non vide $\Omega_v \subset T(F_v^{\mathrm{nr}})$, invariant par $\mathrm{Gal}(F_v^{\mathrm{nr}}/F)$. Enfin la dernière donnée est celle d'une extension finie L/F.*

Alors il existe une extension finie galoisienne F'/F linéairement disjointe de L et un point $P \in T(F')$ tels que :

- *chaque $v \in S_1$ se décompose complètement dans F', et pour w une place de F' au-dessus de v (remarquer que F'_w s'identifie alors à F_v), on a : $P \in \Omega_v \subset T(F'_w)$;*
- *chaque $v \in S_2$ est non ramifiée dans F', et pour w une place de F' au-dessus de v (remarquer que F'_w se plonge alors dans F_v^{nr} par un plongement bien défini modulo $\mathrm{Gal}(F_v^{\mathrm{nr}}/F)$), on a : $P \in \Omega_v \cap T(F'_w)$.*

Le principe de base de la démonstration du théorème (1.1), très simplifié, est le suivant : appliquer ce résultat à un espace T_W, avec $N = \ell\ell'$ un produit de deux nombres premiers $> C(n)$ et pour W le produit tensoriel d'une représentation galoisienne symplectique σ_ℓ (modulo ℓ) et d'une autre $\sigma_{\ell'}$ (modulo ℓ').

Supposons que l'on sache que $\sigma_{\ell'}$ provient d'une forme automorphe, et qu'il en soit de même pour sa restriction au groupe de Galois de toute extension F' (vérifiant certaines propriétés) ; noter que ce dernier point n'est pas automatique dans l'état actuel de nos connaissances car on ne sait faire le « changement de base » que pour les extensions résolubles.

Le résultat précédent nous assurera alors, modulo des vérifications locales, l'existence de F', d'un $t \in F' - \mu_{n+1}(F')$ et d'isomorphismes symplectiques $\mathrm{Gal}(\overline{F}/F')$–invariants $V[\ell]_t \simeq \sigma_\ell$ et $V[\ell']_t \simeq \sigma'_\ell$. D'autre part, les deux représentations $V[\ell]_t$ et $V[\ell]_t$ se relèvent en des représentations ℓ- et ℓ'-adiques compatibles $V_{\ell,t}$ et $V_{\ell',t}$.

L'automorphie de $V[\ell']_t$ doit impliquer par relèvement celle de $V_{\ell',t}$. Par compatibilité, celle de $V_{\ell,t}$ en découlera, puis celle de σ_ℓ par réduction. Des hypothèses locales devront assurer que les théorèmes de relèvement de l'automorphie s'appliquent.

Il s'agit en fait d'une élaboration sophistiquée de ce qu'on appelle dans les travaux originels de Wiles le changement de nombre premier ou « ℓ-ℓ' trick ». La mise en œuvre de cette idée est compliquée par les nombreuses hypothèses locales qui doivent être assurées ; également d'autres ingrédients devront y être ajoutés afin de parvenir à la conclusion. Il sera parfois nécessaire d'appliquer la méthode ou des analogues plusieurs fois de suite.

9.2. — La voie suivie dans [**15**] pour prouver le théorème (1.1) énoncé au début de cet exposé passe par la démonstration préalable du suivant :

THÉORÈME 9.2. — *Soient F un corps totalement réel, n un entier pair, ℓ un nombre premier qui est $> \max\{C(n), n\}$, non ramifié dans F et $\equiv 1 \bmod (n+1)$. Soit $q \neq \ell$ un autre nombre premier, qui ne divise pas $(n+1)$, et soit v_q un idéal premier de F tel que le cardinal q_{v_q} du corps résiduel correspondant vérifie : $q_{v_q}^j \not\equiv 1 \bmod \ell$, pour j variant entre 1 et n.*

Supposons donnée une représentation continue dans le groupe des similitudes symplectiques :

$$r : \mathrm{Gal}(\overline{F}/F) \to GSp_n(\mathbb{Z}_\ell)$$

vérifiant les propriétés suivantes :

(i) *le rapport de similitude de r est égal à ϵ_ℓ^{1-n} ;*

(ii) *r ne se ramifie qu'en un nombre fini de places ;*

(iii) *l'image de $\mathrm{Gal}(\overline{F}/F(\zeta_\ell))$ par la semi-simplifiée $\overline{r}$ de la réduction modulo ℓ de r est assez grosse (cf. 4.1) ;*

(iv) *le corps des invariants $\overline{F}^{\mathrm{Ker}(\mathrm{ad}\,\overline{r})}$ ne contient pas $F(\zeta_\ell)$;*

(v) *en chaque place w de F au-dessus de ℓ, la restriction de r au groupe de décomposition correspondant est cristalline de poids $0, 1, \ldots, n-1$, tous de multiplicité 1. De plus la restriction de $\overline{r}$ au groupe d'inertie en w vérifie*

$$\overline{r}_{|I_{F_w}} \simeq 1 \oplus \overline{\epsilon}_\ell^{-1} \oplus \overline{\epsilon}_\ell^{-2} \oplus \cdots \oplus \overline{\epsilon}_\ell^{1-n} ;$$

(vi) *la semi-simplifiée de la restriction de r au groupe de décomposition en v_q est non ramifiée, les valeurs propres de Frobenius correspondantes étant égales à $1, q_{v_q}, q_{v_q}^2, \ldots, q_{v_q}^{n-1}$. La restriction de $\overline{r}$ au groupe de décomposition en v_q est non ramifiée.*

Alors il existe une extension totalement réelle F'/F, linéairement disjointe de $\overline{F}^{\mathrm{Ker}\,\overline{r}}$ et non ramifiée au-dessus de ℓ, et une place w_q de F' au-dessus de v_q, telles que la restriction $r_{|\mathrm{Gal}(\overline{F}/F')}$ soit automorphe de poids 0 et de type $\{Sp_n(1)\}_{\{w_q\}}$.

• *De plus si on suppose donnés un sous-corps F_0 de F sur lequel F est galoisien, et un ensemble fini $\mathcal{L}$ de places finies de F non au-dessus de ℓ ni de q, et en lesquelles r ne se ramifie pas, alors on peut trouver F' vérifiant la conclusion du théorème qui soit galoisienne sur F_0 et telle que les places de $\mathcal{L}$ ne s'y ramifient pas.* •

Remarque 9.3. — En fait on a besoin d'un analogue de ce théorème qui soit simultané pour un ensemble fini donné d'entiers pairs : voir le théorème (0.6) et les commentaires précédant le théorème (1.1). J'ai négligé cette complication dans l'énoncé précédent pour ne pas obscurcir davantage le paysage.

On voudrait prouver le théorème (1.1) en appliquant le précédent à la représentation r_n puissance symétrique $(n-1)$-ième de celle (r) de dimension 2 qui figure dans ses données. Il y a quelques différences dans les hypothèses qui font que cela ne peut être fait directement. La plus essentielle est celle de (v), relative à la restriction de $\overline{r}_n$ au groupe d'inertie des places au-dessus de ℓ et qui n'a aucune raison d'être satisfaite dans l'application que nous avons en vue, à savoir aux puissances symétriques de la représentation de degré 2 associée à une courbe elliptique fixée.

On remédie à cela en appliquant un premier changement de nombre premier, dont le principe est schématiquement le suivant : on se donne un autre nombre premier ℓ' assez grand et vérifiant des propriétés analogues à celles de ℓ (en particulier ℓ' est non ramifié dans F). Soit $\overline{r}'$ une représentation modulo ℓ' obtenue à partir d'une courbe elliptique $\mathcal{E}_1$ admettant bonne réduction en ℓ et bonne réduction ordinaire en ℓ' et telle que la représentation $\overline{r}'$ soit surjective et modérément ramifiée en ℓ'.

Le produit $\overline{r} \times \overline{r}'$ définit un $(\mathbb{Z}/\ell\ell'\mathbb{Z})$-module symplectique W muni d'une action galoisienne et donc un faisceau $\underline{W}$ sur $Spec\, F$. On peut alors, de façon analogue à ce que nous avons fait en (8.3), considérer la variété $T_{\overline{r},\overline{r}'}$ sur F qui classifie les courbes elliptiques munies d'un isomorphisme entre leur cohomologie modulo $\ell\ell'$ et $\underline{W}$.

Une application convenable du théorème de Moret-Bailly nous dit alors que, quitte à effectuer une extension F'/F du corps F, il existe une courbe elliptique $\mathcal{E}$, admettant bonne réduction au-dessus de ℓ et en ℓ' et telle que la restriction de $\overline{r}$ (resp. de $\overline{r}'$) au groupe de Galois de F' soit donné par l'action sur $H^1(\mathcal{E}_{\overline{F}}, \mathbb{F}_\ell)$ (resp. sur $H^1(\mathcal{E}_{\overline{F}}, \mathbb{F}_{\ell'})$). Plus précisément, on applique le théorème avec pour S_1 la réunion des places archimédiennes, de la place v_q et d'une autre $v_{q'}$ où $\mathcal{E}_1$ admet une réduction de type multiplicatif ; quant à S_2, c'est l'ensemble des places au-dessus de ℓ ou de ℓ'. On obtient alors, en imposant certaines conditions locales (ouvertes), un corps F' vérifiant diverses propriétés, étant en particulier totalement réel et non ramifié au-dessus de ℓ et de ℓ'. D'autres conditions (notamment le fait que $\mathcal{E}$ ait bonne réduction au-dessus de ℓ et ℓ' et réduction multiplicative déployée au-dessus de v_q et $v_{q'}$) assurent que les théorèmes de relèvement de l'automorphie s'appliquent à la puissance symétrique $(n-1)$-ième de la représentation ℓ'-adique associée à $\mathcal{E}$.

On conclut alors par un argument semblable à celui esquissé ci-dessus, qui utilise la compatibilité des puissances symétriques des représentations ℓ- et ℓ'-adiques : le théorème (9.2) peut s'appliquer à la représentation sur $\mathrm{Sym}^{n-1} H^1(\mathcal{E}_{\overline{F}}, \mathbb{Z}_{\ell'})$ puisqu'elle satisfait à la condition (v) relative à la restriction aux places divisant ℓ. Elle est donc

automorphe sur une extension de F', et on en déduit par compatibilité qu'il en est de même de $\mathrm{Sym}^{n-1}H^1(\mathcal{E}_{\overline{F}}, \mathbb{Z}_\ell)$ et enfin par réduction de $\mathrm{Sym}^{n-1}H^1(\mathcal{E}_{\overline{F}}, \mathbb{F}_\ell)$, isomorphe à la restriction de $\overline{r}_n$. Une dernière application du théorème de relèvement nous donne alors l'automorphie potentielle de r_n.

9.3. — Il nous reste à expliquer quelle est l'idée de la preuve du théorème (9.2). Le point essentiel consiste à montrer l'automorphie potentielle de la représentation résiduelle $\overline{r}$ et pour cela on fait usage des espaces T_W définis plus haut avec N le produit de ℓ par un autre nombre premier ℓ' supposé « assez grand » et vérifiant de nombreuses propriétés. Le principe de la démonstration est facile à expliquer si on néglige une partie des hypothèses nécessaires à l'application des théorèmes de relèvement de l'automorphie, et tout particulièrement la nécessité de toujours avoir une place du type Steinberg.

Décrivons donc approximativement la méthode. L'idée est de prendre pour W le produit de la représentation $\overline{r}$ par une représentation $I(\overline{\theta})$ modulo ℓ' induite à partir d'un caractère modulo ℓ' convenable du groupe de Galois absolu d'une extension de type CM cyclique de degré n de $\mathbb{Q}$, notée M. Quant à $\overline{\theta}$, il doit vérifier de nombreuses conditions, qui assurent en particulier que l'image de l'induite est symplectique, assez grosse et admet une restriction irréductible à l'un des groupes de décomposition. D'autre part, l'existence de l'« induction automorphe » pour les extensions cycliques assure que cette induite est automorphe et ceci reste vrai pour ses restrictions irréductibles aux groupes de Galois d'extensions de $\mathbb{Q}$ car on obtient alors des induites du même type. D'autres propriétés de $\overline{\theta}$ seront détaillées ci-dessous au moment de les utiliser.

Il s'agit de trouver un point de T_W défini sur un corps de nombres totalement réel F' et vérifiant certaines propriétés locales : dans la situation simplifiée sur laquelle nous raisonnons, nous appliquerions le théorème de Moret-Bailly avec, pour S_1, l'ensemble des places archimédiennes et, pour S_2, l'ensemble des places divisant ℓ ou ℓ'. Pour $w \in S_2$ l'ouvert Ω_w est l'ensemble des points qui se projettent sur un point entier de $T_0(F_w^{\mathrm{nr}})$ et dont la réduction est aussi dans T_0 (cf. la proposition (1.6)). Cet ensemble est non vide car il contient des points au-dessus de 0 : en effet, si w divise ℓ, on doit trouver deux isomorphismes compatibles avec l'action du groupe d'inertie I_w en w

$$V[\ell]_0 \simeq \overline{r} \text{ et } V[\ell']_0 \simeq I(\overline{\theta}).$$

Le premier existe en vertu de l'hypothèse (v) du théorème et de la proposition (8.5). Quant au second, $V[\ell']_0$ est non ramifiée au-dessus de I_w (car la variété Y_0 a bonne réduction au-dessus de $\mathbb{Z}\left[\frac{1}{n+1}\right]$) et on a choisi $\overline{\theta}$ non ramifié en ℓ.

Si au contraire w divise ℓ', on doit toujours choisir deux tels isomorphismes mais compatibles avec l'action du nouveau groupe d'inertie I_w. Le premier isomorphisme

existe parce que les deux membres sont non ramifiés au-dessus de ℓ' (rappelons que r est non ramifié en ℓ'). En ce qui concerne le second, la restriction de $V[\ell']_0$ au groupe d'inertie en w est de nouveau donnée par la proposition (8.5) et l'on a choisi précisément M et $\overline{\theta}$ pour que l'induite ait cette forme : plus exactement, ℓ' est décomposé dans M et les caractères donnés par la restriction de $\overline{\theta}$ aux groupes d'inertie aux différentes places au-dessus de ℓ' correpondent aux $\overline{\epsilon}_\ell^{-j}$.

Dans cette situation idéalisée, on termine le raisonnement suivant l'idée qui a déjà été esquissée plus haut. L'application du théorème de Moret-Bailly nous fournit un corps F' et $t \in F'$ tel qu'on ait des isomorphismes $\mathrm{Gal}(\overline{F}/F')$–invariants

$$V[\ell]_t \simeq \overline{r} \text{ et } V[\ell']_t \simeq I(\overline{\theta}).$$

Or on a déjà remarqué que $I(\overline{\theta})$ est automorphe, ainsi que ses restrictions irréductibles ; le théorème de relèvement de l'automorphie nous dit alors que $V_{\ell',t}$ l'est aussi. Par compatibilité, il en est de même de $V_{\ell,t}$ et on obtient bien finalement par réduction l'automorphie de $\overline{r}$.

En réalité la démonstration donnée dans [**15**] est beaucoup plus compliquée, essentiellement par le fait qu'on doit s'assurer de l'existence de places convenables de type Steinberg pour les représentations automorphes qui interviennent. Ce ne peut pas être le cas des induites automorphes (qui peuvent par contre être supercuspidales en une place), mais un théorème de [**8**] permet de relever avec des conditions de type Steinberg une telle induite résiduelle.

On obtient des points de T_W associés à des représentations qui sont du type Steinberg en certaines places v_q en imposant des conditions de valuation $v_q(t) < 0$ et en appliquant la proposition (8.7). Cela impose une torsion préalable de nos représentations en ces places par des caractères galoisiens à valeurs dans $\{\pm 1\}$. C'est donc avec de telles données et conditions supplémentaires que l'on doit appliquer le théorème de Moret-Bailly.

Dans le même ordre d'idées, une difficulté occultée dans le schéma de démonstration que j'ai esquissé ci-dessus tient au fait que l'automorphie de $\overline{r}$ provient de celle de $I(\overline{\theta})$ pour laquelle on peut trouver une place v'_q où le Frobenius a pour valeurs propres $1, q', q'^2, \ldots, q'^{n-1}$; mais q' est en général distinct de la place q qui apparaît dans l'énoncé du théorème (9.2). Une autre application du résultat de Moret-Bailly permet une sorte d'interversion de v_q et v'_q : on utilise pour cela un espace analogue à T_W – mais pour W simplement attaché à la représentation $\overline{r}$ convenablement tordue. Je renvoie le lecteur à [**15**] pour une démonstration complète.

RÉFÉRENCES

[1] J. ARTHUR & L. CLOZEL – *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies, vol. 120, Princeton University Press, 1989.

[2] F. BEUKERS & G. HECKMAN – Monodromy for the hypergeometric function ${}_nF_{n-1}$, *Invent. Math.* **95** (1989), p. 325–354.

[3] H. CARAYOL – Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet, in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, Contemp. Math., vol. 165, Amer. Math. Soc., 1994, p. 213–237.

[4] ———, Preuve de la conjecture de Langlands locale pour GL_n : travaux de Harris-Taylor et Henniart, Séminaire Bourbaki, vol. 1998/99, exp. n° 857, *Astérisque* **266** (2000), p. 191–243.

[5] L. CLOZEL – The Sato-Tate conjecture, prépublication.

[6] ———, Représentations galoisiennes associées aux représentations automorphes autoduales de $\mathrm{GL}(n)$, *Publ. Math. I.H.É.S.* **73** (1991), p. 97–145.

[7] ———, On the cohomology of Kottwitz's arithmetic varieties, *Duke Math. J.* **72** (1993), p. 757–795.

[8] L. CLOZEL, M. HARRIS & R. TAYLOR – Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations, prépublication.

[9] F. DIAMOND – The Taylor-Wiles construction and multiplicity one, *Invent. Math.* **128** (1997), p. 379–391.

[10] B. EDIXHOVEN – Rational elliptic curves are modular (after Breuil, Conrad, Diamond and Taylor), Séminaire Bourbaki, vol. 1999/2000, exp. n° 871, *Astérisque* **276** (2002), p. 161–188.

[11] J.-M. FONTAINE & G. LAFFAILLE – Construction de représentations p-adiques, *Ann. Sci. École Norm. Sup. (4)* **15** (1982), p. 547–608.

[12] K. FUJIWARA – Galois deformations and arithmetic geometry of Shimura varieties, in *International Congress of Mathematicians. Vol. II*, Eur. Math. Soc., Zürich, 2006, p. 347–371.

[13] A. GENESTIER & J. TILOUINE – Systèmes de Taylor-Wiles pour GSp_4, *Astérisque* **302** (2005), p. 177–290, Formes automorphes. II. Le cas du groupe $\mathrm{GSp}(4)$.

[14] M. HARRIS – Potential automorphy of odd-dimensional symmetric powers of elliptic curves, and applications, prépublication.

[15] M. HARRIS, N. SHEPHERD-BARRON & R. TAYLOR – A family of Calabi-Yau varieties and potential automorphy, prépublication.

[16] M. HARRIS & R. TAYLOR – *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, vol. 151, Princeton University Press, 2001.

[17] E. HRUSHOVSKI & A. PILLAY – Definable subgroups of algebraic groups over finite fields, *J. reine angew. Math.* **462** (1995), p. 69–91.

[18] Y. IHARA – On modular curves over finite fields, in *Discrete subgroups of Lie groups and applications to moduli (Internat. Colloq., Bombay, 1973)*, Oxford Univ. Press, 1975, p. 161–202.

[19] N. M. KATZ – *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, 1990.

[20] M. KISIN – Moduli of flat group schemes and modularity, à paraître dans *Ann. of Math.*

[21] J.-P. LABESSE – Cohomologie, stabilisation et changement de base, *Astérisque* **257** (1999), p. 161.

[22] C. R. MATTHEWS, L. N. VASERSTEIN & B. WEISFEILER – Congruence properties of Zariski-dense subgroups. I, *Proc. London Math. Soc. (3)* **48** (1984), p. 514–532.

[23] L. MORET-BAILLY – Groupes de Picard et problèmes de Skolem. I, II, *Ann. Sci. École Norm. Sup. (4)* **22** (1989), p. 161–179, 181–194.

[24] M. V. NORI – On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$, *Invent. Math.* **88** (1987), p. 257–275.

[25] J. OESTERLÉ – Travaux de Wiles (et Taylor, ...). II, Séminaire Bourbaki, vol. 1994/95, exp. n° 804, *Astérisque* **237** (1996), p. 333–355.

[26] J-P. SERRE – *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[27] F. SHAHIDI – On nonvanishing of L-functions, *Bull. Amer. Math. Soc. (N.S.)* **2** (1980), p. 462–464.

[28] R. TAYLOR – Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations II, prépublication.

[29] ———, Remarks on a conjecture of Fontaine and Mazur, *J. Inst. Math. Jussieu* **1** (2002), p. 125–143.

[30] ———, On the meromorphic continuation of degree two L-functions, *Doc. Math.* **Extra Vol.** (2006), p. 729–779.

[31] R. TAYLOR & A. WILES – Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141** (1995), p. 553–572.

[32] R. TAYLOR & T. YOSHIDA – Compatibility of local and global Langlands correspondences, *J. Amer. Math. Soc.* **20** (2007), p. 467–493.

[33] M.-F. VIGNÉRAS – *Représentations l-modulaires d'un groupe réductif p-adique avec $l \neq p$*, Progress in Mathematics, vol. 137, Birkhäuser, 1996.

[34] A. WILES – Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), p. 443–551.

Henri CARAYOL

Institut de Recherche Mathématique Avancée
Université Louis Pasteur et CNRS
7, rue René Descartes
F-67084 Strasbourg Cedex
E-mail : carayol@math.u-strasbg.fr