Séminaire BOURBAKI Novembre 2005
58ème année, 2005-2006, n° 956

LA CONJECTURE DE MODULARITÉ DE SERRE : LE CAS DE CONDUCTEUR 1 [d'après C. Khare]

par **Jean-Pierre WINTENBERGER**

INTRODUCTION

Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Notons $G_{\mathbb{Q}}$ le groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$. Soit p un nombre premier et soit $\overline{\mathbb{F}_p}$ une clôture algébrique du corps à p éléments. Soit $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ une représentation continue (donc à image finie), irréductible et impaire ($\det(\overline{\rho}(c)) = -1$ où c est la conjugaison complexe). Nous appelons une telle représentation galoisienne une représentation de type S.

Soit $\overline{\mathbb{Q}_p}$ une clôture algébrique du corps des nombres p-adiques $\mathbb{Q}_p$. Eichler, Shimura, Deligne, Deligne et Serre ont associé aux formes modulaires (propres) pour les sous-groupes de congruence de $\mathrm{SL}_2(\mathbb{Z})$ des représentations galoisiennes $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$, dont les réductions modulo p, lorsqu'elles sont irréductibles, sont de type S ([18],[20]; pour le poids 2, on pourra voir l'appendice de Conrad dans [44]). La conjecture de Serre, qui apparaît pour la première fois en 1972 (p.9 de [56]), dit que toute représentation de $G_{\mathbb{Q}}$ de type S est *modulaire i.e.* provient comme ceci d'une forme modulaire. Elle est énoncée dans [50] pour les représentations $\overline{\rho}$ non ramifiées en dehors de p (cas de niveau $N = 1$). Dans [52], Serre énonce pour tout niveau N ce que nous appelons la *forme forte* de la conjecture par opposition à sa *forme qualitative*. La forme forte précise le poids k, le niveau N et le caractère ϵ d'une forme primitive pour $\Gamma_1(N)$ dont provient $\overline{\rho}$.

Tate, en réponse à une lettre de Serre, prouve qu'il n'y a pas de représentation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_2})$ qui soit irréductible et non ramifiée hors de 2, prouvant ainsi la conjecture pour $p = 2$ et $N = 1$ (1973, [57]). La méthode de Tate, qui repose sur une minoration de discriminant, a été étendue par Serre au cas $p = 3$ et $N = 1$ (p.710 de [51]), et, sous l'hypothèse de Riemann généralisée, par Brueggeman pour $p = 5$ ([11]).

Grâce aux travaux de Ribet, Mazur, Carayol, Gross, Coleman-Voloch, Edixhoven, Diamond,..., on sait, pour $p \neq 2$, que la forme qualitative entraîne la forme forte. C'est un grand théorème sur lequel on trouvera d'excellents rapports dans [43], [26] et [44] : un cas de ce théorème a permis de déduire Fermat de la conjecture de Taniyama-Weil !

La démonstration, à la suite de Wiles, que toute courbe elliptique sur $\mathbb{Q}$ est modulaire, donne la conjecture de Serre pour les représentations galoisiennes $\overline{\rho}$ provenant des points d'ordre p des courbes elliptiques sur $\mathbb{Q}$. Pour ce faire, Wiles prouve des énoncés du type suivant ("MR" : modularité des relèvements ; § 3) : si $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ est *géométrique* *i.e.* vérifie des propriétés de ramification convenables, et si la réduction de ρ est du type S et modulaire, alors ρ est modulaire ([67],[64]). De plus, Wiles utilise un argument de “changement de nombre premier” : pour prouver que la représentation galoisienne $\overline{\rho_5} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_5)$ sur les points d'ordre 5 de la courbe elliptique E est modulaire, Wiles prouve l'existence d'une courbe elliptique E' sur $\mathbb{Q}$ dont la représentation sur les points d'ordre 5 est isomorphe à $\overline{\rho_5}$, et la représentation $\overline{\rho_3}$ sur les points d'ordre 3 est irréductible. La représentation $\overline{\rho_3}$, dont l'image est résoluble, est modulaire d'après Langlands-Tunnell ([66]). Un théorème “MR” entraîne alors que la représentation 3-adique associée à E' est modulaire, donc aussi E' et $\overline{\rho_5}$.

A l'aide de théorèmes “MR” et d'un argument de “changement de nombre premier”, Taylor prouve une version potentielle de la conjecture de Serre : une représentation de type S provient d'une forme modulaire de Hilbert après restriction à un corps de nombres totalement réel F ([61],[60]; § 4). On est alors confronté à un problème de changement de base de F à $\mathbb{Q}$. Dans certains cas, on peut s'assurer que $F/\mathbb{Q}$ est résoluble, et, alors le théorème de Langlands et Tunnell permet de prouver la conjecture ([38],[27]). Les théorèmes de Taylor, le théorème de changement de base résoluble d'Arthur-Clozel ([3]), et des arguments de Taylor ([63]) permettent à Dieulefait de prouver que, étant donnée une représentation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ possèdant les propriétés d'une représentation galoisienne associée à une forme modulaire, il existe un système compatible (ρ_λ) de représentations ℓ-adiques de $G_{\mathbb{Q}}$ dont fait partie ρ ([24] : §6).

La conjecture de Serre entraîne qu'une représentation $\overline{\rho}$ de type S admet des relèvements $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$, qui de plus sont géométriques. Ramakrishna, utilisant des techniques de déformations de représentations galoisiennes, le prouve dans de nombreux cas sans supposer $\overline{\rho}$ modulaire ([41]). Khare réalise que ces techniques de déformation et en particulier des résultats de Böckle ([7]), la version potentielle de la conjecture de Serre due à Taylor et les théorèmes de type “MR” pour les corps totalement réels, permettent d'obtenir des relèvements de représentations de type S qui ont des propriétés de ramification plus précises que celles obtenues par Ramakrishna, et qui sont prédites par la forme forte de la conjecture de Serre.

L'existence de relèvements avec ces propriétés de ramification précises et l'existence de systèmes compatibles, permettent d'utiliser la technique de changement de nombre premier de Wiles. Dans [34], la conjecture de Serre pour $N = 1$ est prouvée pour $p = 5, 7$, et pour les poids $k \leq 14, k \neq 10$. Des stratégies sont données pour la ramener dans le cas général à des énoncés “MR”. Utilisant des relèvements de poids 2 avec Nebentypus, Khare parvient à déduire des théorèmes “MR” connus le cas général de niveau (conducteur) 1 ([35]; pour un “survey” : [36]).

Enfin signalons que ce cercle d'idées a permis de grands progrès dans la preuve de la conjecture d'Artin pour les représentations impaires $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ ([13],[62]).

Je remercie Böckle de m'avoir communiqué son preprint [8] qui m'a beaucoup aidé pour la rédaction du § 5. Je remercie Khare pour ses remarques sur une première version du texte.

1. CONJECTURES DE MODULARITÉ DE SERRE ET DE FONTAINE-MAZUR

1.1. Représentations galoisiennes associées aux formes modulaires

Pour N entier ≥ 1, soit $\Gamma_1(N)$ le groupe des matrices :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ c \equiv 0 \bmod N,\ a \equiv d \equiv 1 \bmod N.$$

Soit k un entier ≥ 1. Soit $S_k(\Gamma_1(N))$ le $\mathbb{C}$-espace vectoriel des formes modulaires paraboliques de poids k et de niveau N. Une forme $f \in S_k(\Gamma_1(N))$ a un développement de Fourier à la pointe $i\infty$:

$$f(z) = \sum_{n=1}^{\infty} a_n q^n,\ q = e^{2\pi i z}.$$

Une forme primitive f est propre pour les opérateurs de Hecke T_n, n entier > 1, et pour les opérateurs diamant $\langle \overline{d} \rangle$, $\overline{d} \in (\mathbb{Z}/N\mathbb{Z})^*$. Elle est normalisée : $a_1 = 1$. Pour $n > 1$, a_n est la valeur propre de T_n. Notons $\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ le caractère $\langle \overline{d} \rangle (f) = \epsilon(\overline{d}) f$. On a :

$$(1)\ :\ f\left(\frac{az+b}{cz+d}\right) = \epsilon(\overline{d})(cz+d)^k f(z),\ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ c \equiv 0 \bmod N,$$

$\overline{d}$ étant l'image de d dans $(\mathbb{Z}/N\mathbb{Z})^*$. Les a_n et $\epsilon(\overline{d})$ engendrent un ordre de l'anneau des entiers d'une extension finie E_f de $\mathbb{Q}$ contenue dans $\mathbb{C}$; E_f est le corps des coefficients de f.

Eichler, Shimura, Deligne, et Deligne et Serre ont associé à f et à un plongement ι de E_f dans $\overline{\mathbb{Q}_p}$ une représentation galoisienne : $\rho_{f,\iota} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ qui est caractérisée à conjugaison près par les propriétés suivantes :

- $\rho_{f,\iota}$ est non ramifiée en dehors de $\{p\} \cup S_N$, S_N étant l'ensemble des nombres premiers qui divisent N ;

- pour $\ell \notin \{p\} \cup S_N$, si Frob_ℓ un élément de $G_{\mathbb{Q}}$ qui relève le Frobenius, on a : $\mathrm{tr}(\rho_{f,\iota}(\mathrm{Frob}_\ell)) = \iota(a_\ell)$.

Soit $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ le caractère cyclotomique. Le déterminant de $\rho_{f,\iota}$ est $\epsilon \chi_p^{k-1}$, où nous avons identifié de la manière naturelle $(\mathbb{Z}/N\mathbb{Z})^*$ avec le groupe de Galois de l'extension cyclotomique $\mathbb{Q}(\mu_N)/\mathbb{Q}$.

La représentation $\rho_{f,\iota}$ est impaire. En effet, il n'existe pas de forme parabolique non nulle de poids k et de caractère ϵ si l'on n'a pas $\epsilon(-1)(-1)^{k-1} = -1$, comme on le voit en considérant la matrice $-\mathrm{id}$ dans (1).

La représentation $\rho_{f,\iota}$ est irréductible ([20],[42]).

Elle est *géométrique* : elle est non ramifiée en dehors d'un ensemble fini de nombres premiers et sa restriction au groupe de décomposition D_p est potentiellement semi-stable, au sens de la théorie de Fontaine ([1]). Ceci résulte, si $k \neq 1$, de ce que $\rho_{f,\iota}$

apparait dans la cohomologie étale d'une variété algébrique et des théorèmes de comparaison p-adiques ([65]). Pour $k = 1$, $\overline{\rho}$ a une image finie et est donc aussi géométrique.

1.2. La conjecture de Fontaine et Mazur ([31])

CONJECTURE 1.1. — *Soit $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ une représentation p-adique impaire, irréductible et géométrique. Alors, il existe f, ι comme ci-dessus et un entier j tels que ρ soit isomorphe à $\rho_{f,\iota}$ tordue par χ_p^j.*

La forme f, (N, k, ϵ) et j sont bien déterminés par ρ (f à conjugaison galoisienne près). En effet, les poids de Hodge-Tate de ρ sont $(j, j + k - 1)$. Après torsion par χ_p^{-j}, on se ramène au cas $j = 0$. Soit pour nombre premier ℓ, r_ℓ la représentation F-semi-simple du groupe de Weil-Deligne WD_ℓ à valeurs dans $\mathrm{GL}_2(\overline{\mathbb{Q}_p})$ qui est associée à la restriction de ρ au groupe de décomposition D_ℓ. Pour $\ell \neq p$, r_ℓ a été définie par Grothendieck et Deligne (§8 de [19]). Pour $\ell = p$, elle a été définie par Fontaine à partir de l'action de D_p sur le module de Dieudonné filtré associé à la représentation potentiellement semi-stable $\rho_{|D_p}$ ([29]).

A r_ℓ est associée la partie ℓ primaire N_ℓ du conducteur. On a $N_\ell = 1$ si et seulement si soit $\ell \neq p$ et ρ est non ramifiée en ℓ, soit $\ell = p$ et $\rho_{|D_p}$ est cristalline. Le conducteur N est le produit des N_ℓ. Le caractère ϵ est défini par la formule $\det(\rho) = \epsilon\chi_p^{k-1}$.

Enfin f est déterminée par ρ par la formule $\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = \iota(a_\ell)$ pour ℓ premier à N et p, puisque l'on a pris soin de choisir f primitive. On peut aussi dire que la correspondance de Langlands locale associe à r_ℓ une représentation π_ℓ de $\mathrm{GL}_2(\mathbb{Q}_\ell)$. La représentation automorphe associée à f a pour composantes locales les π_ℓ, π_∞ étant la représentation de $\mathrm{GL}_2(\mathbb{R})$ correspondant aux formes modulaires de poids k.

1.3. La conjecture de Serre

Soient f et ι comme au 1.1. Notons $\overline{\mathbb{Z}_p}$ l'anneau des entiers de $\overline{\mathbb{Q}_p}$ et fixons un isomorphisme du corps résiduel de $\overline{\mathbb{Z}_p}$ avec $\overline{\mathbb{F}}_p$.

On peut conjuguer $\rho_{f,\iota}$ de sorte que $\rho_{f,\iota}$ soit à valeurs dans $\mathrm{GL}_2(\overline{\mathbb{Z}_p})$. Par l'homomorphisme de réduction $\overline{\mathbb{Z}_p} \to \overline{\mathbb{F}}_p$, on en déduit une représentation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. La semi-simplifiée de cette représentation est bien déterminée à isomorphisme près. On la note $\overline{\rho_{f,\iota}}$. Elle est bien sûr impaire.

On dit qu'une représentation irréductible $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ est *modulaire* si elle est isomorphe à $\overline{\rho_{f,\iota}}$, pour f et ι comme ci-dessus. La forme qualitative de la conjecture de Serre est :

CONJECTURE 1.2. — *Soit $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ une représentation de type S i.e. irréductible et impaire. Alors $\overline{\rho}$ est modulaire.*

C'est un fait central dans le sujet qu'une représentation $\overline{\rho}$ peut provenir de formes f de niveaux et de poids différents. La forme forte de la conjecture définit $(k(\overline{\rho}), N(\overline{\rho}), \epsilon(\overline{\rho}))$ minimal, en un sens précisé, tel que $\overline{\rho}$ provienne de f de poids $k(\overline{\rho})$, de niveau $N(\overline{\rho})$. Si l'on exclut certaines représentations diédrales pour $p = 2$ ou 3, on peut de plus imposer que le caractère de f soit $\epsilon(\overline{\rho})$.

On peut formuler une version de la forme forte de la conjecture, en terme de formes modulaires modulo p de Katz, qui de plus prédit quand $\overline{\rho}$ provient d'une forme modulaire de Katz de poids 1. Si $p \neq 2$, la version qualitative de la conjecture entraîne la version forte (sous l'une ou l'autre de ses deux formes). On renvoie pour ceci au rapport d'Edixhoven ([26]).

Le niveau $N(\overline{\rho})$ est défini par la formule usuelle pour le conducteur d'une représentation, sauf que l'on ne tient compte que de la ramification en dehors de p. En particulier, on a $N(\overline{\rho}) = 1$ si et seulement si $\overline{\rho}$ est non ramifiée en dehors de p.

Le poids $k(\overline{\rho})$ ne dépend que de l'action de la ramification en p. Notons $I_p \subset G_{\mathbb{Q}}$ le sous-groupe d'inertie pour une valuation p-adique de $\overline{\mathbb{Q}}$. La définition de $k(\overline{\rho})$ repose sur les propriétés que l'on connait de l'action de I_p dans les représentations p-adiques associées aux formes modulaires ([52],[25]). Rappelons en quelques propriétés, pour $p \neq 2$.

Soit $\overline{\chi_p} : G_{\mathbb{Q}} \to \mathbb{F}_p^*$ la réduction modulo p du caractère cyclotomique, et notons encore $\overline{\chi_p}$ sa restriction à I_p. Soit Ψ un caractère fondamental de niveau 2 de I_p : on peut prendre pour Ψ la restriction à I_p du caractère de Kummer pour l'extension $K(p^{\frac{1}{(p^2-1)}})/K$, K étant l'extension quadratique non ramifiée de $\mathbb{Q}_p$ dans $\overline{\mathbb{Q}_p}$.

On a : $2 \leq k(\overline{\rho}) \leq p^2 - 1$. Il existe j entier tel que l'on ait : $2 \leq k(\overline{\chi_p}^j \otimes \overline{\rho}) \leq p + 1$. On a $2 \leq k(\overline{\rho}) \leq p + 1$ si et seulement si l'on est dans l'un des deux cas suivants :

- il existe une droite D dans l'espace V de $\overline{\rho}$ telle que I_p opère trivialement sur V/D. L'action de I_p s'écrit alors :

$$\begin{pmatrix} \overline{\chi_p}^b & \eta \\ 0 & 1 \end{pmatrix}.$$

avec $1 \leq b \leq p - 1$. Si $b \neq 1$, on a : $k(\overline{\rho}) = 1 + b$. Si $b = 1$, η est un 1-cocycle de $Z^1(I_p, \overline{\mathbb{F}}_p(\overline{\chi_p}))$. Sa classe de cohomologie $c(\eta)$ provient par la théorie de Kummer d'un élément de $\mathbb{Q}_{p,\mathrm{nr}}^* \otimes \overline{\mathbb{F}_p}$, $\mathbb{Q}_{p,\mathrm{nr}}$ désignant l'extension maximale non ramifiée de $\mathbb{Q}_p$. Soit $v : \mathbb{Q}_{p,\mathrm{nr}}^* \otimes \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ l'homomorphisme défini par la valuation. On a $k(\overline{\rho}) = 2$ si $v(c(\eta)) = 0$ (cas peu ramifié) et $k(\overline{\rho}) = p + 1$ sinon (cas très ramifié). Dans le cas peu ramifié, la restriction de $\overline{\rho}$ à D_p provient d'un schéma en groupes fini et plat sur $\mathbb{Z}_p$.

- on a un caractère fondamental Ψ de niveau 2 de I_p tel que l'action de I_p sur V soit semi-simple de caractères Ψ^b et Ψ^{pb} avec $1 \leq b \leq p - 1$. On a : $k(\overline{\rho}) = b + 1$.

Le caractère $\det(\overline{\rho})\overline{\chi_p}^{1-k(\overline{\rho})}$ se factorise à travers $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. Il s'identifie donc à un caractère de $(\mathbb{Z}/N\mathbb{Z})^*$, que l'on note $\epsilon(\overline{\rho})$.

La forme forte de la conjecture de Serre s'énonce :

Conjecture 1.3. — *Soit $\overline{\rho}$ une représentation de type S. Alors, $\overline{\rho}$ provient d'une forme primitive de $S_{k(\overline{\rho})}(\Gamma_1(N(\overline{\rho})))$.*

Supposons de plus que si $p = 2$ (resp. $p = 3$), $\overline{\rho}$ n'est pas induite de $\mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{-3})$). Alors, la conjecture dit que l'on peut supposer de plus que le caractère de la forme soit $\epsilon(\overline{\rho})$.

2. LE THÉORÈME DE KHARE

Khare prouve la conjecture de Serre pour le niveau 1 :

Théorème 2.1. — *Soit $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ une représentation irréductible impaire et non ramifiée en dehors de p. Alors, $\overline{\rho}$ provient d'une forme propre de $S_{k(\overline{\rho})}(\mathrm{SL}_2(\mathbb{Z}))$.*

Remarque 2.2. — La condition de parité entraîne que $S_k(\mathrm{SL}_2(\mathbb{Z}))$ est trivial si k n'est pas pair. Le théorème de Kronecker-Weber entraîne que, pour $\overline{\rho}$ non ramifiée hors de p, $\det(\overline{\rho})$ est une puissance de $\overline{\chi_p}$. La définition de $k(\overline{\rho})$ entraîne $\det(\overline{\rho}) = \overline{\chi_p}^{k(\overline{\rho})-1}$. On voit donc que la condition $\overline{\rho}$ impaire est équivalente à $k(\overline{\rho})$ pair.

Explicitons l'énoncé pour $k \leq 12$ (qui est prouvé dans [34] pour $k(\overline{\rho}) \neq 10$). Pour $0 < k < 12$, $S_k(\mathrm{SL}_2(\mathbb{Z}))$ est trivial et $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ est de dimension 1, engendré par $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$. Swinnerton-Dyer a prouvé que pour $p \neq 2, 3, 5, 7, 691$, la représentation $\overline{\rho}(\Delta)$ est irréductible et qu'elle est réductible pour $p = 2, 3, 5, 7, 691$. Par torsion, on voit qu'il n'existe pas de $\overline{\rho}$ de type S non ramifiée hors de p si $p < 11$. Il n'existe pas de $\overline{\rho}$ de type S non ramifiée hors de p avec $k(\overline{\rho}) < 12$, ou si $k(\overline{\rho}) = 12$ et $p = 691$. Si $p \geq 11$ et $k(\overline{\rho}) = 12$, une telle $\overline{\rho}$ provient de Δ.

L'énoncé pour $k = 2$ entraîne qu'il n'existe pas de schéma en groupes sur $\mathbb{Z}$ de hauteur 2 tel que la représentation galoisienne associée soit irréductible.

Corollaire 1. — *On suppose $p \neq 2$. Soit $\overline{\rho}$ de type S, avec $k(\overline{\rho}) = 2$, $N(\overline{\rho}) = q$, q premier, alors $\overline{\rho}$ est modulaire.*

On a le cas particulier de la conjecture de Fontaine-Mazur :

Corollaire 2. — *On suppose $p \neq 2$. Soit $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ une représentation continue irréductible géométrique et impaire de poids de Hodge-Tate $(0, k-1)$ avec $k \geq 2$. On suppose ρ non ramifiée hors de p. On suppose de plus que la restriction $\rho_{|D_p}$ de ρ au groupe de décomposition D_p est :*

- soit cristalline de poids $2 \leq k \leq p+1$;

- soit ordinaire (voir 3).

Alors ρ provient d'une forme modulaire f.

3. MODULARITÉ DES RELÈVEMENTS DE REPRÉSENTATIONS MODULAIRES

La démonstration du théorème 2.1 nécessite des théorèmes "MR" pour des représentations du groupe de Galois des corps totalement réels.

Soit F un corps totalement réel de degré d sur $\mathbb{Q}$. Le groupe $\mathrm{GL}_2(F)$ agit sur le produit de d copies du demi-plan de Poincaré, ce qui permet de généraliser à $\mathrm{GL}_2(F)$ la théorie des formes modulaires pour $\mathrm{GL}_2(\mathbb{Q})$. On définit ainsi les formes modulaires de Hilbert. Le poids d'une telle forme est une collection de d entiers $(k_1, \ldots, k_d)$ indexés par les plongements de F dans $\mathbb{R}$. Nous considérons ici les formes de poids parallèle $k = k_1 = \ldots = k_d$, $k \geq 2$.

Pour f forme propre, les valeurs propres des opérateurs de Hecke engendrent une extension finie E_f de $\mathbb{Q}$. Pour f parabolique primitive et ι un plongement du corps E_f dans $\overline{\mathbb{Q}_p}$, on sait associer une représentation $\rho_{f,\iota}$ du groupe de Galois G_F de $\overline{\mathbb{Q}}/F$ ([58]). Elle est *impaire, i.e.* pour tout $g \in G_{\mathbb{Q}}$, on a $\det(\rho_{f,\iota}(gcg^{-1})) = -1$, irréductible, non ramifée en dehors d'un ensemble fini d'idéaux premiers de F. Sous différentes hypothèses, on sait que sa restriction aux groupes de décompositions $D_\wp$ pour $\wp$ idéal premier au dessus de p est potentiellement semi-stable de poids de Hodge-Tate $(0, k-1)$ ([6],[59],[9]).

Soit $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ une représentation irréductible impaire, géométrique de poids de Hodge-Tate $(0, k-1)$ pour les idéaux premiers de F au dessus de p. On dit que ρ est *quasi-ordinaire* si pour tout premier $\wp$ de F au dessus de p, $\rho_{|D_\wp}$ est de la forme :

$$\begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$$

avec $\psi_2(I_\wp)$ finie, $I_\wp$ désignant le sous-groupe d'inertie ; ρ est *ordinaire* si ψ_2 est de plus non ramifié. On a la notion de forme f quasi-ordinaire (relativement à un plongement ι de son corps des coefficients dans $\overline{\mathbb{Q}_p}$) , et pour une telle f, $\rho_{f,\iota}$ est quasi-ordinaire.

Si ρ est quasi-ordinaire, on dit que ρ est $D_\wp$*-distinguée* si les réductions $\overline{\psi_1}$ et $\overline{\psi_2}$ des caractères ψ_1 et ψ_2 sont distinctes pour tout $\wp$. Si ρ est $D_\wp$-distinguée et si ρ' est un relèvement quasi-ordinaire de $\overline{\rho}$, de caractères ψ'_1 et ψ'_2, on dit que ρ' est un $\overline{\psi_2}$*-relèvement* de $\overline{\rho}$ si les caractères $\overline{\psi_2}$ et $\overline{\psi_2}'$ coïncident pour tout $\wp$.

On a :

Théorème 3.1. — *Supposons $p \neq 2$. Soit k un entier ≥ 2. Soit F un corps de nombres totalement réel. Soit $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ une représentation irréductible impaire, géométrique et dont les poids de Hodge-Tate sont $(0, k-1)$ pour tout premier $\wp$ de F au dessus de p. Soit $\overline{\rho}$ la réduction de ρ (1.3).*

On suppose que l'on a l'une des hypothèses suivantes :

- i) $F = \mathbb{Q}$, $\overline{\rho}$ réductible, ρ quasi-ordinaire et D_p-distinguée ;

- ii) $\overline{\rho}$ est irréductible, ρ est quasi-ordinaire et $D_\wp$ distinguée, $\overline{\rho}$ provient par réduction modulo p d'une forme f et d'un plongement ι de son corps des coefficients dans $\overline{\mathbb{Q}_p}$, f quasi-ordinaire relativement à ι, telle que $\rho_{f,\iota}$ soit un $\overline{\psi_2}$ relèvement de $\overline{\rho}$;

- iii) le commutant de $\overline{\rho}_{D_p}$ est réduit aux homothéties, $2 \leq k \leq 2p-1$, p est complètement décomposé dans F, pour tout idéal premier $\wp$ de F au dessus de p, $\rho_{|D_\wp}$ est cristalline de poids de Hodge-Tate $(0, k-1)$, la restriction de $\overline{\rho}$ à $F(\mu_p)$ est irréductible, et $\overline{\rho}$ provient d'une forme de Hilbert f de poids parallèle k ;

- iv) $F = \mathbb{Q}$, $k = 2$, $\rho_{|D_\wp}$ est potentiellement cristalline, $\overline{\rho}$ provient d'une forme modulaire, et la restriction de $\overline{\rho}$ à $\mathbb{Q}(\mu_p)$ est irréductible ;

Alors ρ provient d'une forme modulaire de poids parallèle k.

Les i) et ii) sont des théorèmes de Skinner-Wiles ([53], [55]). Les iii) et iv) sont dus à Kisin ([37]). Pour $F \neq \mathbb{Q}$ et $k > 2$, le iii) necessite la généralisation de [54] au cas $k > 2$, qui n'est pas écrite (mais ce cas n'est pas necessaire à la démonstration du théorème de Khare). Pour un cas particulier de iii), voir Taylor ([60]). Il y a une difficulté technique pour $p = 3$ ([35]). On trouvera une excellente introduction aux théorèmes "MR" dans [17].

4. VERSION POTENTIELLE DE LA CONJECTURE DE SERRE

Le théorème suivant de Taylor ([61],[60]) est fondamental :

Théorème 4.1. — *On suppose $p \neq 2$. Soit $\overline{\rho}$ une représentation de type S à image non résoluble. Supposons $2 \leq k(\overline{\rho}) \leq p+1$ et $k(\overline{\rho}) \neq p$. Alors, il existe une extension finie galoisienne de $\mathbb{Q}$, totalement réelle, non ramifiée en p, telle que $\overline{\rho}_{|G_F}$ provienne d'une forme modulaire de Hilbert f pour F, vérifiant l'une ou l'autre propriété suivante :*

- f est de poids parallèle $k(\overline{\rho})$ et de conducteur 1 ;

- f est de poids parallèle 2 et de conducteur divisant p.

Remarque 4.2. — Soit H un sous-groupe fini de $\mathrm{PGL}_2(\overline{\mathbb{F}_p})$. Rappelons le théorème de Dickson : H est conjugué :

- soit à un sous-groupe des matrices triangulaires supérieures ;

- soit à $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ ou à $\mathrm{PSL}_2(\mathbb{F}_{p^r})$, pour un entier $r > 0$;

- soit à A_4, S_4 (si $p \neq 2$), A_5 ou au groupe diédral d'ordre $2r$ pour un entier $r > 1$ non divisible par p.

Il en résulte facilement que, si $\overline{\rho}$ est de type S et d'image non résoluble, pour toute extension galoisienne totalement réelle de $\mathbb{Q}$, $\overline{\rho}(G_F)$ n'est pas résoluble.

Donnons une idée de la preuve du théorème. Taylor considère un problème de modules classifiant les données (A, i, j, α), où :

- A est une variété abélienne de dimension d ;

- i est un plongement de l'anneau des entiers O_M d'un corps de nombres M de degré d dans $\mathrm{End}(A)$;

- j est une donnée de polarisation de A ;

- α est une structure de niveau $\lambda\mathcal{L}_1$ ou $\lambda\mathcal{L}_1\mathcal{L}_2$ selon les cas. On a un idéal premier λ de O_M au dessus de p tel que α définisse un isomorphisme des points de λ-torsion $A[\lambda]$ avec $\overline{\rho}$. On a $\mathcal{L}_1$ de caractéristique résiduelle $\ell_1 \neq p$ tel que α induise un isomorphisme de $A[\mathcal{L}_1]$ avec un module induit irréductible $\mathrm{ind}_{\mathbb{Q}}^{L}(\theta)$, L corps quadratique imaginaire.

Ce problème de modules est représentable par un schéma X sur $\mathbb{Q}$, qui est lisse, géométriquement irréductible et quasi-projectif. Les ensembles $X(\mathbb{R})$, $X(\mathbb{Q}_p)$ et $X(\mathbb{Q}_{\ell_i})$ sont non vides. Il résulte alors d'un théorème de Moret-Bailly que X a un point dans une extension F_0 de $\mathbb{Q}$ qui est galoisienne finie et totalement décomposée aux places ∞, p et ℓ_i ([40]).

On sait, d'après Hecke (Math.Werke, pp.442-447 et p.703), que $\mathrm{ind}_{\mathbb{Q}}^{L}(\theta)$ est modulaire (voir aussi 5.1. de [52]). Ce module induit ind reste irréductible après restriction au groupe de Galois de $F_0(\mu_{\ell_1})$ et, avec la représentation ℓ_1-adique associée à A, il satisfait aux hypothèses du ii) du théorème 3.1. Il en résulte que A_{F_0} provient d'une forme modulaire de Hilbert f_0 de poids 2.

Un théorème de Skinner-Wiles donne l'existence de $F_1 \supset F_0$ tel que $\overline{\rho}_{|G_{F_1}}$ provienne d'une forme f_1 non ramifiée hors de p ([54]). Taylor prouve par une analyse de la réduction de A modulo les idéaux premiers de F_1 au dessus de p et par la théorie des congruences entre formes modulaires que l'on peut trouver $F \supset F_1$ et f vérifiant de plus les conditions en p du théorème.

5. RELÈVEMENTS AVEC CONDITIONS DE RAMIFICATION

On suppose $p \neq 2$. Soit $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ une représentation de type S à image non résoluble.

La conjecture de Serre entraîne l'existence d' un relèvement géométrique de $\overline{\rho}$. Ceci a été prouvé dans de nombreux cas par Ramakrishna sans supposer $\overline{\rho}$ modulaire ([41]). En fait, on s'attend à pouvoir être plus précis sur la ramification des relèvements. En effet, Diamond et Taylor prouvent dans beaucoup de cas le résultat suivant ([22],[23]). Supposons $\overline{\rho}$ modulaire. Soit S un ensemble fini de nombres premiers $\neq p$, pour tout $\ell \in S$ une représentation $\tau_\ell : D_\ell \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ qui relève la restriction de $\overline{\rho}$ au groupe de décomposition D_ℓ. Alors, il existe un relèvement modulaire ρ de $\overline{\rho}$ tel que, pour tout $\ell \in S$, la restriction de ρ au groupe d'inertie I_ℓ soit isomorphe à la restriction de τ_ℓ à I_ℓ.

Les théorèmes suivants prouve dans certains cas l'existence de relèvement avec conditions de ramification sans supposer que $\overline{\rho}$ est modulaire, et en incluant le cas $\ell = p$.

5.1. Relèvements minimaux

Soit ℓ un nombre premier $\neq p$. On sait que la restriction de $\overline{\rho}$ à I_ℓ est soit de l'un des types suivants :

$$\xi \otimes \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}, \operatorname{Ind}_{I_M}^{I_p}(\xi),$$

M étant une extension quadratique ramifiée de $\mathbb{Q}_\ell$, soit $\ell = 2$ et l'image de I_2 dans la représentation projective $\overline{\rho}_{\text{proj}}$ associée à $\overline{\rho}$ est un sous-groupe de A_4 ([21]).

Soit ρ un relèvement de $\overline{\rho}$. Si $\ell \neq p$, on dit que ρ est *minimal* en ℓ si la restriction de ρ à I_ℓ est soit:

$$\tilde{\xi} \otimes \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \tilde{\xi}_1 & 0 \\ 0 & \tilde{\xi}_2 \end{pmatrix}, \operatorname{Ind}_{I_M}^{I_p}(\tilde{\xi}),$$

$\tilde{*}$ désignant le représentant de Teichmüller de $*$, soit, si on est dans le cas $\ell = 2$ et $\overline{\rho}_{\text{proj}}(I_2) \subset A_4$, que $\overline{\rho}(I_2)$ et $\rho(I_2)$ soient isomorphes.

Si $2 \leq k(\overline{\rho}) < p + 1$, on dit que ρ est *minimal* en p si la restriction de ρ à I_p est cristalline de poids de Hodge-Tate $(0, k(\overline{\rho}) - 1)$. Si $k(\overline{\rho}) = p + 1$, on dit que ρ est en p *minimal de type cristallin* si la restriction de ρ à I_p est cristalline de poids de Hodge-Tate $(0, p)$, et *minimal de type semi-stable* si la restriction de ρ à I_p est semi-stable de poids de Hodge Tate $(0, 1)$.

THÉORÈME 5.1. — *([34]) Soit $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ une représentation de type S à image non résoluble. On suppose que $2 \leq k(\overline{\rho}) \leq p + 1$ et que $k(\overline{\rho}) \neq p$. Alors, $\overline{\rho}$ a un relèvement qui est minimal pour tout ℓ et si $k(\overline{\rho}) = p + 1$, on peut imposer en p soit que ρ soit minimal de type cristallin soit que ρ soit minimal de type semi-stable.*

5.2. Relèvements de poids 2

Le théorème suivant correspond au fait que toute forme modulaire de poids k, $2 \leq k \leq p + 1$, et de niveau N premier à p, est congruente modulo p à une forme de poids 2 pour $\Gamma_1(pN)$ (§3 de [49], prop 9.3 de [32]).

On suppose que $\overline{\rho}_{|I_p}$ est ordinaire *i.e.* du type :

$$\begin{pmatrix} \overline{\chi_p}^{k-1} & * \\ 0 & 1 \end{pmatrix},$$

pour un entier k avec $2 \leq k \leq p$. Soit ω_p le relèvement de Teichmüller de $\overline{\chi_p}$. On dit qu'un relèvement ρ de $\overline{\rho}$ est *minimal en p de poids* 2 si $\rho_{|I_p}$ est du type :

$$\begin{pmatrix} \omega_p^{k-2}\chi_p & \eta \\ 0 & 1 \end{pmatrix},$$

et, pour $k(\overline{\rho}) = 2$, si de plus $\rho_{|D_p}$ est finie *i.e.* provient d'un schéma en groupes fini et plat sur $\mathbb{Z}_p$ (le cocycle η provient via la théorie de Kummer d'une unité).

Théorème 5.2. — *([35]) Soit $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ une représentation de type S à image non résoluble avec $k(\overline{\rho}) \neq p$ et $\overline{\rho}$ ordinaire. Alors $\overline{\rho}$ a un relèvement qui est minimal en tout $\ell \neq p$ et minimal de poids 2 en p.*

Remarque 5.3. — On devrait pouvoir étendre le théorème aux cas où $k(\overline{\rho}) = p$ et $\overline{\rho}_{|D_p}$ non ordinaire.

5.3. Relèvements avec Nebentypus

Le théorème suivant correspond à un théorème de Carayol qui dit que pour $p \geq 5$ ou pour $p = 3$ (resp. $p = 2$) et $\overline{\rho}$ n'est pas induite de $\mathbb{Q}(\sqrt{-3})$ (resp. $\mathbb{Q}(\sqrt{-1})$), si $\overline{\rho}$ provient par réduction d'une forme propre normalisée de $S_2(\Gamma_0(N), \chi)$, et si χ et χ' ont même réduction modulo p, $\overline{\rho}$ provient aussi d'une forme propre normalisée de $S_2(\Gamma_0(N), \chi')$ ([15]).

On suppose que l'on a un nombre premier q tel que p divise $q-1$, que $\overline{\rho}$ soit ramifiée en q, et que $\overline{\rho}_{|I_q}$ soit de la forme :

$$\begin{pmatrix} \gamma & * \\ 0 & 1 \end{pmatrix}$$

où γ est un caractère $\mathrm{Gal}(\mathbb{Q}_q(\mu_q)/\mathbb{Q}_q) \to \overline{\mathbb{F}_p}^*$.

Soit $\omega_q : \mathrm{Gal}(\mathbb{Q}_q(\mu_q)/\mathbb{Q}_q) \to \mu_{q-1}(\overline{\mathbb{Q}_q})$ le relèvement de Teichmüller du caractère cyclotomique. On choisit un isomorphisme de $\mu_{q-1}(\overline{\mathbb{Q}_q})$ sur $\mu_{q-1}(\overline{\mathbb{Q}_p})$, de sorte que l'on puisse voir ω_q comme un caractère de I_q à valeurs dans $\overline{\mathbb{Q}_p}^*$. Soit p^r l'exacte puissance de p qui divise $q-1$ et posons $\eta_q = \omega_q^{\frac{q-1}{p^r}}$, de sorte que η_q est un caractère d'ordre p^r et donc que sa réduction modulo p est triviale.

Théorème 5.4. — *([35]) Mêmes hypothèses que pour le théorème 5.1. Soit i un entier. Soit $\hat{\gamma}$ le relèvement de Teichmüller de γ. Alors $\overline{\rho}$ a un relèvement ρ qui est minimal en tout nombre premier $\ell \neq q$ et est tel que $\rho_{|I_q}$ soit de la forme :*

$$\begin{pmatrix} \hat{\gamma}\eta_q^i & * \\ 0 & 1 \end{pmatrix}.$$

5.4. Esquisse de la preuve des théorèmes

Commençons par quelques rappels sur la théorie des déformations des représentations galoisiennes ([39]).

Soit $\mathbb{F}$ un corps fini tel que l'image de $\overline{\rho}$ soit contenue dans $\mathrm{GL}_2(\mathbb{F})$. Notons W l'anneau des vecteurs de Witt à coefficients dans $\mathbb{F}$ et soit $O = W$ pour les deux premiers théorèmes et $O = W(\mu_{p^r}(\overline{\mathbb{Q}_p}))$ pour le théorème 5.4. Notons $\mathcal{C}_O$ la catégorie des O-algèbres R noethériennes locales séparées et complètes avec un isomorphisme i_R du corps résiduel $R/\mathcal{M}_R$ avec $\mathbb{F}$. Les morphismes dans $\mathcal{C}_O$ sont les morphismes $f : R \to R'$ de O-algèbres tels que $i_{R'} \circ f \simeq i_R$. Un *relèvement* de $\overline{\rho}$ est un morphisme : $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ avec un isomorphisme de ρ mod.$\mathcal{M}_R$ sur $\overline{\rho}$. Les *déformations* de $\overline{\rho}$

sont les classes d'isomorphisme de tels relèvements : deux relèvements ρ et ρ' sont donc isomorphes s'il existe $g \in \mathrm{GL}_2(R)$, $g \equiv \mathrm{id}\ \mathrm{mod}.\mathcal{M}_R$ tel que $\rho = \mathrm{int}(g)(\rho')$.

Pour chacun des théorèmes, on a un ensemble fini S de places de $\mathbb{Q}$ contenant p, ∞ et les nombres premiers ramifiés dans $\overline{\rho}$ tel que les relèvements ρ cherchés soient ceux qui sont non ramifiés hors de S et qui sont tels que pour tout $v \in S$, la restriction de ρ à I_v vérifie une condition que l'on notera $\mathcal{L}_v$. On dira que les relèvements cherchés sont ceux qui vérifient $\mathcal{L}$.

Soit G_S le groupe de Galois de l'extension maximale de $\mathbb{Q}$ qui est non ramifiée hors de S. Le groupe G_S vérifie la condition : pour tout sous-groupe ouvert H de G_S, si $H(p)$ est le plus grand quotient de H qui est un pro-p-groupe, $H(p)$ est engendré topologiquement par un ensemble fini. Il en résulte que le foncteur des déformations de $\overline{\rho}$ qui sont non ramifiées hors de S a une enveloppe, et même est représentable puisque les endomorphismes de $\overline{\rho}$ sont réduits aux homothéties. On note $\rho_{\mathrm{univ}} : G_S \to \mathrm{GL}_2(R_{\mathrm{univ}})$ la déformation universelle. Pour toute O-algèbre R de $\mathcal{C}_O$, on a donc une bijection de l'ensemble $\mathrm{specf}(R_{\mathrm{univ}})(R)$ sur l'ensemble des déformations de $\overline{\rho}$ à valeurs dans R.

De même, pour chaque $v \in S$, on a une déformation verselle $\rho_{v,\mathrm{vers}} : D_v \to \mathrm{GL}_2(R_{v,\mathrm{vers}})$ de $\overline{\rho}_{|D_v}$. Il n'est pas difficile de voir que l'on a un quotient $R_{\mathcal{L}_v}$ de $R_{v,\mathrm{vers}}$ tel que les déformations de $\overline{\rho}_{|D_v}$ qui satisfont à la condition $\mathcal{L}_v$ sont exactement celles qui proviennent d'un point de $\mathrm{specf}(R_{\mathcal{L}_v})$. On note $J_{\mathrm{vers}/\mathcal{L}_v}$ le noyau de $R_{v,\mathrm{vers}} \to R_{\mathcal{L}_v}$.

Pour $v \in S$, la restriction de ρ_{univ} au groupe de décomposition D_v induit un morphisme $r_v : R_{v,\mathrm{vers}} \to R_{\mathrm{univ}}$. On voit que le quotient $R_{\mathcal{L}}$ de R_{univ} par l'idéal engendré par les $r_v(J_{\mathrm{vers}/\mathcal{L}_v})$ représente les déformations de $\overline{\rho}$ qui satisfont à la condition $\mathcal{L}$.

L'énoncé suivant et son corollaire rassemblent des résultats dus essentiellement à Böckle, Ramakrishna et Taylor ([7],[41],[62]).

Théorème 5.5. — *On a une présentation $R_{\mathcal{L}} = O[[T_1, \ldots, T_h]]/(f_1, \ldots, f_r)$, avec moins de relations que de générateurs : $r \leq h$.*

Corollaire 3. — *Si $R_{\mathcal{L}}$ est, en tant que O-module, de type fini, alors $R_{\mathcal{L}}$ est une O-algèbre plate d'intersection complète, en particulier, $\overline{\rho}$ a un relèvement ρ qui vérifie la condition $\mathcal{L}$ cherchée.*

Esquissons la démonstration du théorème 5.5.

Remarquons tout d'abord que le déterminant des déformations qui satisfont à $\mathcal{L}$ est fixé. En effet, la condition $\mathcal{L}_v$ définit un morphime $\tilde{\eta_v} : I_v \to O^*$ tel que, si ρ_v satisfait à $\mathcal{L}_v$, la restriction du déterminant de ρ_v à I_v a pour déterminant $\tilde{\eta_v}$. Pour $v \notin S$, on pose $\tilde{\eta_v} = 1$. Comme le groupe de Galois $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ de l'extension maximale abélienne de $\mathbb{Q}$ est isomorphe au produit de ses sous-groupes d'inertie pour ℓ décrivant les nombres premiers, on voit que les η_ℓ définissent un caractère $\eta : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to O^*$ tel que les déformations qui vérifient $\mathcal{L}$ sont de déterminant η (la condition de parité $\det(\eta(c)) = -1$ est vérifiée car elle l'est pour $\overline{\rho}$ et que $p \neq 2$). On note η_v la restriction de η au groupe de décompositions D_v. La condition $\det(\rho) = \eta$ définit un sous-foncteur qui est une immersion fermée de celui des déformations qui sont non ramifiées hors de

S. On note $\rho_\eta : G_{\mathbb{Q}} \to \mathrm{GL}_2(R_\eta)$ la déformation universelle de $\overline{\rho}$ de déterminant η. De même, pour tout $v \in S$, on note $\rho_{\eta_v} : D_v \to \mathrm{GL}_2(R_{\eta_v})$ la déformation verselle de déterminant η_v de $\overline{\rho}_{|D_v}$.

Pour $R_?$ dans $\mathcal{C}_O$, on note $t_?$ le $\mathbb{F}$-espace vectoriel tangent relatif et $t_?^*$ son dual. On a donc : $t_?^* \simeq \mathcal{M}_{R_?}/(\mathcal{M}_{R_?})^2 + \mathcal{M}_O R_?$, $\mathcal{M}_O$ désignant l'idéal maximal de O. Le choix de relèvements des éléments d'une base de $t_?^*$ dans $\mathcal{M}_{R_?}$ permet d''ecrire $R_?$ comme quotient d'un anneau de séries formelles $S_?$ sur O qui identifie les espaces tangents $t_{R_?}$ et $t_{S_?}$. Il est facile de voir que deux telles présentations sont isomorphes. Si J est le noyau de $S_? \to R_?$, on pose $\mathrm{rel}(R_?) = \dim_{\mathbb{F}}(J/\mathcal{M}_{R_?}J)$. Elle ne ne dépend pas de la présentation : c'est le nombre minimal de générateurs de J.

Les espaces tangents s'identifient à des groupes de cohomologie galoisienne. En effet, t_η s'identifie l'ensemble des déformations de $\overline{\rho}$ à valeurs dans $\mathbb{F}[\epsilon]/\epsilon^2$ qui sont non ramifiées hors de S et de déterminant égal à celui de $\overline{\rho}$, et $t_{\mathcal{L}}$ sont celles qui vérifient les conditions $\mathcal{L}_v$. On a un isomorphisme $t_\eta = H_0^1 := H^1(G_S, \mathrm{ad}_0(\overline{\rho}))$, où $\mathrm{ad}_0(\overline{\rho})$ est le $\mathbb{F}$-espace vectoriel des matrices de trace nulle, G_S agissant par la conjugaison.

Pour tout $v \in S$, les déformations de $\overline{\rho}_{|D_v}$ à valeurs dans $\mathbb{F}[\epsilon]/\epsilon^2$ qui sont de déterminant η_v forment un espace vectoriel qui s'identifie à $H^1(D_v, \mathrm{ad}^0(\overline{\rho}))$. On le note $H^1_{v,0}$. Celles qui vérifient $\mathcal{L}_v$ forment un sous-espace vectoriel de $H^1_{v,0}$ que l'on note L_v. Le sous-espace $t_{\mathcal{L}} \subset t_\eta$ s'identifie au sous-espace vectoriel des $c \in H^1(G_S, \mathrm{ad}^0(\overline{\rho}))$ tels que, pour tout $v \in S$, l'image c_v de c dans $H^1(D_v, \mathrm{ad}^0(\overline{\rho}))$ appartienne à L_v. On le note $H^1_{\mathcal{L}}$. On note h^1_0, $h^1_{\mathcal{L}}$, $h^1_{v,0}$, et l_v les dimensions des $\mathbb{F}$-espaces vectoriels correspondants.

Soit, pour tout $v \in S$, $L_v^\perp$ le dual de L_v dans la dualité :

$$H^1(D_p, \mathrm{ad}_0) \times H^1(D_p, \mathrm{ad}_0(1)) \to \mathbb{F},$$

où (1) est la torsion par le caractère cyclotomique.

On note $H^1_{\mathcal{L}^\perp}$ le sous-espace vectoriel de $H^1(G_{\mathbb{Q}}, \mathrm{ad}_0(1))$ formés des c dont les images c_v dans $H^1(D_p, \mathrm{ad}_0(1))$ appartiennent à $L_v^\perp$.

Le théorème suivant est dû à Böckle ([7]).

Théorème 5.6. — *On a :*

$$\mathrm{rel}(R_{\mathcal{L}}) \leq h^1_{\mathcal{L}^\perp} + \sum_{v \in S} \mathrm{rel}(R_{\mathcal{L}_v}).$$

Donnons quelques indications sur la preuve. On peut écrire pour chaque v, la O-algèbre R_{η_v} comme un quotient d'une algèbre de séries formelles S_{η_v} à $h^1_{v,0}$ variables. Soit J_{η_v} le noyau. La théorie des déformations nous dit que l'on a un morphisme surjectif $(H^2(G_S, \mathrm{ad}_0))^* \to J_\eta/\mathcal{M}_\eta J_\eta$ et de même pour les J_{η_v}. Il en résulte que le noyau J_η d'une présentation de R_η est engendré topologiquement par les J_{η_v} et par $\mathrm{sh}^2 := \dim(\text{Ш}^2_S(\mathrm{ad}_0))$ éléments. On a donc :

$$\mathrm{rel}(R_\eta) \leq \mathrm{sh}^2 + \sum_{v \in S} \mathrm{rel}(R_{\eta_v}).$$

Pour $s \in S$, notons $\tilde{J}_v$ le noyau de $S_{\eta_v} \to R_{\eta_v} \to R_{\mathcal{L}_v}$. Alors, $R_{\mathcal{L}}$ est le quotient de S_η par l'idéal engendré par J_η et les $\tilde{J}_v$. Une chasse au diagramme permet d'en déduire que :

$$\mathrm{rel}(R_{\mathcal{L}}) \leq \sum_{v \in S} \mathrm{rel}(R_{\mathcal{L}_v}) + \mathrm{sh}^2 + \sum_{v \in S} (h^1_{\eta_v} - l_v) - h^1_\eta + h^1_{\mathcal{L}}.$$

La suite exacte de Poitou-Tate donne alors le théorème 5.6.

L' énoncé suivant rassemble des calculs locaux faits dans ([7],[41],[62]).

Théorème 5.7. — *Pour nombre premier $\ell \in S$, la O-algèbre $R_{\mathcal{L}_\ell}$ est lisse de dimension relative $h^0(D_\ell, \mathrm{ad}_0)$ si $\ell \neq p$, et $h^0(D_p, \mathrm{ad}_0) + 1$ si $\ell = p$.*

Notons d_ℓ la dimension de $R_{\mathcal{L}_\ell}$ et $d_\infty = 0$. Le théorème 5.6 donne alors, puisque $R_{\mathcal{L}_v}$ est d'intersection complète :

$$\mathrm{rel}(R_{\mathcal{L}}) \leq h^1_{\mathcal{L}^\perp} + \sum_{v \in S} (l_v - d_v).$$

On a la formule de Wiles ([67]):

$$h^1_{\mathcal{L}} - h^1_{\mathcal{L}^\perp} = h^0(G_{\mathbb{Q}}, \mathrm{ad}_0) - h^0(G_{\mathbb{Q}}, \mathrm{ad}_0(1)) + \sum_{v \in S} (l_v - h^0(D_v, \mathrm{ad}_0)).$$

Les h^0 globaux sont nuls. La contribution de ∞ est -1. On en déduit :

$$h^1_{\mathcal{L}} - \mathrm{rel}(R_{\mathcal{L}}) \geq -1 + \sum_{\ell \in S} (d_\ell - h^0(D_\ell, \mathrm{ad}_0)).$$

Le théorème 5.5 résulte alors du théorème 5.7.

Prouvons les théorèmes 5.1, 5.2 et 5.4.

D'après le corollaire 3, il suffit de prouver que $R_{\mathcal{L}}/p$ est finie. Comme $\overline{\rho}$ est absolument irréductible, $R_{\mathcal{L}}/p$ est engendrée par les traces des images des éléments de $G_{\mathbb{Q}}$ ([16]). Par un lemme simple d'algèbre commutative, on voit alors qu'il suffit de prouver que l'image de $G_{\mathbb{Q}}$ dans $\mathrm{GL}_2(R_{\mathcal{L}}/p)$ est finie ([34]).

Soit F un corps totalement réel comme dans le théorème 4.1. On considère alors dans chacun des cas la déformation universelle $G_F \to \mathrm{GL}_2(R_F)$ de la représentation irréductible $\overline{\rho}_{|G_F}$, de déterminant $\eta_{|G_F}$ et satisfaisant à certaines conditions locales. Rappelons que η est le déterminant des déformations satisfaisant $\mathcal{L}$. Ces conditions locales sont choisies de sorte qu'elles sont satisfaites par la restriction à G_F de tout relèvement $\rho : G_{\mathbb{Q}} \to GL(R)$ de $\overline{\rho}$, R étant une O-algèbre de $\mathcal{C}_O$ telle que $pR = 0$. Par exemple, dans le cas des relèvements minimaux pour $k(\overline{\rho}) \neq p + 1$, ces conditions locales sont d'être non ramifiée pour tout idéal premier de F qui n'est pas au dessus de p, et pour $\wp$ au dessus de p, la condition est d'être un quotient d'une représentation cristalline de $D_\wp$ de poids de Hodge-Tate $(0, k(\overline{\rho}) - 1)$, et donc de provenir d'un module de Fontaine-Laffaille de poids 0 et $k - 1$ ([30]).

Ainsi, on a un morphisme $R_F \to R_{\mathcal{L}}$ tel que $G_F \to \mathrm{GL}_2(R_{\mathcal{L}}/p)$ se factorise à travers $G_F \to \mathrm{GL}_2(R_F)$. Pour prouver que l'image de $G_{\mathbb{Q}}$ dans $\mathrm{GL}_2(R_{\mathcal{L}}/p)$ est finie, il suffit donc de prouver que celle de G_F dans $\mathrm{GL}_2(R_F/p)$ l'est. Pour ceci, il suffit de prouver que R_F est de type fini en tant que O-module. Pour ceci, on considère l'algèbre de Hecke $\mathbb{T}$ des formes modulaires de Hilbert relatives à F de poids et niveau convenables. Par exemple, dans le cas des relèvements minimaux, le poids est $k(\overline{\rho})$ et le niveau 1. La représentation $\overline{\rho}_{|G_F}$ étant modulaire, elle définit un idéal maximal de $\mathbb{T}$; soit $\widehat{\mathbb{T}}$ le complété de $\mathbb{T}$ en cet idéal. On a un morphisme $R_F \to \widehat{\mathbb{T}}$. Dans le cas où $\overline{\rho}_{|D_p}$ est irréductible, le iii) du théorème 3.1 entraîne que $R_F \simeq \widehat{\mathbb{T}}$, et donc que R_F est un O-module de type fini puisque $\widehat{\mathbb{T}}$ l'est. Dans le cas ordinaire, comme, dans le cas ii) de théorème 3.1, on utilise [55] qui n'implique pas que $R_F \simeq \widehat{\mathbb{T}}$, il faut vérifier que [55] entraîne bien que R_F est un O-module de type fini, ce qui est fait dans [35], utilisant la théorie de Hida ([33]).

6. SYSTÈMES COMPATIBLES

Soit, comme dans le paragraphe précédent, $\overline{\rho}$ une représentation de type S à image non résoluble ($p \neq 2$). Soit ρ un relèvement de $\overline{\rho}$ comme dans l'un des théorèmes 5.1, 5.2, 5.4. Pour tout ℓ, on note r_ℓ la représentation du groupe de Weil-Deligne $\mathrm{WD}_\ell \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ associée à la représentation géométrique ρ (1.2). La conjecture de Fontaine-Mazur entraîne que ρ devrait être membre d'un système compatible de représentations ℓ-adiques (ρ_ι). Le théorème suivant, moins fort, suffit pour prouver le théorème 2.1. Il est essentiellement dû à Dieulefait ([24]; voir aussi [68]) :

Théorème 6.1. — *Il existe un corps de nombres E et, pour tout q et tout plongement $\iota_q : E \hookrightarrow \overline{\mathbb{Q}_q}$, une représentation $\rho_\iota : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_q})$ qui est impaire, irréductible. De plus :*

- i) il existe $\iota_p : E \hookrightarrow \overline{\mathbb{Q}_p}$ tel que ρ_{ι_p} soit isomorphe à ρ ;

- ii) pour ℓ et q nombres premiers avec $\ell \neq p, q$, et pour ι_q plongement de E dans $\overline{\mathbb{Q}_q}$, les représentations du groupe de Weil-Deligne WD_ℓ associèes à ρ et à ρ_{ι_q} sont isomorphes, via ι et ι_q ;

- iii) On suppose que dans le cas de relèvement avec Nebentypus (5.4) on a $k(\overline{\rho}) = 2$. Soit ι_q de caractéristique $q \neq 2, p$. La restriction à I_p de ρ_{ι_q} est celle définie par r_p. Si ρ n'est pas ramifiée en q, la restriction de ρ_{ι_q} à D_q est cristalline de même poids que ρ. Si $\rho_{|I_q}$ est comme dans 5.3, $\rho_{|D_q}$ est soit semi-stable de poids $(0,1)$, soit cristalline après restriction à $\mathbb{Q}_q(\mu_q)$ et de poids de Hodge-Tate $(0,1)$.

La preuve utilise des idées de Taylor ([63]). La version potentielle de la conjecture de Serre (th. 4.1) donne qu'il existe F corps totalement réel galoisien sur $\mathbb{Q}$ tel que $\rho_{|G_F}$ provienne d'une forme modulaire de Hilbert f pour F. Par [3], pour tout sous-corps F' de F tel que F/F' soit un groupe résoluble, $\rho_{|G_{F'}}$ provient d'une forme modulaire de Hilbert $f_{F'}$ pour F'. L'existence de E et de ι_p provient alors de l'existence des corps des coefficients pour les formes $f_{F'}$. Grâce au théorème de Brauer, on écrit ρ comme une somme virtuelle de tordues de représentations associées aux $f_{F'}$ et à ι_p. On définit ρ_ι comme la somme virtuelle correspondante, ι_p étant remplacé par ι. On prouve que c'est une vraie représentation. Les propriétés de compatibilité résultent d'un théorème de Carayol et Taylor ([14],[58]), de Saito ([46],[45]), Breuil ([9]) et Berger ([4]).

7. PREUVE DU THÉORÈME

Pour p un nombre premier, soit $\mathrm{S}(p)$ l'énoncé : une représentation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ de type S non ramifiée hors de p provient d'une forme modulaire. Pour p nombre premier $\neq 2$ et k entier avec $2 \leq k \leq p+1$, soit $\mathrm{S}(k,p)$ l'énoncé : une représentation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ de type S non ramifiée hors de p avec $k(\overline{\rho}) = k$ provient d'une forme modulaire. Par torsion par une puissance du caractère cyclotomique, on voit que $\mathrm{S}(p)$ est la conjonction des énoncés $\mathrm{S}(k,p)$. Comme $k(\overline{\rho})$ est pair pour toute représentation de type S qui est non ramifiée hors de p, on voit que l'on a à considérer $\mathrm{S}(k,p)$ que pour k pair.

L'énoncé $\mathrm{S}(2)$ est un théorème de Tate. La démonstration utilise la structure des groupes de décompositions et les minorations de discriminants. Serre a prouvé $\mathrm{S}(3)$ par un argument analogue.

Théorème 7.1. — *(Tate, Serre) Soit $\overline{\rho}$ une représentation continue de $G_{\mathbb{Q}}$ dans* $\mathrm{GL}_2(\overline{\mathbb{F}_2})$ *(resp.* $\mathrm{GL}_2(\overline{\mathbb{F}_3})$*) qui est non ramifiée hors de* 2 *(resp.* 3*). Alors $\overline{\rho}$ est réductible.*

Comme $\mathrm{S}(2)$ est vrai, on suppose désormais p impair.

La stratégie pour prouver $\mathrm{S}(p)$ pour tout p est une récurrence sur p (on peut aussi la présenter comme une récurrence sur le poids k). Soit $\overline{\rho}$ une représentation de type S de poids $k(\overline{\rho}) = k$ et de conducteur 1. Si $\overline{\rho}$ a une image résoluble, $\overline{\rho}$ est modulaire grâce au théorème de Langlands et Tunnell. Sinon, on relève $\overline{\rho}$ en une représentation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ grâce à l'un des théorèmes du §5. On obtient grâce au théorème 6.1 un système compatible (ρ_ι) dont ρ fait partie. On choisit un ι_q de caractéristique q et on considère la réduction $\overline{\rho_{\iota_q}}$ modulo q de ρ_{ι_q}. Si elle est irréductible, l'hypothèse de récurrence entraîne qu'elle est modulaire. On vérifie que l'on peut appliquer le théorème 3.1 et ρ_{ι_q} est modulaire (si $\overline{\rho_{\iota_q}}$ est réductible , on doit vérifier les hypothèses du i) du théorème 3.1). Il en résulte que (ρ_ι) est modulaire, et donc $\overline{\rho}$.

Proposition 7.2. — *i)* $\mathrm{S}(2,p)$ *et* $\mathrm{S}(4,p)$ *sont vrais.*

ii) On suppose $\mathrm{S}(k,p)$ *(donc $k \leq p+1$). Alors* $\mathrm{S}(k,q)$ *est vrai pour tout nombre premier q (tel que $k \leq q+1$).*

En particulier, si $\mathrm{S}(p)$ est vrai, $\mathrm{S}(k,q)$ l'est pour $k \leq p+1$. Il en résulte que $\mathrm{S}(q)$ l'est si $q < p$ et, pour prouver le théorème de Khare, il suffit de prouver $\mathrm{S}(p)$ pour une infinité de premiers.

Preuve de la proposition

Prouvons $\mathrm{S}(2,p)$. Soit $\overline{\rho}$ une représentation modulo p de type S, de poids 2 et de conducteur 1 et dont l'image est non résoluble. On relève en un sytème compatible (ρ_ι) de poids 2 non ramifié partout. On considère la réduction modulo 3 de ρ_{ι_3}, pour ι_3 de caractéristique 3. On sait par la proposition précédente que cette réduction n'est pas irréductible. Comme son déterminant est $\overline{\chi_3}$, on voit qu'elle est isomorphe à $1 \oplus \overline{\chi_3}$. Alors comme ρ a poids $2 \leq 3-1$, il résulte facilement de la théorie des schémas en groupes finis et plats que la restriction de ρ_{ι_3} à D_3 est ordinaire. Il résulte alors du i) du théorème 3.1 que ρ_{ι_3} provient d'une forme modulaire. Il en est de même de (ρ_λ) et par suite de $\overline{\rho}$.

Prouvons le ii). On relève $\overline{\rho}$ de caractéristique q en ρ minimal de type cristallin, puis on met ρ dans un système compatible (ρ_ι). On choisit ι_p de caractéristique p et on considère la réduction $\overline{\rho_{\iota_p}}$ de ρ_{ι_p}. La restriction de ρ_{ι_p} à D_p est cristalline de poids de Hodge-Tate 0 et $k-1$. Il résulte de [30] que si $k \leq p-1$, on a $k(\overline{\rho_{\iota_p}}) = k$ et que, si la restriction de $\overline{\rho_{\iota_p}}$ à D_p est réductible, alors $\rho_{\iota_p|D_p}$ est ordinaire. Si $k = p+1$, il résulte de [5] que soit $\rho_{\iota_p|D_p}$ est ordinaire, soit $k(\overline{\rho_{\iota_p}}) = 2$ et la restriction à D_p de $\overline{\rho_{\iota_p}}$ est irréductible.

Le i) entraîne que si $k(\overline{\rho_{\iota_p}}) = 2$, $\overline{\rho_{\iota_p}}$ est réductible, donc aussi sa restriction à D_p. On voit que l'on est dans l'un des cas :

- $\overline{\rho_{\iota_p}}$ est irréductible, et si $k = p+1$, $(\rho_{\iota_p})_{|D_p}$ est ordinaire ;
- $\overline{\rho_{\iota_p}}$ est réductible et $\rho_{p|D_p}$ est ordinaire.

Dans le premier cas, $\overline{\rho_{\iota_p}}$ est modulaire par hypothèse. Un lemme facile prouve que si la restriction de $\overline{\rho_{\iota_p}}$ à $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ est réductible, $\rho_{\iota_p|D_p}$ est ordinaire. On voit que les hypothèses du ii) ou du iii) du théorème 3.1 sont vérifiées et ρ_{ι_p} est modulaire. Dans le cas $\overline{\rho_{\iota_p}}$ réductible, le i) de 3.1 donne la modularité de ρ_{ι_p}. On en déduit celle de $\overline{\rho}$. Le ii) est prouvé.

L'énoncé $\mathrm{S}(4,p)$ résulte du ii) et du fait que $\mathrm{S}(3)$ est vraie.

Proposition 7.3. — $\mathrm{S}(6,p)$ *est vrai pour tout* $p \geq 5$ *;* $\mathrm{S}(5)$ *est vraie.*

Preuve. La proposition précédente entraîne qu'il suffit de prouver $\mathrm{S}(6,5)$ *i.e.* qu'il n'existe pas de représentations de type S de poids 6 et de caractéristique 5 qui soit non ramifiée hors de 5. Soit donc $\overline{\rho_5}$ une telle représentation . On la relève en une représentation ρ irréductible qui est minimale de type semi-stable. Elle est donc de poids 2 semi-stable en 5. La version potentielle de la conjecture de Serre (th. 4.1) et le ii) du théorème 3.1 entraînent qu'il existe un corps totalement réel F galoisien sur $\mathbb{Q}$ tel que la restriction de ρ à G_F provienne d'une forme modulaire de Hilbert pour F qui est de poids 2 et Steinberg en 5. La représentation ρ_{G_F} provient alors d'une variété abélienne. Un argument de descente donne que ρ provient d'une variété abélienne sur $\mathbb{Q}$

qui a bonne réduction hors de 5 et est semi-stable en 5 ([34]). Mais Brumer et Kramer ont prouvé qu'une telle variété abélienne n'existe pas ([12], voir aussi Schoof [48]). Les résultats de Brumer-Kramer et Schoof utilisent des minorations de discriminants comme pour le théorème 7.1. L'étude de la ramification en p est beaucoup plus délicate ; ces résultats généralisent des théorèmes de Fontaine et Abrashkin ([28],[2]).

7.0.1. Le cas général de conducteur 1. — On a donc prouvé $\mathrm{S}(p)$ pour $p \leq 5$. Avec la proposition 7.2, on voit qu'il suffit de prouver que, si $p \geq 5$ et si $\mathrm{S}(p)$ est vrai, il existe $P > p$ tel que $\mathrm{S}(P)$ soit vrai. On prend pour P le plus petit premier $> p$ qui n'est pas de Fermat : $P-1$ est divisible par un nombre premier ℓ impair, et on note ℓ^r la plus grande puissance de ℓ qui divise $P-1$.

La théorie analytique des nombres premiers donne que l'on peut choisir ℓ tel que :

Lemme 1. — *([35]) Posons $\ell^r = 2m+1$. On a :*

$$\frac{P}{p} \leq \frac{2m+1}{m+1} - \frac{m}{p(m+1)},\ p+1 \geq \frac{m+1}{2m+1}(P-1)+2 = (P+1) - \frac{m}{2m+1}(P-1).$$

Soit donc $\overline{\rho}$ une représentation de type S de caractéristique P, de poids k, $2 \leq k \leq P+1$, non ramifiée hors de P. Par la proposition 7.1, on connait $\mathrm{S}(k,P)$ pour $k \leq p+1$.

Si la restriction au groupe de décomposition D_P est irréductible, la représentation obtenue en tordant $\overline{\rho}$ par une puissance du caractère cyclotomique convenable est de poids $P+3-k$. Il résulte de la première inégalité du lemme 1 que soit k, soit $P+3-k$ est $\leq p+1$, et on conclut.

Supposons donc $\overline{\rho}$ ordinaire. On la relève en un système compatible (ρ_ι) de poids 2 grâce aux théorèmes 5.2 et 6.1. Soit ι_ℓ un plongement de caractéristique ℓ et soit $\overline{\rho_{\iota_\ell}}$ la réduction de ρ_{ι_ℓ}. Si la restriction de $\overline{\rho_{\iota_\ell}}$ à $\mathbb{Q}(\mu_\ell)$ est réductible, ou si $\overline{\rho_{\iota_\ell}}$ est irréductible à image résoluble donc modulaire par Langlands-Tunnell, on vérifie, de manière similaire à la proposition 7.2, que le théorème 3.1 s'applique, et ρ_{ι_ℓ} est modulaire, donc aussi $\overline{\rho}$. Sinon, on choisit un relèvement avec Nebentypus ρ' de $\overline{\rho_{\iota_\ell}}$ grâce au théorème 5.4. On choisit dans le théorème 5.4 l'entier i de sorte que le caractère $\hat{\gamma}\eta_q^i$ soit égal à ω_P^j avec :

$$j \in [\frac{m}{2m+1}(P-1), \frac{m+1}{2m+1}(P-1)],$$

où ω_P est le représentant de Teichmüller du caractère cyclotomique $\mathrm{Gal}(\mathbb{Q}_P(\mu_P)/\mathbb{Q}_P) \to \mathbb{F}_P^*$ (rappelons que l'on choisit un isomorphisme de $\mu_{P-1}(\overline{\mathbb{Q}_\ell})$ sur $\mu_{P-1}(\overline{\mathbb{Q}_P})$). On prolonge ρ' en un système compatible $(\rho'_{\iota'})$ tel qu'il existe ι'_ℓ de caractéristique ℓ avec ρ'_{ι_ℓ} isomorphe à ρ' grâce à 6.1. On choisit ι'_P de caractèristique P de sorte que ι'_ℓ et ι'_P soient compatibles à l'identification $\mu_{P-1}(\overline{\mathbb{Q}_\ell}) \simeq \mu_{P-1}(\overline{\mathbb{Q}_P})$. Il résulte alors de [47] et [10] que la réduction $\overline{\rho'_{\iota_P}}$, tordue par une puissance convenable du caractère cyclotomique $\overline{\chi_p}$, est de poids $j+2$ ou $P+1-j$. Le choix de j et le lemme 1 font que $j+2$ et $P+1-j$ sont $\leq p+1$. On a donc que $\overline{\rho'_{\iota_P}}$ est soit modulaire soit réductible. On s'assure que les théorèmes "MR" permettent d'en déduire que $(\rho'_{\iota'})$, puis que (ρ_ι) sont modulaires, donc aussi $\overline{\rho}$. Ceci achève la preuve du théorème 2.1.

Le corollaire 1 résulte alors de la technique qui consiste à “tuer la ramification” ([34]). Si $q \neq 2$, on relève $\overline{\rho}$ de poids 2 et de niveau q en un système compatible (ρ_ι) qui est minimal de poids 2. On considère $\overline{\rho_{\iota_q}}$ pour ι_q de caractéristique q. On la relève en un système compatible qui est minimal, donc n'est pas ramifié en q (mais n'est plus en général de poids 2). On déduit du théorème 2.1 qu'il est modulaire.

Le corollaire 2 résulte du théorème et des théorèmes “MR” ([36]).

RÉFÉRENCES

[1] *Périodes p-adiques*. Société Mathématique de France, Paris, 1994. Papers from the seminar held in Bures-sur-Yvette, 1988, Astérisque No. 223 (1994).

[2] Victor A. Abrashkin. Ramification in étale cohomology. *Invent. Math.*, 101(3):631–640, 1990.

[3] James Arthur and Laurent Clozel. *Simple algebras, base change, and the advanced theory of the trace formula*, volume 120 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1989.

[4] Laurent Berger. Limites de représentations cristallines. *Compos. Math.*, 140(6):1473–1498, 2004.

[5] Laurent Berger, Hanfeng Li, and Hui June Zhu. Construction of some families of 2-dimensional crystalline representations. *Math. Ann.*, 329(2):365–377, 2004.

[6] Don Blasius and Jonathan D. Rogawski. Motives for Hilbert modular forms. *Invent. Math.*, 114(1):55–87, 1993.

[7] Gebhard Böckle. A local-to-global principle for deformations of Galois representations. *J. Reine Angew. Math.*, 509:199–236, 1999.

[8] Gebhard Böckle. Presentations of universal deformation rings. *preprint*, pages 1–27, 2005.

[9] Christophe Breuil. Une remarque sur les représentations locales p-adiques et les congruences entre formes modulaires de Hilbert. *Bull. Soc. Math. France*, 127(3):459–472, 1999.

[10] Christophe Breuil and Ariane Mézard. Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbf{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ en $l = p$. *Duke Math. J.*, 115(2):205–310, 2002. With an appendix by Guy Henniart.

[11] Sharon Brueggeman. The nonexistence of certain Galois extensions unramified outside 5. *J. Number Theory*, 75(1):47–52, 1999.

[12] Armand Brumer and Kenneth Kramer. Non-existence of certain semistable abelian varieties. *Manuscripta Math.*, 106(3):291–304, 2001.

[13] Kevin Buzzard and Richard Taylor. Companion forms and weight one forms. *Ann. of Math. (2)*, 149(3):905–919, 1999.

[14] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[15] Henri Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[16] Henri 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)*, volume 165 of *Contemp. Math.*, pages 213–237. Amer. Math. Soc., Providence, RI, 1994.

[17] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Internat. Press, Cambridge, MA, 1994.

[18] Pierre Deligne. Formes modulaires et représentations ℓ-adiques. In *Séminaire Bourbaki 355*, pages 139–172. Lecture Notes in Math., Vol. 179. Springer, Berlin, 1971.

[19] Pierre Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[20] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[21] Fred Diamond. An extension of Wiles' results. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 475–489. Springer, New York, 1997.

[22] Fred Diamond and Richard Taylor. Lifting modular mod l representations. *Duke Math. J.*, 74(2):253–269, 1994.

[23] Fred Diamond and Richard Taylor. Nonoptimal levels of mod l modular representations. *Invent. Math.*, 115(3):435–462, 1994.

[24] Luis V. Dieulefait. Existence of families of Galois representations and new cases of the Fontaine-Mazur conjecture. *J. Reine Angew. Math.*, 577:147–151, 2004.

[25] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[26] Bas Edixhoven. Serre's conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 209–242. Springer, New York, 1997.

[27] J. Ellenberg. Serre's conjecture over $\mathbb{F}_9$. *Annals of Mathematics*, 161(3):1111–1142, 2005.

[28] Jean-Marc Fontaine. Il n'y a pas de variété abélienne sur $\mathbf{Z}$. *Invent. Math.*, 81(3):515–538, 1985.

[29] Jean-Marc Fontaine. Représentations l-adiques potentiellement semi-stables. *Astérisque*, (223):321–347, 1994. Périodes p-adiques (Bures-sur-Yvette, 1988).

[30] Jean-Marc Fontaine and Guy Laffaille. Construction de représentations p-adiques. *Ann. Sci. École Norm. Sup. (4)*, 15(4):547–608 (1983), 1982.

[31] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 41–78. Internat. Press, Cambridge, MA, 1995.

[32] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990.

[33] Haruzo Hida. On p-adic Hecke algebras for GL_2 over totally real fields. *Ann. of Math. (2)*, 128(2):295–384, 1988.

[34] C Khare and J.-P Wintenberger. On Serre's reciprocity conjecture for 2-dimensional mod p representations of the Galois group $G_{\mathbb{Q}}$. *arXiv math.NT/0412076*, 2004.

[35] Chandrashekhar Khare. On Serre's modularity conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified outside p, preprint.

[36] Chandrashekhar Khare. Serre's modularity conjecture, preprint.

[37] Mark Kisin. Modularity for some geometric Galois representations. *preprint*, pages 1–21, 2005.

[38] Jayanta Manoharmayum. Serre's conjecture for mod 7 Galois representations. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 141–149. Birkhäuser, Basel, 2004.

[39] Barry Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 243–311. Springer, New York, 1997.

[40] Laurent Moret-Bailly. Groupes de Picard et problèmes de Skolem. I, II. *Ann. Sci. École Norm. Sup. (4)*, 22(2):161–179, 181–194, 1989.

[41] Ravi Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur. *Ann. of Math. (2)*, 156(1):115–154, 2002.

[42] Kenneth A. Ribet. Galois representations attached to eigenforms with Nebentypus. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 17–51. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[43] Kenneth A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[44] Kenneth A. Ribet and William A. Stein. Lectures on Serre's conjectures. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 143–232. Amer. Math. Soc., Providence, RI, 2001.

[45] Takeshi Saito. Hilbert modular forms and p-adic Hodge theory. *preprint*, pages 1–40.

[46] Takeshi Saito. Modular forms and p-adic Hodge theory. *Invent. Math.*, 129(3):607–620, 1997.

[47] David Savitt. On a conjecture of Conrad, Diamond, and Taylor. *Duke Math. J.*, 128(1):141–197, 2005.

[48] René Schoof. Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only. *Compos. Math.*, 141(4):847–868, 2005.

[49] Jean-Pierre Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 191–268. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[50] Jean-Pierre Serre. Valeurs propres des opérateurs de Hecke modulo l. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, 1974)*, pages 109–117. Astérisque, Nos. 24–25. Soc. Math. France, Paris, 1975.

[51] Jean-Pierre Serre. *Œuvres. Vol. III.* Springer-Verlag, Berlin, 1986. 1972–1984.

[52] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[53] C. M. Skinner and A. J. Wiles. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.*, (89):5–126 (2000), 1999.

[54] C. M. Skinner and A. J. Wiles. Base change and a problem of Serre. *Duke Math. J.*, 107(1):15–25, 2001.

[55] C. M. Skinner and A. J. Wiles. Nearly ordinary deformations of irreducible residual representations. *Ann. Fac. Sci. Toulouse Math. (6)*, 10(1):185–215, 2001.

[56] H. P. F. Swinnerton-Dyer. On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 1–55. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[57] John Tate. The non-existence of certain Galois extensions of $\mathbf{Q}$ unramified outside 2. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 153–156. Amer. Math. Soc., Providence, RI, 1994.

[58] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[59] Richard Taylor. On Galois representations associated to Hilbert modular forms. II. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 185–191. Internat. Press, Cambridge, MA, 1995.

[60] Richard Taylor. On the meromorphic continuation of degree two L-functions. *Preprint*, pages 1–53, 2001.

[61] Richard Taylor. Remarks on a conjecture of Fontaine and Mazur. *J. Inst. Math. Jussieu*, 1(1):125–143, 2002.

[62] Richard Taylor. On icosahedral Artin representations. II. *Amer. J. Math.*, 125(3):549–566, 2003.

[63] Richard Taylor. Galois representations. *Ann. Fac. Sci. Toulouse Math. (6)*, 13(1):73–119, 2004.

[64] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[65] Takeshi Tsuji. Semi-stable conjecture of Fontaine-Jannsen: a survey. *Astérisque*, (279):323–370, 2002. Cohomologies p-adiques et applications arithmétiques, II.

[66] Jerrold Tunnell. Artin's conjecture for representations of octahedral type. *Bull. Amer. Math. Soc. (N.S.)*, 5(2):173–175, 1981.

[67] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[68] Jean-Pierre Wintenberger. On p-adic geometric representations of $G_{\mathbb{Q}}$. *preprint*, pages 1–9, 2005.

Jean-Pierre WINTENBERGER

Université Louis Pasteur et CNRS
I.R.M.A.
7, rue René Descartes
F–67084 Strasbourg Cedex
E-mail : wintenb@math.u-psud.fr