

POTENTIAL MODULARITY AND MODULARITY LIFTING THEOREMS

JEAN-PIERRE WINTENBERGER

These notes are preliminary. I apologize for obscurities and possible mistakes. (?) are points to be precised.

1) Introduction.

- Galois representations attached to automorphic forms
- Modularity and potential modularity of Galois representations

2) Potential modularity theorem

- Statement
- Plan of the proof
- existence of abelian varieties
- end of the proof.

3) Modularity lifting theorem

- Automorphic representations for definite quaternion algebras. Morphism $R \rightarrow T$
- Auxiliary primes ; freeness of space of modular forms
- Galois cohomology
- Patching argument

1. INTRODUCTION

The references for the introduction are [2], [7], [3], [4] and [8].

Let F be a number field (finite extension of \mathbb{Q}). Let $\overline{\mathbb{Q}}$ be an algebraic closure of F and let G_F be the Galois group $\text{Gal}(\overline{\mathbb{Q}}/F)$. For p a prime number, a p -adic Galois representation ρ is a continuous morphism $G_F \rightarrow \text{GL}_n(\overline{\mathbb{Q}}_p)$. It is not difficult to prove that the continuity of ρ implies that ρ has image in $\text{GL}_n(E)$ for a finite extension E of \mathbb{Q}_p (Breuil Mezard "Multiplicité modulaires..." Duke 115). For this course, we will be interested in (absolutely) irreducible ρ .

Cuspidal automorphic representations that satisfy a condition of algebraicity should give rise to irreducible p -adic Galois representations. More precisely, the picture is that if π is an algebraic cuspidal automorphic representation, there is a finite extension E of \mathbb{Q} (the field of coefficients), and for every embedding $\lambda : E \hookrightarrow \overline{\mathbb{Q}}_p$ for p a prime number, there exists an irreducible p -adic Galois representation $\rho_{\pi,\lambda}$ associated to π and λ . The link between ρ and π is given by the local Langlands correspondence.

An important question in the subject is the characterisation of the irreducible p -adic Galois representations ρ arising from such π . There are conditions. They come from the conjectured fact that ρ should come from

algebraic geometry, more precisely should be a subrepresentation of a quotient of the Galois representation given by the étale p -adic cohomology of a smooth projective variety defined over F ([4]). The representation ρ then has to be "geometric" *i.e.*

- unramified outside a finite set of primes of F : outside the primes the bad reduction and the primes above p ;
- for v a place of F above p , its restriction to the decomposition group D_v should satisfy the Fontaine's condition to be potentially semi-stable ([3]). This is a condition on the restriction of ρ to the inertia subgroup I_v .

A conjecture of Fontaine and Mazur states that an irreducible p -adic Galois representation that is geometric comes from algebraic geometry. It is conjectured these properties characterise the Galois irreducible representations that arise from a π .

A justification to the fact that Galois representations that come from algebraic geometry should come from a π are the (conjectured) converse theorems : roughly L functions which has convenient functional equations comes from a π .

The picture is proved for $n = 1$ ([7]) and almost proved for if $n = 2$ and $F = \mathbb{Q}$ and ρ odd (it corresponds to modular forms of weight $k \geq 1$ for $\Gamma_1(N)$; for $k \geq 2$ they appear in the cohomology of varieties that are symmetric fibre product of the universal generalised elliptic curve over modular curves. For even Galois representations which should correspond to Maass forms one know nothing. For $k = 1$ it is geometric as it has finite image !

1.1. Algebraic automorphic cuspidal representations and their Galois representations. We will be very below the ambition of the title ! We will not give a systematic survey on automorphic representation. We will give some facts and based on examples : $n = 1$ and $E = \mathbb{Q}$, $n = 2$. For more details see Taylor's ICM paper [8].

Let $G = \mathrm{GL}_n$ and F a number field, $\mathbb{A} := \mathbb{A}_F$ the adèles of F and $\mathrm{GL}_n(\mathbb{A}_F)$ the linear adelic group. Cuspidal automorphic representations π are adelic tensor product of representations π_v for v place of F . The local representation π_v is for v finite a representation of $\mathrm{GL}_n(F_v)$. For v infinite, π_v is a representation of $\mathfrak{gl}_n \times \mathcal{O}_n$. So we may view a cuspidal automorphic representation π as a collection of π_v . What links the π_v is that π and define the cuspidal automorphic representations is that they are realised as irreducible factor of representations on smooth functions $f : \mathrm{GL}_n(F) \backslash \mathrm{GL}_n(\mathbb{A}_F) \rightarrow \mathbb{C}$. Smoothness means C^∞ on $\mathrm{GL}_n(\mathbb{A}_\infty)$ and locally constant on $\mathrm{GL}_n(\mathbb{A}_f)$.

Local Langlands correspondence for v non archimedean establishes a bijection of the isomorphism classes of smooth irreducible representations of $\mathrm{GL}_n(F_v)$ in a \mathbb{C} -vector space with isomorphism classes of ϕ semisimple representations of the Weil-Deligne groupe WD_v . (smooth means that the stabiliser of every vector v is open ; smooth are admissible that means that

for U open compact subgroup of $\mathrm{GL}_n(F_v)$, V^U is finite dimensional)(it has been proved by Harris-Taylor).

Let v be a non archimedean prime. The Weil group W_{F_v} noted W_v is the group of elements of D_v whose image in D_v/I_v belongs to the subgroup of $\mathrm{Gal}(\overline{k_v}/k_v)$ generated by Frob_v ($\mathrm{Frob}_v(x) = x^{q_v}$ for $x \in \overline{k_v}$, where q_v is the number of elements of k_v). We have an exact sequence :

$$1 \rightarrow I_v \rightarrow W_v \rightarrow \mathbb{Z} \rightarrow 1.$$

The map $W_v \rightarrow \mathbb{Z}$ is designed by $\| \quad \|$. Let K be any field. We call a representation \underline{r} of the Weil-Deligne WD_v group in $\mathrm{GL}(V)$, V a finite dimensional vector space a pair (r, N) of a representation r of W_v which is trivial on an open subgroup of I_v and a nilpotent element $N \in \mathrm{End}(V)$ satisfying $\rho(w)N\rho(w)^{-1} = q^{\|w\|}N$, where q is the cardinality of the residue field k_v .

The notion of Weil-Deligne group representations is justified by a theorem of Grothendieck :

Theorem 1.1. *Let v be of characteristic $\neq p$. There is an equivalence of categories between continuous representations of D_v in $\mathrm{GL}_n(\overline{\mathbb{Q}_p})$ and representations of WD_v that are such that $r(\phi)$ is a p -adic unit for every ϕ lifting the Frobenius.*

Proof. Let us sketch a proof. There exists a finite extension F'_v of F_v such that the restriction of ρ to $G_{F'_v}$ is tame. Let Δ'_v be the Galois group of the maximal tamely ramified extension of F'_v . Let σ' and ϕ' be elements of Δ'_v that generates the inertia subgroup and project to the Frobenius respectively. One has $\phi'\sigma'\phi'^{-1} = \sigma'^{q'}$ where q' is the number of elements of the residue field of F'_v . From this relation one deduces that the eigenvalues of $\rho(\sigma')$ are roots of unity (they form a multiset that is invariant by raising to the q' power). We enlarge F'_v so that $\rho(\sigma')$ is unipotent. Let t_p be the projection of $I_v \rightarrow \mathbb{Z}_p(1)$ to its p -part. We choose a generator of $\mathbb{Z}_p(1)$. We define the restriction of r to I_v by the formula : $r(\tau) = \rho(\tau) \exp(-t_p(\tau)N)$ with N the nilpotent such that $\rho(\sigma') = \exp(t_p(\sigma')N)$. This defines a representation of I_v as $\rho(I_v)$ commutes with N . We extend r to W_v by the formula $r(\phi) = \rho(\phi)$ where $\phi \in D_v$ lifts the Frobenius. It defines a representation. We have the formula :

$$\rho(\phi^n \sigma) = r(\phi^n \sigma) \exp(t_p(\sigma)N)$$

where $n \in \mathbb{Z}$ and $\sigma \in I_v$.

□

Remark The Frobenius simplification of \underline{r} consists to replace $r(\phi)$ by its semisimple part.

For almost all nonarchimedean v , π_v is not ramified (is an unramified principal series). That means that $\pi_v(\mathrm{GL}_n(\mathbb{Z}_p)) = \{1\}$. Then, by local Langlands, it corresponds to an admissible unramified representation of WD_v . The representation \underline{r} is unramified if r is trivial on the inertia I_v and $N = 0$ (it is

compatible with the theorem of Grothendieck). They correspond to the date of the image of Frobenius which a semisimple conjugacy class in $\mathrm{GL}_n(\mathbb{C})$

Example The Steinberg representation is the quotient of the space of smooth functions on G/B by the constant functions. Local Langlands associate to it the Weil-Deligne representation which is trivial on I_v and sends Frobenius to : $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and N to : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ The Galois representation is isomorphic to the Galois representation on the Tate module of a Tate elliptic curve.

If v is above p , and if $D_v \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}_p})$ is potentially semistable, it defines a representation of the Weil-Deligne group WD_v (L. Berger's course).

There is also a Weil group for archimedian prime. Let v an archimedian prime. If F_v is isomorphic to reals, the Weil group $W_{\mathbb{R}}$ is isomorphic to the non-trivial extension given by the quaternions :

$$1 \rightarrow \mathbb{C}^* \rightarrow W_{\mathbb{R}} \rightarrow \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \rightarrow 1$$

It is generated by \mathbb{C}^* and τ such that $\tau^2 = -1$ and $\tau\lambda\tau^{-1} = \bar{\lambda}$. If F_v is isomorphic to the complex numbers, $W_{\mathbb{C}}$ is isomorphic to \mathbb{C}^* .

We are interested by complex representations of these Weil groups in $\mathrm{GL}_n(\mathbb{C})$ whose images are of semisimple matrices.

The characters of \mathbb{C}^* can be described by the data of p and $q \in \mathbb{C}$ with the condition $p - q \in \mathbb{Z}$ (if $z = re^{i\theta}$, θ given modulo $2\pi\mathbb{Z}$, $z^p \bar{z}^q$ is well defined if $p - q \in \mathbb{Z}$). The irreducible complex representations of $W_{\mathbb{C}}$ are the characters $z \mapsto z^p \bar{z}^q$. The irreducible complex representations of $W_{\mathbb{R}}$ are :

- of dimension 1 and factors through $W_{\mathbb{R}} \rightarrow \mathbb{R}^*$ (sending λ to its norm $N(\lambda)$ and τ to $-1 \in \mathbb{R}^*$) We note $|\cdot|$ the compositum of $W_{\mathbb{R}} \rightarrow \mathbb{R}^*$ with the absolute value. The representation of dimension 1 are $|\cdot|^p \mathrm{sign}^a$ with $p \in \mathbb{C}$ and $a = 0, 1$ and where sign is the non trivial morphism $\mathbb{R}^* \rightarrow \pm 1$;
- of dimension 2 with parameter (p, q) with $p \neq q$.

To the first one with associate (p, p) and to the second one the pair $(p, q)(q, p)$. So to a semisimple representation of $W_{\mathbb{R}}$ of dimension n we associate a multiset p_1, \dots, p_n .

For every archimedian prime v of F we get a multiset $H_v (p_{1,v}, \dots, p_{n,v})$. This date H_v is equivalent to the data of the infinitesimal character of π_v . The "algebraicity" condition is that the elements of the H_v are integers.

Let $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$.

Conjecture 1.2. *Let π be an algebraic cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$. Then, there is a finite extension $E(\pi)$ of \mathbb{Q} , $E(\pi) \subset \overline{\mathbb{Q}}$, such $\underline{r}(\pi_v)$ can be defined over $E(\pi)$ for every non archimedian v ($\underline{r}(\pi_v)$ is the representation of the Weil-Deligne group WD_v associated by local Langlands correspondence to π_v ; defined over $E(\pi)$ means that it comes from a morphism $\mathrm{WD}_v \rightarrow \mathrm{GL}_n(E(\pi))$ that we still denote by $\underline{r}(\pi_v)$). For every p and every embedding $\lambda : E(\pi) \hookrightarrow \overline{\mathbb{Q}_p}$ there is a p -adic representation $\rho(\pi)_{\lambda} : G_F \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ that is irreducible and such that for every non archimedian prime v , $\underline{r}(\rho_v)$ (ρ_v is the restriction of ρ to the decomposition*

group D_v) coincide up to Frobenius simplification (and to isomorphism) with $\lambda \circ \underline{r}(\pi_v)$. Furthermore, the Hodge-Tate weights of $\rho(\pi)_{\lambda,v}$ for v above p are given in a precise way by the H_v for v archimedean.

Remarks.

As $\rho(\pi)_\lambda$ is supposed to be irreducible it is determined by the traces of the image of Frob_v for v outside a finite set of primes which contains the primes where π_v is ramified.

We describe how the H_v, v archimedean, determine the Hodge-Tate weights (cf Buzzard and Gee "The conjectural connections between automorphic representations and Galois representations" available at the web page of Kevin Buzzard). Let v_p be a p -adic place of F . Let us give ourself an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}_p}$ that induces v_p . It gives a bijection between p -adic and complex embeddings of $\overline{\mathbb{Q}}$. Let $\bar{\lambda}$. We extend it to a p -adic embedding, it gives a complex embedding of $\overline{\mathbb{Q}}$, hence a non archimedean place v_∞ of F . Then $\text{HT}(\rho(\pi)_{\lambda,v_p})$ is H_{v_∞} .

- The π_v, v real place, determines the conjugacy class of $\rho(c_v), c_v$ the complex conjugation (cf Buzzard Gee above).

- What do we know ?

We know nothing if F is not CM. We have to suppose hypotheses of the type ; RAESDC (regular, algebraic, essentially self dual cuspidal) + additional technical hypothesis. The regularity condition say that the elements of H are distinct. Essentially self dual means that $\pi^\vee \simeq \pi \otimes \eta$ for a character η . These conditions follows from the construction of the ρ_π as the method implies that they appear in the cohomology of an Shimura variety (Clozel,...). The additional condition are the existence of a place v where π_v is square integral (ρ_v indecomposable). The progresses in trace formula allows to remove this last condition. The condition of regularity can sometimes be ruled out : $n = 2$ weight 1 (Deligne Serre uses congruences). Irreducibility of Galois representations is not known in general (?).

Examples. $n = 1$. We choose as above embeddings of $\overline{\mathbb{Q}}$ in \mathbb{C} and $\overline{\mathbb{Q}_p}$.

The automorphic representations are continuous characters Ψ of ideles $(\mathbb{A}_F)^*$ that are trivials on F^* . We get Grossencharacters. The condition of algebraicity is the only one : it is that the grossencharacter is of type A^0 . That means that the restriction of Ψ to $(F \otimes \mathbb{R})^{*,0}$ comes from an algebraic character χ (0 is the connected component). More precisely, let T_F be the torus obtained from \mathbb{G}_m by scalar restriction from F to \mathbb{Q} . For every \mathbb{Q} -algebra A , one has $T_F(A) = (A \otimes_{\mathbb{Q}} F)^*$. In particular, $T_F(\mathbb{R}) = (F \otimes \mathbb{R})^*$. We can identify χ to a character of T_F defined over $\overline{\mathbb{Q}}$. We have the decomposition $\Psi : \prod_v \Psi_v, v$ describing the places of F . For v outside a finite number of primes, Ψ_v is unramified. The condition of algebraicity implies that if $x \in F^*, \Psi_v(x) \in \overline{\mathbb{Q}}^*$, hence Ψ_v have images in $(\overline{\mathbb{Q}})^*$ for v non archimedean. For every place w of \mathbb{Q} , we denote Ψ_w the product of the Ψ_v for v above w . We denote by χ_w the morphism $T_F(\mathbb{Q}_w) \rightarrow (\overline{\mathbb{Q}_w})^*$ defined by χ . In particular, we see that χ_∞ and Ψ_∞ coincide on $(F \otimes \mathbb{R})^{*,0}$. We

see that $\Psi\chi_\infty^{-1}$ has image in $(\overline{\mathbb{Q}})^*$, hence $\Psi\chi_\infty^{-1}\chi_p$ has image in $(\overline{\mathbb{Q}_p})^*$. It is continuous and is trivial on F^* . Hence it defines a Galois representation.

- $n = 2$ $F = \mathbb{Q}$. We obtain up to twist the modular forms of weight $k \geq 2$ ($(p, q) = (0, k - 1)$), the forms of weight 1 ($p = q = 0$ $a_1 \neq a_2$) and the Maass forms ($p = q = 0$ $a_1 = a_2$ (?)). In the last two cases, the Galois representations should arise from a motive of weight 0 and should have finite image (see a paper of Kisin and Wortmann). In the case of forms of weight 1, one have significative results of Buzzard and Taylor ; in the case of Maass forms no.

Remark.

The character χ has to be trivial on an open subgroup of the unite E_F . It implies that it has to verify the condition of Serre (if F is real it is a power of the norm. ; if $\chi = \sum n_\tau \tau$, τ describing the embeddings of E in \mathbb{C} with $n_\tau \in \mathbb{Z}$, we must have $n_\tau + n_{c\circ\tau} = w$ does not depend on τ).

For abelian p -adic representations of a p -adic field, the condition to be crystalline is the algebraicity condition (via Class Field Theory).

Case $n = 2$, $F = \mathbb{Q}$. The π_∞ is either irreducible of dimation 2 of type $(p, q)(q, p)$ with $p \neq q$ integers. One obtains up to cyclotomic twist modular forms of weight $|p - q| + 1$. If π_∞ is the sum of two irreducible representations of dimension 1 parametrized by (p_1, a_1) (p_2, a_2) we must have by cuspidality $p_1 = p_2$ (?). Up to twist we obtain either a form of weight 1 (a_1 and a_2 distinct) or a Maass form if $a_1 = a_2$).

In the case of Maass form one does not know how to construct Galois representations.

Let f a modular form of weight $k \geq 1$ and level $N \geq 1$ for $\Gamma_0(N)$.

Let N be an interger ≥ 1 . Let $\Gamma_0(N)$:

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

and $\Gamma_1(N)$:

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

Let k be an integer ≥ 1 . Let $S_k(\Gamma_1(N))$ be the \mathbb{C} vector space of parabolic forms for $\Gamma_1(N)$ of weight k (among the references : [?], [?]) . An element f of $S_k(\Gamma_1(N))$ is an holomorphic function on the Poincaré half plane \mathcal{H} $\mathrm{im}(z) > 0$. It must satisfy the functional equations :

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. It must satisfy a condition of growth at each cusp. More precisely, for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, let $(f | [\gamma]_k)(z) = (cz +$

$d)^{-k} f(\gamma(z))$, $\gamma(z) = \frac{az+b}{cz+d}$. One asks that $(f | [\gamma]_k)(z)$ have a Fourier expansion $\sum_{n \geq 1} a_n q^{n/h}$, $q^{1/h} = \exp(2\pi iz/h)$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ (h divides N and is 1 for the cusp ∞ *i.e.* if $\gamma \in \Gamma_1(N)$). When we speak of the q -expansion without more precision we mean the q -expansion at ∞ . The quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$ by $\gamma \mapsto d \bmod N$. Then $S_k(\Gamma_1(N))$ carries an action of $(\mathbb{Z}/N\mathbb{Z})^*$. that is noted $f \mapsto \langle (d) \rangle (f)$. One has a the decomposition $S_k(\Gamma_1(N)) = \sum_{\eta} S_k(\Gamma_0(N), \eta)$ into eigenspaces, η describing the characters of $(\mathbb{Z}/N\mathbb{Z})^*$. It is trivial if $\eta(-1) \neq (-1)^k$ as the functional equation shows (with $\gamma = -\mathrm{id}$).

The vector space $S_k(\Gamma_1(N))$ is finite dimensional. In fact, we have the projective smooth modular curve $X_1(N)$, which for $N \geq 5$ classify couples (E, P) , E generalised elliptic curves, P point of order N , and coherent sheaves ω such that the elements of $S_k(\Gamma_1(N))$ are sections in $\Gamma(X_1(N), \omega^k)$ that vanish at the cusps. For every n prime to N , let T_n be the Hecke operator acting on $S_k(\Gamma_1(N))$ (and $S_k(\Gamma_0(N))$). The T_n and $\langle (d) \rangle$ commute and generate the Hecke algebra (ring) $\mathbb{T}_1(N)$. The T_n are semi-simple (they are normal linear transformation relatively to the Petersson scalar product). $\mathbb{T}_1(N)$ is a \mathbb{Z} -module of finite type. It is because, if $S_k(\Gamma_1(N))_{\mathbb{Z}}$ is the \mathbb{Z} -module of forms whose q -expansion is in \mathbb{Z} ,

$$S_k(\Gamma_1(N)) = \mathbb{C} \otimes S_k(\Gamma_1(N))_{\mathbb{Z}}.$$

For that a theory of $X_1(N)$ over \mathbb{Z} is needed (or one can also use the action of $\mathbb{T}_1(N)$ on the singular cohomology of $X_1(N)$).

Let d and M be such that dM divides N . Then $f(z) \mapsto f(dz)$ defines an injection of $S_k(\Gamma_1(M))$ in $S_k(\Gamma_1(N))$. Let $S_k^{\mathrm{new}}(\Gamma_1(N))$ be the orthogonal, for Petersson product, of the sum of the images of $S_k(\Gamma_1(M))$. Then, by Atkin-Lehner, $S_k^{\mathrm{new}}(\Gamma_1(N))$ has a basis f_i that are eigenvectors for $\mathbb{T}_1(N)$, each one appearing with multiplicity one. In fact, they are eigenforms for all Hecke operators T_n . If λ_n is the eigenvalue, one has $a_n(f_i) = \lambda_n a_1(f_i)$. It follows that $a_1(f_i) \neq 0$, and one can normalize f_i such that $a_1(f_i) = 1$. The f_i are the primitive forms. If f is primitive, $a_n(f) = \lambda_n$ generates over \mathbb{Q} a number field E_f , the coefficient field. The $a_n(f)$ are integers. For n prime to N this is because $\mathbb{T}_1(N)$ is finitely generated as \mathbb{Z} -module. For p dividing n , we have formulas for a_p (th. 1.27 of [1]).

Let f be a primitive form. Let p be a prime number. Let $\iota_p : E_f \hookrightarrow \overline{\mathbb{Q}}_p$. Deligne if $k \geq 1$, and Deligne-Serre if $k = 1$, constructed a Galois representation $\rho_{f, \iota_p} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$. It is unramified at ℓ if ℓ is prime to pN and is characterized by that for all ℓ prime to pN ,

$$\mathrm{tr}(\rho(\mathrm{Frob}_{\ell})) = \iota_p(a_{\ell}), \det(\rho(\sigma)) = \eta(\sigma) \chi_p(\sigma),$$

for all $\sigma \in G_{\mathbb{Q}}$, where we identify $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ with $(\mathbb{Z}/N\mathbb{Z})^*$. For $k \geq 2$, the representation is part of the p -adic etale cohomology of an algebraic variety over \mathbb{Q} . If $k = 1$, the construction of Deligne-Serre use congruences with Galois representations of weight ≥ 2 . When $k = 1$, the image is finite.

Taylor constructed Galois representations attached to Hilbert modular forms for F totally real and $n = 2$ by congruence method. The algebraicity condition is that the different weights k_v , v non archimedean, have the same parity (exercise : use the determinant).

1.2. Modularity and potential modularity of Galois representations. Geometric Galois representation give rise to \underline{r}_v for each v that are unramified for almost every v hence to $\otimes \pi_v$.

Conjecture 1.3. *Let $\rho : G_F \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ be a geometric irreducible Galois representation. Then $\otimes \pi_v$ is an automorphic representation π .*

Known $n = 1$, or $F = \mathbb{Q}$ $n = 2$ and ρ is odd in many cases (Kisin)

1.3. Properties of automorphic Galois representations ; potential automorphy. Automorphic Galois representations satisfy :

- The L -function of the Galois representation can be extended to \mathbb{C} holomorphic function (Godement-Jacquet). (with the exception to holomorphy : ζ_F -function has a pole at $s = 1$) with the functional equation with constants given by the π_v .

- Often ρ is proved to come from geometry. More precisely, there exists a smooth projective variety X defined over F such that ρ appears in the etale cohomology of an algebraic variety. In all known cases (other than weight 1 modular forms) these varieties are essentially Shimura varieties. When it is the case it implies Ramanujan. More precisely, one has an integer w such that the eigenvalues of $\rho(\mathrm{Frob}_v)$ are (algebraic) Weil numbers of weight $w[k_v : \mathbb{F}_p]$. (if one takes geometric Frobenius). An algebraic number α is a Weil number if for every embedding τ of $\overline{\mathbb{Q}}$ in \mathbb{C} one has $|\tau(\alpha)|^2 = p^w$. (One has $w = p + q$ for all (p, q)).

Remark Even for Hilbert modular forms one does not know in all cases Ramanujan (one does not know when some of the weights are 1 ; for weights ≥ 2 one knows that the symmetric square comes from algebraic dimension hence Ramanujan (?).

Potential automorphy is that there exists F'/F finite such that $\rho|_{G_{F'}}$ is automorphic. We will consider it for Hilbert modular forms and F' real. The two above properties of automorphic Galois representations remain valid for potential automorphic except the holomorphy. But it suffices for Sato-Tate, putting a ρ in compatible system,

2. POTENTIAL MODULARITY THEOREM

2.1. Statement. Let $p > 2$. Let $I_p \subset D_p$ the inertia and decomposition subgroups.

Let k be an integer with $2 \leq k \leq p + 1$. Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. Recall that $\bar{\rho}$ has Serre's weight k :

- if $k \leq p$, either $\bar{\rho}$ has a quotient with trivial action of I_p by a line with action of I_p by ω^{k-1} or the action of I_p is by the two fundamental characters of level 2 ω_2^{k-1} and $\omega_2^{p(k-1)}$;

- if $k = p+1$, $\bar{\rho} \text{ mod } I_p$ is a very ramified extension of 1 dimensional trivial representation by a 1-dimensional representation with action ω .

In Khare W proof of Serre conjecture, the following theorem was used.

Theorem 2.1. *Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$ be an odd mod p Galois representation. One supposes that the weight k of $\bar{\rho}$ satisfy $2 \leq k \leq p+1$ and that the restriction of $\bar{\rho}$ to $G_{\mathbb{Q}(\mu_p)}$ is irreducible. Then there is a totally real number field F and a cuspidal automorphic representation π of $\text{GL}_2(\mathbb{A}_F)$ and an embedding λ of $E(\pi)$ in $\overline{\mathbb{Q}}_p$ such that $\rho|_{G_F}$ and $\rho(\pi)_{\lambda}$ have isomorphic reductions. Furthermore one can impose to π to satisfy each of the conditions (alpha) or (beta) below :*

- (α) π_v is unramified at all places v of F above p and of weight k at all the infinite places of F ;

- (β) π_v is of weight 2 at infinite places and at all places v above p , is of conductor dividing v and Weil-Deligne parameter restricted to inertia $(\omega_p^{k-2} \oplus 1, 0)$ if $2 \leq k \leq p$ and (id, N) if $k = p+1$.

Remark

In fact, we can impose :

- F is unramified at p and totally decomposed at p if $\bar{\rho}|_{D_v}$ is irreducible or if $k = p+1$.

- F is linearly disjoint from a given finite extension of \mathbb{Q} (in particular, we will need this property for the field $L(\mu_p)$ where L is the field cut by $\ker(\bar{\rho})$ in the next theorem).

We have the modularity lifting theorem :

Theorem 2.2. *Let $\bar{\rho}$, F and π and k as in the theorem and the remark, Consider ageometric lift ρ_F of $\bar{\rho}|_{G_F}$ such that at all places v of F above p , the ρ_v satisfy simultaneously one of the conditions (A), (B), (C) below. Then ρ_F is modular.*

The condition (A), (B) and (C) for ρ_v for v a place of F above p :

(A) crystalline of weight k , (we have $2 \leq k \leq p+1$), with the case $k = p+1$ considered only when F is split at p and $k(\bar{\rho}) = p+1$;

(B) crystalline of weight 2 over $\mathbb{Q}_p^{\text{nr}}(\mu_p)$ of Weil-Deligne parameter $(\omega_p^{k-2} \oplus 1, 0)$ for a fixed k ;

(C) In the case $k = p+1$, semistable, non-crystalline of weight 2 so of the form

$$\begin{pmatrix} \gamma_v \chi_p & * \\ 0 & \gamma_v \end{pmatrix},$$

where χ_p is the p -adic cyclotomic character, and γ_v is an unramified character.

Remark We need (α) in case (A) and (β) in cases (B) and (C).

Putting the two theorems together, we get :

Theorem 2.3. *Let $p > 2$. Let $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be an odd 2 dimensional geometric representation satisfying one of the conditions (A), (B) or (C) for a k with $2 \leq k \leq p+1$ (and when $k = p+1$ we suppose $k(\bar{\rho}) = p+1$). Suppose that the restriction of $\bar{\rho}$ to the Galois group of $\mathbb{Q}(\mu_p)$ is absolutely irreducible. Then there is a totally real field F such that the restriction of ρ to G_F is modular.*

Remark To prove Serre's conjecture we need also Lifting Modularity Theorems of Kisin for representations ρ that are potentially crystalline of weight 2.

It implies that the L function of ρ can be extended to a meromorphic function on the complex plane satisfying the functional equation with correct constant terms (use Brauer theorem). It does not imply holomorphy. It also implies that the eigenvalues of the Frobenius Frob_v at primes of good reduction and different from p are Weil numbers of weight $[k_v : k](k-1)$.

2.2. Plan of the proof. We will have to consider Hilbert-Blumenthal abelian varieties (HBAV). Let M be a totally real number field. An M-HBAV over a perfect field K is an abelian variety A of dimension $[M : \mathbb{Q}]$ with an embedding $i : O_M \hookrightarrow \mathrm{End}(A)$ and a data of polarisation j .

Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}_p})$. We will prove modularity of $\bar{\rho}|_{G_{F'}}$. We consider the case $\rho|_{D_p}$ is reducible.

After replacing if necessary \mathbb{Q} by an unramified at p real quadratic extension and a twist, we can suppose that $\det(\bar{\rho}) = \overline{\chi}_p$. We call F this quadratic extension or \mathbb{Q} (in fact Taylor starts from a $\bar{\rho} : G_F \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}_p})$).

The strategy of the proof is to find a totally real extension F' of F and an M-HBAV defined over F' and a prime number $\ell \neq p$ such that

- 1) ℓ and p are unramified in F'
- 2) there is a prime λ of M over p such that $A[\lambda]$ is isomorphic to the restriction of $\bar{\rho}$ to $G_{F'}$

- 3) A has good ordinary reduction at primes of F' above ℓ
- 4) there is a prime \mathfrak{l} of M above ℓ such that $A[\mathfrak{l}]$ is isomorphic to the restriction of $\mathrm{Ind}_{G_L}^{G_F}(\theta)$ to $G_{F'}$, with L a totally imaginary extension of F , places w of F above ℓ are split in L , $w = w_1 w_2$, and θ some character of G_L such that θ is unramified at w_1 but not $c(\theta)$.

This implies that $V_{\mathfrak{l}}(A)$ is ordinary, the restriction of $\mathrm{Ind}_{G_L}^{G_F}(\theta)$ to $G_{F'}$ is irreducible and distinguished. A theorem of Skinner Wiles then implies the modularity of $V_{\mathfrak{l}}(A)$, hence of $V_{\lambda}(A)$, hence of $\rho_{G_{F'}}$.

Then one has to find π that verify (α) and a π that verify (β) .

How we find F' and A ? Let X be the Shimura variety that classifies M-HBAV with λ level structure $\bar{\rho}$ and \mathfrak{l} level structure $\mathrm{Ind}_{G_L}^{G_F}(\theta)$. It is defined over F and absolutely irreducible. We apply to it a theorem of Moret-Bailly.

Theorem 2.4. *Let F be a number field and S_1, S_2 disjoint finite set of places of F . Let L be a finite extension of F . Let X/F be a smooth geometrically connected variety. Let given for $v \in S_1$ be a non empty open subset $\Omega_v \subset$*

$X(F_v)$ and for $v \in S_2$ be a non empty open $\text{Gal}(F_v^{\text{ur}}/F)$ invariant subset of $X(F_v^{\text{ur}})$. Then, there exist a finite Galois extension F'/F and a point $\in X(F')$ such that :

- F'/F and L/F are linearly disjoint ;
- every places $v \in S_1$ splits completely in F' and if w is a place of F' above v then $P \in \Omega_v$;
- every finite place of S_2 is unramified in F' and if w is a prime of F' above v , $P \in \Omega_v$.

So it will suffices to find points of X in F_v for v above p , l and v archi-median.

We precise the data of polarisation in the definition of an M-HBAV (A, i, j) . An M-HBAV (A, i, j) over K is

By an ordered invertible O_M -module we mean an invertible O_M -module and a choice of a connected component X_x^+ of $(X \otimes M_x) - \{0\}$ for each infinite place x of M . The ordered invertible module O_M^+ is O_M where we choose for every x the connected component containing 1. The ordered invertible module $\mathcal{P}(A, i)$ is the O_M -module of symmetric homomorphisms $f : (A, i) \rightarrow (A^\vee, i^\vee)$ where we choose the set of components that contain a polarization. The data j is an isomorphism $O_M^+ \simeq \mathcal{P}(A, i)$

Lemma 2.5. *For each place v of F above p , we can find an M-HBAV (A_v, i_v, j_v) over F_v such that :*

- A_v either has potentially good reduction or potentially multiplicative reduction
- the action of D_v on $A_v[\lambda]$ is isomorphic to $\bar{\rho}|_{D_v}$
- the action of D_v on $A_v[l]$ is isomorphic to $\bar{\psi}_{v_1} \oplus \bar{\psi}_{v_1^c}$, v_1 place of L above v .

We have to say how we choose M , L and ψ .

We define $\chi_v : D_v \rightarrow k^*$ (k^* such that $\bar{\rho}$ has image in $\text{GL}_2(k)$)

$$\begin{pmatrix} \bar{\chi}_p \chi_v^{-1} & * \\ 0 & \chi_v \end{pmatrix}$$

2.2.1. *Choice of Weil numbers.* We choose N a CM field and lifts of image of Frobenius that are Weil numbers. M will be the maximal real subfield of N .

For v a place of F above p , we let F_v^{atr} the maximal abelian tamely ramified extension of F . We choose a lift ϕ_v of Frobenius in $\text{Gal}(F_v^{\text{atr}}/F_v)$ and denote by \tilde{F}_v the field fixed by ϕ_v .

Let ζ denotes a primitive root of unity of order $|k^*|$ and $N_0 = \mathbb{Q}(\zeta, \sqrt{1-4p})$. We assume that k is large enough such that N_0 is ramified over its maximal real subfield. Let λ_0 be a prime of N_0 over p and an isomorphism $O_{N_0}/\lambda_0 \simeq k$. For v a prime of F above p set :

$$\beta_v = \zeta^{b_v} ((1 + \sqrt{1-4p})/2)^{[k(v):\mathbb{F}_p]}$$

where we choose b_v such that $\beta_v \equiv \chi_v(\phi_v) \pmod{\lambda_0}$ for $\phi_v \in G_{\tilde{F}_v}$ a lift of Frobenius. Here \tilde{F}_v is the smallest totally tamely ramified extension of F_v over which χ_v becomes unramified. β_v is a Weil number of weight $[k_v : \mathbb{F}_p]$.

We will treat the case where χ_v^2 is not 1. If $\chi_v^2 = 1$, Taylor use M-HBAV with multiplicative reduction. We let $\tilde{\chi}_v$ the character of W_{F_v} with values on N_{0,λ_0}^* which takes ϕ_v to β_v and on inertia is the Teichmuller lift of χ_v .

Choose ℓ a prime which does not divide $6p$. such that :

- ℓ is split in F

- for all place w of F above ℓ , $\bar{\rho}$ is unramified and $\bar{\rho}(\text{Frob}_w)$ has distinct eigenvalues. This is possible as $\bar{\rho}$ has been supposed with non solvable image (otherwise we know modularity) and a non solvable subgroup of $\text{GL}_2(k)$ contains an element with distinct eigenvalues.

- ℓ splits completely in the Hilbert class field of N_0 .

- ℓ is coprime to $\beta_v - \beta_v^c$ for all places v of F above p .

Choose a prime \mathfrak{l}_0 of N_0 above ℓ . For each place w of F above ℓ choose $\alpha'_w \in \mathbb{Z}[(1 + \sqrt{1 - 4p})/2]$ with norm ℓ (this is possible because ℓ splits completely in the Hilbert class field of $\mathbb{Q}[(1 + \sqrt{1 - 4p})/2]$). Set

$$\alpha_w = \zeta^{a_w} \alpha'_w$$

with a_w chosen so that α_w is congruent modulo λ_0 to an eigenvalue of $\bar{\rho}(\text{Frob}_w)$.

2.2.2. Choice of L and $\bar{\psi}$. We choose a CM quadratic extension L/F and a continuous character $\psi : G_L \rightarrow (N_{0,\mathfrak{l}_0}^{\text{ac}})^*$ such that :

- L is not contained in $F(\mu_\ell)$

- each place v of F above p splits as v_1 and v_1^c in L and $\psi|_{W_{L_{v_1}}} = \tilde{\chi}_v$ in $(O_{N_0}/\mathfrak{l}_0)^{\text{ac}}$ (this will imply the correct action of D_v on the level structure at \mathfrak{l}).

- each place w of F above ℓ splits as w_1 w_1^c in L and $\psi|_{G_{w_1}}$ is unramified and takes arithmetic Frobenius to a lift of the image of α_w in O_{N_0}/\mathfrak{l}_0 .

- $\det(\text{Ind}_{G_L}^{G_F} \psi) = \chi_\ell$.

This is an exercise of Class Field Theory to prove the existence of ψ .

Let $\bar{\psi}$ the reduction of ψ modulo \mathfrak{l}_0 . As $\beta_v - c(\beta_v)$ is coprime to ℓ we have that $\bar{\psi}$ is $\neq c(\bar{\psi})$, hence $\text{Ind}_{G_L}^{G_F} \bar{\psi}$ is absolutely irreducible. It is D_w distinguished for places of F above ℓ as $\psi|_{G_{w_1}}$ is unramified and $\psi|_{G_{w_2}}$ is ramified as $\det(\text{Ind}_{G_L}^{G_F} \psi) = \chi_\ell$ and F is unramified at ℓ . Hence we can apply the theorem of Skinner-Wiles.

2.2.3. Choice of M and N . Let M_0 the maximal totally real subfield of N_0 . We choose N a CM extension of N_0 of maximal totally real subfield M , such that :

- primes above p splits in N/N_0 ;

- primes above ℓ are unramified in N/N_0

- there is a prime \mathfrak{l} of N above \mathfrak{l}_0 such that the image of $\bar{\psi}$ is contained in O_N/\mathfrak{l}

- primes of M_0 that ramify in N_0 are unramified in N/N_0 . As there are such primes (choice of Weil numbers), this implies that the norm map from the class group of N to the strict class group of M is surjective.

2.2.4. *Choosing the reduction of (A, i, j) .* We define A_0 to be an ordinary abelian variety defined by Honda-Tate from the Weil number β_v . More precisely there is an abelian variety over k_v of dimension $[\mathbb{Q}(\beta_v) : \mathbb{Q}]$ with an embedding of $O_{\mathbb{Q}(\beta_v)}$ in $\text{End}(A_0/k_v)$ with $A_0[p](\bar{k}_v)$ isomorphic to $O_{\mathbb{Q}(\beta_v)}/(\beta_v^c)$ with action of Frobenius β_v . We define A_v to be $A_0 \otimes_{O_{\mathbb{Q}(\beta_v)}} O_N$ with the natural embedding of O_N in the endomorphisms. To get j start from a polarisation and use the surjectivity of the class group of O_N to the strict class group of O_M .

2.2.5. *Constructing A over on $O_{\tilde{F}_v}$.* Recall that \tilde{F}_v is the field fixed by ϕ_v . Let $\tilde{\chi}'_v : D_v \rightarrow O_{N,(\beta_v^c)}^* \simeq O_{M,p}^*$ the unramified character which takes ϕ_v to β_v .

Serre-Tate theorem says that to give a lift (A_1, i_1, j_1) of (A_0, i_0, j_0) to $O_{\tilde{F}_v}$ is the same as to give a p -divisible group that is extensions of $M_p/O_{M,p}(\tilde{\chi}'_v)$ by $\mu_{p^\infty} \otimes O_{M,p}((\tilde{\chi}'_v)^{-1})$ hence $x \in H^1(G_{\tilde{F}_v}, O_{M,p}(\chi_p(\tilde{\chi}'_v)^{-2}))$. One defines (A_x, i_x, j_x) to be obtained from (A_1, i_1, j_1) by $O_N \otimes_{O_{\mathbb{Q}(\beta_v)}}$.

2.2.6. *Descent to F_v .* As the commutator of O_M in $\text{End}(A_1)$ is O_N , a morphism f of A_1 lift to a morphism of (A_x, i_x, j_x) to (A_y, i_y, j_y) if it is a $\gamma \in O_N$ such that $\gamma\gamma^c = 1$ and $\gamma^2 x = y$. Thus a data of descent to F_v is the same as a character $\phi : \text{Gal}(\tilde{F}_v/F_v) \rightarrow \mu_{p^\infty}(N)$ and an $x \in H^1(G_{\tilde{F}_v}, O_{M,p}(\chi_p(\tilde{\chi}'_v)^{-2}))$ such that $\sigma(x) = \phi(\sigma)^2 x$ for all $\sigma \in \text{Gal}(\tilde{F}_v/F_v)$.

It is the same as to give $\chi' : D_v \rightarrow O_{M,p}^*$ that extends the restriction of $\tilde{\chi}_v$ to \tilde{F}_v and an $x \in H^1(D_v, O_{M,p}(\overline{\chi}_p(\chi')^{-2}))$. One takes $\chi' = \tilde{\chi}_v$. One takes x such that its λ component maps to the class of $\bar{\rho}_{|D_v}$ in $H^1(D_v, O_M/\lambda(\overline{\chi}_p\chi_v^{-2}))$. This is possible as $H^2(D_v, O_{M,\lambda}(\overline{\chi}_p\chi_v^{-2}))$ as χ_v^2 is not trivial in D_v .

One still have to prove that A is ordinary at places above ℓ (follows that it has good reduction after a extension of ramification degree at most 3 at places w above ℓ and the reduction mod ℓ is ordinary). One also have to check that A has good ordinary reduction over $F'(\mu_p)$ with correct restriction of Weil Deligne parameter to inertia . One has π of weight 2 and correct Weil Deligne parameter. (One also have to check it is χ_v -good : Taylor does it when $k \neq p$). One can obtain π of weight k by Hida theory and unramified at primes above p .

In the case of $\bar{\rho}_{D_v}$ is irreducible, Taylor uses reduction of CM abelian varieties to get A over F' that is split at p . But the Weil-Deligne parameter at places above p is $\omega_2^{k-p-1} \oplus \omega_2^{p-k-p-1}$ and weight 2. Then one has to adjust the weight and Weil-Deligne parameter , using the fact that the F' is split at p (Conrad Diamond Taylor technics).

3. MODULARITY LIFTING THEOREM

We sketch the proof the following theorem which is an extension of a theorem of Wiles Taylor-Wiles ; we use improvements of the method by Diamond, Fujiwara, Kisin, . :

Theorem 3.1. *Let $p > 2$. Let $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be an odd Galois representation. One supposes that :*

- *the restriction to $G_{\mathbb{Q}(\mu_p)}$ of "the reduction" $\bar{\rho}$ is irreducible (hence ρ is irreducible) ;*
- *$\bar{\rho}$ is modular ;*
- *ρ is unramified outside a finite set of primes ;*
- *$\rho|_{D_p}$ is crystalline of weight k (Hodge-Tate weights $(0, k - 1)$) with $2 \leq k \leq p + 1$.*

Then ρ is modular.

Remark The case $k = p + 1$ and the restriction of $\bar{\rho}$ to D_p is irreducible (hence $\bar{\rho}$ is of weight 2 is due to Kisin). In other case one has that $k(\rho) = k(\bar{\rho})$ and, $\bar{\rho}$ arises from a modular form of weight k by the theorem that the weak form of the Serre's conjecture implies the strong one (for $k = p + 1$ use the Hasse invariant).

3.1. Automorphic representations for definite quaternion algebras.

Morphism $R \rightarrow T$. We introduce a solvable totally real field F . We prove that $\rho|_{G_F}$ is modular, *i.e.* arises from a cuspidal automorphic representation of $(D \otimes \mathbb{A}_F)^*$, D a suitable quaternion algebra of center F . Then, by Langlands base change and Jacquet-Langlands, we will know that ρ is modular.

One advantage of considering F is that we can suppose that $\rho|_{G_F}$ is unramified outside primes V_p over p and primes in a finite set Σ where at $v \in \Sigma$, the Weil-Deligne parameter of ρ_{D_v} is trivial on I_v and $N \neq 0$ (the representation $\rho|_{I_v}$ is tame and its image is unipotent). Furthermore, D is ramified exactly at infinity and primes in Σ (one imposes that $[F : \mathbb{Q}]$ and the cardinality of Σ are even). One supposes that F is unramified above p . One supposes that $\bar{\rho}|_{G_F}$ arises from π , that is discrete series of weight k at infinity, unramified outside Σ and unramified twist of Steinberg at primes in Σ . These latter conditions might imply to do level lowering or raising.

More precisely, let Σ the set of primes where ρ is potentially Steinberg. By Skinner-Wiles there is a solvable F , unramified at p such that $\bar{\rho}|_{G_F}$ lift to a ρ' which comes from a π which is unramified outside Σ . By replacing F by a solvable extension, we may suppose that the degree of F is even and also the cardinality of Σ . One can impose that F is linearly disjoint from $\ker(\bar{\rho})$ so that $G_{F(\mu_p)}$

One advantage to consider indefinite D is that spaces of modular forms with action of Hecke operators has combinatorial description. Let $(D \otimes_F \mathbb{A}_F^\infty)^*$ be the finite adeles. We fix a maximal order \mathcal{O}_D of D . Let $U_v = (\mathcal{O}_D)_v^*$ and $U = \prod_v U_v$. Let E be an extension of \mathbb{Q}_p which is sufficiently large and

O be its ring of integers. Let $W := \otimes_{F \hookrightarrow E} \text{Sym}^{k-2} O$ with the natural action of U through its quotient $\prod_{v \in V_p} U_v$ (V_p are the primes above p). Let ψ be the character $\det(\rho)\chi_p^{-1}$ where χ_p is the p -adic cyclotomic character. As ψ is even, we can see ψ as a character of the finite ideles $(\mathbb{A}_F^\infty)^*$. We define the space of modular forms $S_{k,\psi}(U)$ with coefficients in O with central character ψ to be the space of functions

$$f : D^* \backslash (D \otimes_F \mathbb{A}_F^\infty)^* \rightarrow W$$

such that:

$$\begin{aligned} f(gu) &= u^{-1}f(g) \\ f(gz) &= \psi(z)f(g) \end{aligned}$$

for all $g \in (D \otimes_F \mathbb{A}_F^\infty)^*$, $u \in U$, $z \in (\mathbb{A}_F^\infty)^*$.

For each finite place v of F we fix a uniformizer π_v of F_v . We consider the left action of $g \in (D \otimes_F \mathbb{A}_F^\infty)^*$ by right translation on the W -valued functions f on $(D \otimes_F \mathbb{A}_F^\infty)^*$ and denote this action by $g \cdot f$ or gf . This induces an action of the double cosets $U \begin{pmatrix} \pi_v & 0 \\ 0 & \pi_v \end{pmatrix} U$ and $U \begin{pmatrix} \pi_v & 0 \\ 0 & 1 \end{pmatrix} U$ on $S_{k,\psi}(U)$ for $v \notin S$ (S is the set of places $V_\infty \cup V_p \cup \Sigma$). We denote these operators by S_v (which is simply multiplication by $\psi(\pi_v)$) and T_v respectively. They do not depend on the choice of π_v . We call $T_{k,\psi}(U)$ the Hecke algebra acting on $S_{k,\psi}(U)$ generated over O by the Hecke operators T_v and S_v at primes $v \notin S$.

By Jacquet-Langlands, $S_{k,\psi}(U)$ with its action of Hecke operators is (essentially) isomorphic of automorphic forms for $\text{GL}_2(F)$ which are of weight k , unramified outside Σ , at $v \in \Sigma$ it is unramified twist of Steinberg, and of central character ψ .

The automorphic representaton π defines a morphism $T_{k,\psi}(U) \rightarrow O$. By reduction it defines a maximal ideal \mathfrak{m} of $T_{k,\psi}(U)$. Let $T_{k,\psi}(U)_{\mathfrak{m}}$ be the completion. By Deligne and Carayol, we get a Galois representation $: G_F \rightarrow \text{GL}_2(T_{\psi}(U)_{\mathfrak{m}})$ that lifts $\bar{\rho}$.

Let \bar{R}_S^ψ be the ring representing deformations of $\bar{\rho}|_{G_F}$ that have determinant $\psi\chi_p$ and satisfies the following properties for $v \in S := V_\infty \cup V_p \cup \Sigma$: odd, crystalline of weight k and for $v \in \Sigma$ of the form $\begin{pmatrix} \gamma\chi_p & * \\ 0 & \gamma \end{pmatrix}$ with $\gamma^2 = \psi$.

We get a surjective map $\bar{R}_S^\psi \rightarrow T_{\psi}(U)_{\mathfrak{m}}$. To get our theorem, we prove that this map is bijective after inverting p .

3.2. Galois cohomology. The existence of \bar{R}_S^ψ as a complete noetherian local noetherian (CNLO) with residue field the residue field \mathbb{F} of O is as follows. Let $G = G_{F,S}$. One can first consider the functor of continuous lifts in $G \rightarrow \text{GL}_2(A)$, for A in CNLO. It is representable by a CNLO-algebra. It is almost obvious, but there is the continuity condition. One can use a representability theorem of Grothendieck which is a particular case of

Schlessinger criteria. One has to use that for any open subgroup G' of G , there are only finitely many continuous morphisms from G' to $\mathbb{Z}/p\mathbb{Z}$. The relative tangent space is the \mathbb{F} -vector space of 1-cocycles $Z^1(G, \text{Ad})$ where Ad is the adjoint representation of $\bar{\rho}$.

A deformation of $\bar{\rho}$ is an equivalence set of lifts, two lifts being equivalent if they are conjugate by a matrix of the kernel $\text{GL}_2(A)_1$ of the morphism $\text{GL}_2(A) \rightarrow \text{GL}_2(\mathbb{F})$. As $\bar{\rho}$ is supposed to be irreducible the action of $\text{PGL}(A)_1$ has no fixed points and Schlessinger criteria easily implies the representability. The relative tangent space is the \mathbb{F} -vector space $H^1(G, \text{Ad})$.

Fixing the determinant is clearly a closed condition (for tangent spaces, as $p \neq 2$, replace Ad by trace 0 matrices Ad^0). The condition to be crystalline is closed. At least when $k \leq p-1$, it is because one can define a crystalline representation of weight $(0, k-1)$ with coefficients in a CNLO artinian algebra and the category is stable by direct sums, subobjects and quotients. For $v \in \Sigma$, we impose that the action is tame, the action of inertia is unipotent and the characteristic polynomial of a lift of Frobenius.

We want to prove that R is not too big and that T is not too small. In fact we have to do it allowing ramification at a finite set of auxiliary primes Q_n disjoint of S is allowed.

Let Q_n be a finite set of primes disjoint of S . We suppose :

- AUX1 $\bar{\rho}(\text{Frob}_v)$ has distinct eigenvalues α_v and β_v and $\mathbb{N}(v) \equiv 1 \pmod{p^n}$.

For $v \in Q_n$ let Δ_v the maximal p -quotient of k_v^* so by classfield theory it identifies to the maximal p -quotient of tame inertia at v . It is not difficult to see that the restriction to I_v of the universal representation in $\text{GL}_2(\bar{R}_{S \cup Q_n}^\psi)$ factors through Δ_v : the action of D_v is $\gamma_{\alpha_v} \oplus \gamma_{\beta_v}$ with γ_{α_v} having unramified reduction with the image of Frobenius α_v , idem for γ_{β_v} and the restriction γ_{α_v} and γ_{β_v} to I_v are inverse. Let $\Delta_n := \prod_{v \in Q_n} \Delta_v$. We have an action of Δ_v , hence of Δ_n on $\bar{R}_{S \cup Q_n}^\psi$ (by multiplication by $\gamma_{\alpha_v}(\sigma)$ where σ is a generator of tame inertia at v). The quotient of $\bar{R}_{S \cup Q_n}^\psi$ by the augmentation ideal is \bar{R}_S^ψ .

We have a compatible action on Hecke-algebras. The space $S_{k,\psi}(U_{Q_n})$ is defined in the same way as $S_{k,\psi}(U)$ but for $v \in Q_n$, one replaces $U_v = (\mathcal{O}_D)_v^* \simeq \text{GL}_2(\mathcal{O})$ by :

$$(U_{Q_n})_v = \left\{ g \in \text{GL}_2(\mathcal{O}_{F_v}) : g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \text{ mod. } (\pi_v), ad^{-1} \rightarrow 1 \in \Delta_v \right\},$$

The natural action of $g \in \Delta_v$, denoted by $\langle g \rangle$, arises from the double coset

$$U_{Q_n} \begin{pmatrix} \tilde{g} & 0 \\ 0 & 1 \end{pmatrix} U_Q$$

where \tilde{g} is a lift of g to $(\mathcal{O}_F)_v^*$. One also needs Γ_0 level.

$$(U_Q^0)_v = \left\{ g \in \text{GL}_2(\mathcal{O}_{F_v}) : g = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \text{ mod. } (\pi_v) \right\}.$$

We have corresponding modules of modular forms and Hecke-algebras and maximal ideals \mathfrak{m}

We have the following proposition (at least for $p > 3$, otherwise more technical) :

Proposition 3.2. *$S_{k,\psi}(U_{Q_n})_{\mathfrak{m}}$ is a free $O[\Delta_n]$ -module of rank equal to the rank of $S_{k,\psi}(U_{Q_n}^0)_{\mathfrak{m}}$ as an O -module. $S_{k,\psi}(U_{Q_n}^0)_{\mathfrak{m}}$ is isomorphic to $S_{k,\psi}(U)_{\mathfrak{m}}$.*

For the proof one uses the combinatorial description of spaces of modular forms. For U one of the open subgroups defined above, if $(D \otimes_F \mathbb{A}_F^\infty)^*$ is the disjoint union of $D^*t_i U(\mathbb{A}_F^\infty)^*$, $i \in I$ for a finite set I and with $t_i \in (D \otimes \mathbb{A}_F^\infty)^*$, then $S_{k,\psi}(U)$ can be identified with

$$(1) \quad \bigoplus_{i \in I} W^{(U(\mathbb{A}_F^\infty)^* \cap t_i^{-1} D^* t_i) / F^*}$$

via $f \rightarrow (f(t_i))_i$.

If $p > 3$, the groups appearing as exponent are of order prime to p (triviality of isotropy groups : one uses F unramified at p). The first part of the proposition follows. At least it follows that, for η a character of Δ_n , the rank of the part of $S_{k,\psi}(U_{Q_n})_{\mathfrak{m}}$ on which the Δ_n acts with character η does not depend on η . This is because by replacing O by its residue field \mathbb{F} one gets a space of modular form with coefficients in \mathbb{F} which does not depend on η and which is the reduction of the spaces of modular forms with coefficients in O for the various η . This essentially gives a theorem of Carayol.

The fact that $S_{k,\psi}(U_{Q_n}^0) \simeq S_{k,\psi}(U)$ relies that there is no new at p modular forms for $\Gamma_0(p)$ that reduces to $\bar{\rho}$ as the eigenvalues of Frob_v are distinct and $\mathbb{N}(v) \equiv 1 \pmod p$ and an Ihara lemma to get an isomorphism over O .

As the action of D_v in $\bar{\rho}$ is not necessarily irreducible, we consider for $v \in S$, the ring $\bar{R}_v^{\square,\psi}$ that represents lifts of $\bar{\rho}|_{D_v}$ with the current condition. We define $\bar{R}_S^{\square,\psi}$ (resp. $\bar{R}_{S \cup Q_n}^{\square,\psi}$) the ring that represents deformations of $\bar{\rho}$ of determinant $\psi\chi_p$ that locally at $v \in S$ satisfy the current conditions, are unramified outside S (resp. $S \cup Q_n$) and for $v \in S$ a choice of the basis B_v of the underlying space. Two such datas are isomorphic if $(\rho|_{D_v}, B_v)$ define isomorphic lifts. It is almost clear that $\bar{R}_S^{\square,\psi}$ (resp. $\bar{R}_{S \cup Q_n}^{\square,\psi}$) is a power series algebra over \bar{R}_S^ψ (resp. $\bar{R}_{S \cup Q_n}^\psi$) with $4s - 1$ variables (s is the cardinality of S).

We let $R := \bar{R}_S^{\square,\psi}$, $R_n := \bar{R}_{S \cup Q_n}^{\square,\psi}$, $M := R \otimes_{\bar{R}_S^\psi} S_{k,\psi}(U)_{\mathfrak{m}}$, $M_n := R_n \otimes_{\bar{R}_{S \cup Q_n}^\psi} S_{k,\psi}(U_{Q_n})_{\mathfrak{m}}$. We have to prove that $R[1/p]$ acts faithfully on $M[1/p]$.

We write $\bar{R}_S^{\square,\text{loc},\psi}$ (or B) the completed tensor product $\otimes_{v \in S} \bar{R}_v^{\square,\psi}$. The rings R and R_n are naturally an $\bar{R}_S^{\square,\text{loc},\psi}$ -algebra. We have structure of $O[[y_1, \dots, y_{q_n+4s-1}]]$ -algebra on R_n and an action of $O[[y_1, \dots, y_{q_n+4s-1}]]$ on

M_n that are compatible. The coinvariants by (y_1, \dots, y_{q_n}) are R and M respectively. The module M_n is finite free over the image of $O[[y_1, \dots, y_{q_n+4s-1}]]$ in $\text{End}_{\mathcal{O}}(M_n)$.

We now have to bound the number of generators of R_n as a $\bar{R}_S^{\square, \text{loc}, \psi}$ -module.

We write h^* for the dimension over \mathbb{F} of H^* . For $v \in S \cup Q_n$, we choose $L_v \subset H^1(D_v, \text{ad}^0)$ and $H_{\{L_v\}}^1(S \cup Q_n, \text{ad}^0)$ are the elements of $H^1(S \cup Q_n, \text{ad}^0)$ that at $v \in S \cup Q_n$ localizes to an element of L_v . We choose $L_v = 0$ for $v \in S$ and $L_v = H^1(D_v, \text{ad}^0)$ for $v \in Q_n$. The following lemma is easy :

Lemma 3.3. *The minimal number of generators of $\bar{R}_{S \cup Q_n}^{\square, \psi}$ as a $\bar{R}_S^{\square, \text{loc}, \psi}$ -algebra is $h_{\{L_v\}}^1(S \cup Q_n, \text{ad}^0) + \sum_{v \in S} h^0(D_v, \text{ad}) - 1$.*

We have Wiles formula (we will use it with $V = Q_n$)

$$(2) \quad \frac{|H_{\{L_v\}}^1(S \cup V, \text{Ad}^0)|}{|H_{\{L_v^\perp\}}^1(S \cup V, (\text{Ad}^0)^*(1))|} = \frac{|H^0(G_F, \text{Ad}^0)|}{|H^0(G_F, (\text{Ad}^0)^*(1))|} \prod_{v \in S \cup V} \frac{|L_v|}{|H^0(D_v, \text{Ad}^0)|}$$

We will be able to impose to Q_n the properties :

AUX2 : $q_n = h_{\{L_v^\perp\}}^1(S, (\text{ad}^0)^*(1))$ and $H_{\{L_v^\perp\}}^1(S \cup Q_n, (\text{ad}^0)^*(1)) = 0$.

We write $q_n = q$.

In the Wiles formula, the terms $h^0(G_F)$ are trivial, the contribution of $v \in S$ is $-h^0(D_v, \text{ad}^0)$ and the term for $v \in Q_n$ is 1. Finally, we have proved that

Lemma 3.4. *The minimal number of generators of $\bar{R}_{S \cup Q_n}^{\square, \psi}$ as a $\bar{R}_S^{\square, \text{loc}, \psi}$ -algebra is $q + s - 1$.*

For the rings $\bar{R}_v^{\square, \psi}$ and $B := \bar{R}_S^{\square, \text{loc}, \psi}$, we have :

- $\bar{R}_v^{\square, \psi}$ is flat over \mathcal{O} ,
- The relative to \mathcal{O} dimension of each component of $\bar{R}_v^{\square, \psi}$ is :
 - 3 if $\ell \neq p$;
 - 3 + $[F_v : \mathbb{Q}_p]$ if $\ell = p$;
 - 2 if v is an infinite place.
- $\bar{R}_v^{\square, \psi}[\frac{1}{p}]$ is regular.

It follows that the completed tensor product $\bar{R}_S^{\square, \text{loc}, \psi}$ is flat over \mathcal{O} , with each component of relative dimension $3|S|$, and $\bar{R}_S^{\square, \text{loc}, \psi}[\frac{1}{p}]$ is regular.

3.3. Patching argument. Furthermore, one can reduce to the case B is a domain : this follows from the fact that k is small. For k big, the number of connected component is controlled by a conjecture of Breuil-Mezard that Kisin proves in a lot of cases (and prove the Fontaine-Mazur conjecture).

For example, if $k = p$ and $\bar{\rho}$ is unramified at p and D_p acts by two distinct unramified characters, one has to enlarge F so that the two characters become equal to reduce to the case B is a domain.

By a diagonal process, we form projective limits R_∞ and M_∞ of sufficiently deep quotients of the R_n and the M_n so that we have : $R = R_\infty/(y_1, \dots, y_q)$ and $M = M_\infty/(y_1, \dots, y_q)$.

As $3s + (q + s - 1) = q + 4s - 1$ and M_∞ is finite free of rank > 0 over $O[[y_1, \dots, y_{q+4s-1}]]$, and B is a domain, the morphism $B[[x_1, \dots, x_{q+s-1}]] \rightarrow R_\infty$ is an isomorphism (otherwise R_∞ would have dimension $< q + 4s - 1$ and M_∞ could not be free over $O[[y_1, \dots, y_{q+4s-1}]]$).

As $M_\infty[1/p]$ is finite free over $O[[y_1, \dots, y_{q+4s-1}]] [1/p]$, it has a regular sequence of length $q + 4s - 1$, hence by Auslander-Buchsbaum, as $R_\infty[1/p]$ is regular, $M_\infty[1/p]$ is finite free over $R_\infty[1/p]$. It follows that $M[1/p]$ is finite free over $R[1/p]$. The argument was given by Diamond and Fujiwara independently.

We still have to prove the existence of auxiliary primes.

Let $[c]$ be a non zero class $\in H^1_{\{L_v^+\}}(S \cup Q_n, \text{ad}^0(1)) = 0$. We have to find a prime q of F such that

- (1) $q \equiv 1 \pmod{p^n}$
- (2) $q \notin S$ so $\bar{\rho}$ is unramified at q and $\bar{\rho}(\text{Frob}_q)$ has distinct eigenvalues
- (3) The image of $[c]$ in $H^1(\mathbb{F}, \text{ad}^0 \bar{\rho}(1))$ is non trivial.

Here we use that $H^2(D_q, \text{ad}^0)$ is 1-dimensional.

By Chebotarev, it suffices to find $\sigma \in G_F$ such that

- (1) $\sigma|_{F(\mu_{p^n})} = 1$
- (2) $\bar{\rho}(\sigma)$ has distinct eigenvalues
- (3) $c(\sigma) \notin (\sigma - 1)(\text{ad}^0)$.

Let F_n be the extension of $F(\mu_{p^n})$ cut out by ad^0 . It suffices to prove that :

- $H^1(\text{Gal}(F_n/F), \text{ad}^0(1)) = (0)$

- for any non trivial irreducible $\text{Gal}(F_n/F)$ -submodule V of ad^0 we can find $\sigma \in \text{Gal}(F_n/F(\mu_{p^n}))$ such that $\text{ad}^0(\sigma)$ has an eigenvalue other than 1 but σ has eigenvalue 1 on V .

Indeed, if we have that, by the first condition, $c(G_{F_n})$ is non trivial. Let $V_c \subset \text{ad}^0$ be the \mathbb{F} -vector space generated by $c(G_{F_n})$. Let $V \subset V_c$ be irreducible non trivial and let σ as in the second condition. We can suppose that $\bar{\rho}(\sigma)$ is semi-simple. If $c(\sigma) \notin (\sigma - 1)(\text{ad}^0)$, we are done. If $c(\sigma) \in (\sigma - 1)(\text{ad}^0)$, let us decompose ad^0 as the direct sum of $V \oplus V'$ stable by $\bar{\rho}(\sigma)$ and $V = V_1 \oplus V'_1$ stable by $\bar{\rho}(\sigma)$ with V_1 the fixed points of $\bar{\rho}(\sigma)$ in V . There exists $\sigma' \in G_{F_n}$ such that the projection of $c(\sigma')$ to V_1 is non trivial. We have $c(\sigma') \notin (\sigma - 1)(\text{ad}^0 - 1)$. This implies $c(\sigma'\sigma) = c(\sigma') + c(\sigma) \notin (\sigma - 1)(\text{ad}^0 - 1)$.

It remains to prove the existence of σ . If V is of dimension 3, it suffices to choose σ such that $\bar{\rho}(\sigma)$ has distinct eigenvalues. If V is of dimension 1 or 2, $\bar{\rho}$ is induced from a character of a quadratic extension E of F (as ad^0 is

auto dual $\bar{\rho}$ stabilizes a line which is generated by a semisimple matrix and the eigenspaces of this matrix are permuted by G_F). If V is of dimension 1, if χ is the character of G_E and χ' the conjugate character, we can choose $\sigma \in G_{E(\mu_{p^n})}$ such that $\chi(\sigma) \neq \chi'(\sigma)$. This is possible as the restriction of $\bar{\rho}$ to $G_{F(\mu_{p^n})}$ is irreducible. If V is of dimension 2, we choose σ such that $\sigma \notin G_E$ (this is possible as E is not a subfield of $F(\mu_{p^n})$).

REFERENCES

- [1] H. Darmon, F. Diamond, R. Taylor. Fermat's last theorem. Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), 2-140, Int. Press, Cambridge, MA, 1997.
- [2] F. Diamond and J. Shurman. A first course in Modular Forms. Graduate Texts in Mathematics, 228, 2005.
- [3] J.-M. Fontaine and Y. Ouyang Theory of p -adic Galois Representations
- [4] J.-M. Fontaine and B. 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.
- [5] Mark Kisin Moduli of finite flat group schemes and modularity Annals of Math. 170(3) (2009), 1085-1180.
- [6] The Fontaine-Mazur conjecture for GL2 J.A.M.S 22(3) (2009) 641-690.
- [7] Jean-Pierre Serre Abelian l -adic representations and elliptic curves, Research Notes in Mathematics, 7. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original, A K Peters Ltd., Wellesley, MA, 1998.
- [8] Richard Taylor. Galois representations. Annales de la Faculté des Sciences de Toulouse 13 (2004), 73-119.
- [9] Richard Taylor. Remarks on a conjecture of Fontaine and Mazur. Inst. Math. Jussieu, 1(1):125–143, 2002.
- [10] Richard Taylor. On the meromorphic continuation of degree two L-functions. Documenta Math. Extra Volume: John H. Coates' Sixtieth Birthday (2006) 729–779.
- [11] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2), 141(3), 553–572, 1995.
- [12] A. Wiles. Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2), 141(3), 443–551, 1995.

E-mail address: wintenb@math.u-strasbg.fr

UNIVERSITÉ LOUIS PASTEUR, DÉPARTEMENT DE MATHÉMATIQUE, MEMBRE DE L'INSTITUT UNIVERSITAIRE DE FRANCE, 7, RUE RENÉ DESCARTES, 67084, STRASBOURG CEDEX, FRANCE