COMPOSITIO MATHEMATICA

B. MAZUR

Two-dimensional p-adic Galois representations unramified away from p

Compositio Mathematica, tome 74, nº 2 (1990), p. 115-133
<http://www.numdam.org/item?id=CM_1990__74_2_115_0>

Compositio Mathematica **74**: 115–133, 1990.

Two-dimensional p-adic Galois representations unramified away from p

B. MAZUR
Dept. of Mathematics, Harvard University, Cambridge, MA 02138, USA

Received 1 March 1989; accepted 23 August 1989

Let $G_{\mathbf{Q}}$ be the absolute Galois group of an algebraic closure of $\mathbf{Q}$.

The purpose of this note is to examine the following type of problem: Fix f a newform on $\mathrm{SL}_2(\mathbb{Z})$. For each non-archimedean valuation v of the field of fractions of the ring of Fourier coefficients of f, Deligne, in [D], has attached to f a two-dimensional semi-simple Galois representation with values in k_v, the residue field of v,

$$\bar{\rho}_{f,v}: G_{\mathbf{Q}} \to \mathrm{GL}_2(k_v),$$

which is unramified outside the characteristic (call it p) of k_v. We would like to have a complete classification, for fixed f and a "general enough" choice of valuation v, of all possible liftings of $\bar{\rho}_{f,v}$

$$\rho_A: G_{\mathbf{Q}} \to \mathrm{GL}_2(A) \qquad (*)$$

where A is any complete noetherian local ring with residue field k, and where by 'liftings' we mean ones which are unramified outside p.

Since we are mainly interested in the behavior for "general enough" v, we suppose that $\bar{\rho}_{f,v}$ is absolutely irreducible and we suppose further that v is an *ordinary* valuation for the newform f. This implies that $\bar{\rho}_{f,v}$ is *p-ordinary* as a Galois representation (See Section 2 below).

The kind of answer we give to the above problem comes from the main proposition (Section 3) and the Conjecture of Section 6 below. Our main proposition asserts that, under mild hypotheses, knowledge of all *p-ordinary* liftings (*) gives us very strong control over *all* liftings (*). The Conjecture formulated in Section 6 asserts, in essence, that all p-ordinary liftings are *modular* in that they are built, in a suitable sense, out of p-adic representations attached to p-adic, p-ordinary modular forms. This conjecture (reformulated in a somewhat general context), and a survey of the existing evidence for it, will be discussed more fully elsewhere ([M-T]). As for the p-ordinary liftings (*) that *are* modular in the above sense, these (for "general enough" v) can be completely classified using Hilda's theory (as made explicit by Gouvêa, cf. [G1] and Proposition 1 in Section 7 below).

Using the main proposition, the conjecture of Section 6, and the result from Hida's theory to which we have just alluded, we obtain the surprisingly precise, (but admittedly only conjectural) answer to our problem in Section 7 below (cf. Propositions 2, 3).

To be specific, let us illustrate our result with the modular form

$$\Delta = q\Pi(1-q^n)^{24} = \sum\tau(n)\, q^n,$$

the unique cusp form of level 1 of weight 12 (See Section 7 below). Let p be any prime number such that $\tau(p)$ is not congruent to 0 mod p. Let $\bar{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be the Galois representation modulo p associated to Δ. Using Hida's theory (cf. [G1] or the Proposition of Section 6 below) one sees that the natural homomorphism $\Lambda \to \mathbf{T}$ of the Iwasawa algebra Λ to Hida's Hecke algebra T is an isomorphism. In rough terms this just means the following:

Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ be any two-dimensional Galois representation of $G_{\mathbb{Q}}$ unramified outside p, which is a lifting of $\bar{\rho}$, where $\mathcal{O}$ is a finite discrete valuation ring extension of $\mathbb{Z}_p$ with residue field $\mathbb{F}_p$.

Suppose that:

(a) The representation ρ is attached to a p-ordinary p-adic eigenform (of tame-level 1).

Then:

(b) The representation ρ is *determined* (up to equivalence) by the one-dimensional representation $\det(\rho)\colon G_{\mathbb{Q}} \to \mathrm{GL}_1(\mathcal{O}) = \mathcal{O}^*$, and, moreover any such one-dimensional representation $\chi\colon G_{\mathbb{Q}} \to \mathrm{GL}_1(\mathcal{O})$ whose reduction to $\mathrm{GL}_1(\mathbb{F}_p)$ is equal to $\det(\bar{\rho})$ comes from (i.e., is the determinant of) such a representation ρ.

The fact that $\Lambda \to T$ is an isomorphism dovetails with the conjecture of Section 6 to give us (conjecturally) that the natural mapping $\Lambda \to R^\circ$ is an isomorphism, where R° is the universal ordinary deformation ring associated to $\bar{\rho}$.

The (conjectural) statement that $\Lambda \to R^\circ$ is an isomorphism translates, in turn, as follows. Let ρ be a representation as above which is not assumed to satisfy (a). Instead, ρ is merely assumed to be ordinary at p (in the sense of Galois representations; compare Section 2). Then (conjecturally) it also satisfies (b), i.e. it is determined by its determinant.

At this point we make use of the Proposition of Section 6, whose proof is given in Sections 8–9. This Proposition tells us that a knowledge of the ordinary deformation problem for $\bar{\rho}$ (i.e., the problem where one seeks only deformations of $\bar{\rho}$ which are ordinary as Galois representations) gives us a tight control of the general deformation problem for $\bar{\rho}$. Specifically, under a mild hypothesis (which in our present case rules out only the prime numbers $p = 11$ and 13) we have that if

$\Lambda \to R^\circ$ is an isomorphism, then the (*full*) universal deformation ring R associated to $\bar{\rho}$ is isomorphic to a power series ring in two variables over Λ. Thus, if the conjecture of Section 6 holds, we would have that R° is isomorphic to Λ and that R is isomorphic to a power series ring in two variables over Λ i.e., in the terminology of Section 6, the deformation theory for $\bar{\rho}$ is *cleanly unobstructed* {for all prime numbers $\rho \neq 11$ and 13 and such that $\tau(p)$ is not congruent to 0 mod p}.

We take comfort in the fact that this (conjectural) answer to the problem meshes well with results of Nigel Boston ([B1], [B2]) and work by Coates and Flach which is currently in progress. Moreover, Boston informs me that the excluded case of $p = 11$ in the above context is particularly interesting; for $\bar{\rho}$ and $p = 11$ he expects, but cannot yet prove, that the deformation theory is in fact obstructed and that R is a (singular) quotient of a power series ring over Λ in three variables by a principal ideal.

This note is the written version of the talk I gave at the Mordell Centennial Birthday Colloquium held in Cambridge, January 1988. I thank the organizers of that colloquium for inviting me, and the IHES and Vaughn Foundation for support during the time I wrote this article.

1. A review of deformation-theoretic results

Let k be a finite field of characteristic p. In this note, a *residual representation* shall mean an absolutely irreducible, continuous, representation

$$\bar{\rho}: G_{\mathbf{Q}} \to \mathrm{GL}_2(k)$$

which is unramified at all (finite) primes different from p. By a calculation of Tate (cf. [Se]) there are no such representations if $p = 2$, and consequently with no loss of generality *we assume that p is odd.* We say that $\det(\bar{\rho})$ is *odd* or *even* if it is, respectively, an odd or an even power of

$$\omega: G_{\mathbf{Q}} \to \mathbf{F}_p^* \subset k^*,$$

the basic character (which takes a *geometric* Frobenius element at the prime $l \neq p$ to the image of l in $\mathbf{F}_p^*$). It is convenient to assume that the field k is generated by the image of the trace, $\mathrm{tr} \circ \bar{\rho}: G_{\mathbf{Q}} \to k$, and we make that assumption.

Recall that if A is a complete local noetherian ring with residue field k, a *deformation* of $\bar{\rho}$ to A is a *strict* equivalence class of liftings $\rho_A: G_{\mathbf{Q}} \to \mathrm{GL}_2(A)$ of $\bar{\rho}$ which are unramified at (finite) primes different from p, where we recall that two liftings are said to be *strictly equivalent* if one can be brought to the other by conjugation with an element in $\mathrm{GL}_2(A)$ whose reduction to $\mathrm{GL}_2(k)$ is the identity (cf. [M], [B1], [B-M]). Recall also (loc. cit.) that since $\bar{\rho}$ has been assumed to be absolutely irreducible a *universal deformation ring*, $R = R(\bar{\rho})$ and a *universal deformation* $\rho: G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ exist. The ring $R(\bar{\rho})$ is determined up to unique isomorphism by the equivalence class of $\bar{\rho}$ where, by abuse of language, we allow $\boldsymbol{\rho}$ to stand for a choice of lifting, unique up to strict equivalence.

In [M] it is shown that if $\det \bar{\rho}$ is *odd* the Krull dimension of R/pR is $\geqslant 3$, and, moreover, if the Zariski tangent dimension of R/pR is equal to 3 then R is a formal power series ring on 3 parameters over $W(k)$, the ring of Witt vectors of k. If $\det \bar{\rho}$ is *even*, the assertions in the previous sentence remain valid with the number 3 replaced by 1. If, in the odd case, the Zariski tangent dimension of R/pR is $= 3$ (or, in the even case, if it is $= 1$) we shall say that the deformation theory for $\bar{\rho}$ is *unobstructed*. Recall also (loc. cit.) that the universal deformation ring for $\det \bar{\rho}: G_{\mathbf{Q}} \to k^*$ is canonically isomorphic to the Iwasawa algebra

$$\Lambda := \varprojlim_n W(k)[\Gamma/\Gamma_n],$$

where $\Gamma \subset \mathbb{Z}_p{}^*$ is the subgroup of 1-units, and $\Gamma_n \subset \Gamma$ is the closed subgroup of index p^n.

There is a canonical Λ-algebra structure on R obtained functorially by passing from deformations of $\bar{\rho}$ to deformations of $\det \bar{\rho}$ by application of the determinant. Since $p > 2$, Λ is isomorphic to a power series ring on one parameter over $W(k)$. When the deformation theory for $\bar{\rho}$ is unobstructed, R is a power series ring on two parameters over Λ (cf. [M]).

2. p-Ordinary representations

Fix an imbedding of algebraic closures $\bar{\mathbf{Q}} \subset \bar{\mathbf{Q}}_p$, and let I be the inertia subgroup at p in $G_{\mathbf{Q}}$ corresponding to this imbedding.

A representation $\rho_A: G_{\mathbf{Q}} \to \mathrm{GL}_2(A)$ is said to be *ordinary* if, giving $M = A \times A$ (the free A-module of rank 2) a $G_{\mathbf{Q}}$-module structure by composition of ρ_A with the standard representation of $\mathrm{GL}_2(A)$, we have that the submodule, M^I, of invariants under the action of the subgroup I, is a free A-module of rank one and a direct factor in M.

A representation ρ_A is *co-ordinary* if the quotient module M_I of co-invariants is a free A-module of rank one and a direct factor. Clearly the transformation

$$\rho_A \mapsto \rho_A \otimes \det(\rho_A^{-1})$$

interchanges ordinary and co-ordinary representations.

If $\bar{\rho}$ is an ordinary residual representation, then there is a (complete noetherian) local ring with residue field k, denoted $R^\circ = R^\circ(\bar{\rho})$, together with a deformation

$\boldsymbol{\rho}^\circ$ of $\bar{\rho}$ to R° which is universal for *ordinary* deformations of $\bar{\rho}$ ([M] 1.7 Prop. 3). We call R° the *universal ordinary deformation ring* of $\bar{\rho}$. It comes equipped with a canonical R-algebra structure.

3. Relations between ordinary deformations and all deformations

One of the objects of this note is to prove the following.

MAIN PROPOSITION. *If the (ordinary) residual representation $\bar{\rho}$ has the property that*

$$\det \bar{\rho} \neq 1, \omega, \omega^{-1} \text{ and } \omega^{(p-1)/2},$$

then the natural homomorphism $R \to R^\circ$ is surjective and its kernel is an ideal that can be generated by two elements.

For the proof see Section 8 and Section 9.

A consequence of this proposition is the following:

COROLLARY 1. *Let $\bar{\rho}$ be an ordinary residual representation of odd deteminant different from ω, ω^{-1}, and $\omega^{(p-1)/2}$. Then the Krull dimension of R°/pR° is $\geqslant 1$. If the Zariski tangent dimension of R°/pR° is $\leqslant 1$, then R° is a power series ring on one parameter over $\mathbf{Z}_p$ and R is a power series ring on two parameters over Λ.*

Proof of Corollary 1. Since R/pR has Krull dimension $\geqslant 3$, and since, by the main proposition, R°/pR° is a quotient of R/pR by an ideal generated by two elements, the Krull dimension of R°/pR° is $\geqslant 1$. Now suppose that the Zariski tangent dimension of R°/pR° is $\leqslant 1$. The proposition then implies that the Zariski tangent dimension of R/pR is $\leqslant 3$. But by [M], it then follows that R is a regualar local ring of Krull dimension 4, and more precisely a power series ring on two parameters over Λ. By the above proposition and by the hypothesis on the Zariski tangent dimension of R°/pR° it now follows that R° is a regular local ring of Krull dimension 2 and $p \in R^\circ$ is a regular element which yields the assertions in the last sentence of the Corollary. □

REMARK. Corollary 1 does not make precise the Λ-algebra structure of R°.

From now on (but with the exception of Section 8 and Section 9 below) we suppose that *the residual representation $\bar{\rho}$ is an ordinary, absolutely irreducible representation of odd determinant different from*

$$\omega, \omega^{-1} \quad \textit{and} \quad \omega^{(p-1)/2}.$$

If the deformation theory for $\bar{\rho}$ were *unobstructed* we would have things fairly well in hand, e.g., R would be a power series ring in two variables over Λ. But as the above discussion suggests, we may not have very good control over the Λ-algebra structure of R°. This motivates the following.

DEFINITION. We shall say that the deformation theory of $\bar{\rho}$ is *cleanly unobstructed* if the natural homomorphism $\Lambda \to R^\circ$ is an isomorphism and the universal deformation ring R is isomorphic, with its natural Λ-algebra structure, to a power series ring in two variables over Λ.

COROLLARY 2: *We suppose that the residual representation $\bar{\rho}$ satisfies our running hypothesis, i.e., it is an ordinary, absolutely irreducible representation of odd determinant different from ω, ω^{-1}, and $\omega^{(p-1)/2}$. Suppose further that the natural mapping $\Lambda \to R^\circ(\bar{\rho})$ is an isomorphism.*

Then the universal deformation ring R is a formally smooth Λ-algebra on two parameters, i.e, $\bar{\rho}$ has a cleanly unobstructed deformation theory.

Proof: This follows immediately from Corollary 1. □

Cleanly unobstructed deformation theories have been constructed in [B-M]. It was shown there that any "generic, admissible" $\mathscr{S}_3$-representation $\bar{\rho}$ has a cleanly obstructed deformation theory (See [B-M] for definition of 'admissible'). An object of the present note is to show that, conditional on the conjecture formulated in Section 6, cleanly unobstructed deformation theories are quite plentiful.

4. Analytic families of representations with fixed *p*-adic Hodge twists

Let $k = \mathbb{F}_p$ and let $\bar{\rho}$ be as in section 3. Suppose further that it has a cleanly obstructed deformation theory. Let $\mathrm{Hom}(-, -)$ denote *homomorphisms of local rings*, and put $X = \mathrm{Hom}(R, \mathbb{Z}_p)$, and $X^\circ = \mathrm{Hom}(R^\circ, \mathbb{Z}_p)$. We view X° as a p-adic analytic submanifold (over $\mathbb{Q}_p$, of dimension 1) of the three-dimensional p-adic analytic manifold X. The Λ-algebra structure of R gives a mapping (the "*determinant*") from X to $\mathrm{Hom}(\Lambda, \mathbb{Z}_p)$. Identify $\mathrm{Hom}(\Lambda, \mathbb{Z}_p)$ with $\mathbb{Z}_p \subset \mathbb{Q}_p$ by the rule $\varphi \mapsto a \in \mathbb{Z}_p$, where for a p-adic 1-unit $\gamma \in \Gamma \subset \mathbb{Z}_p^*, \varphi(\gamma) = \gamma^a \in \mathbb{Z}_p$. Let $\delta: X \to \mathbb{Q}_p$ denote the composition of the "determinant" mapping with the above imbedding. As in [M], we also have the locally analytic action of $\mathbb{Z}_p$ on X obtained by "twisting with a one-dimensional character". Specifically, if $b \in \mathbb{Z}_p$ define the character $\chi_b: G_{\mathbb{Q}} \to \Gamma \subset \mathbb{Z}_p^*$ by first projecting the cyclotomic character $\chi: G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ to the subgroup of 1-units to get a character $\chi_1: G_{\mathbb{Q}} \to \Gamma \subset \mathbb{Z}_p^*$ and then putting $\chi_b := (\chi_1)^b$. If x is a point of X, let $\rho_x: G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ be the representation associated to x, i.e., induced by specialization of the universal deformation ρ of $\bar{\rho}$ from R to $\mathbb{Z}_p$ via the homomorphism $x: R \to \mathbb{Z}_p$.

Now define, for all $b \in \mathbb{Z}_p$ and $x \in X$, a new point x' (also denoted $b*x$) by the rule $\rho_{x'} = \chi_b \cdot \rho_x$. The rule $(b, x) \mapsto b*x$ defines a locally analytic action of $\mathbb{Z}_p$ on X. We clearly have $\delta(x') = \delta(x) + 2b$.

Let $\rho_x^{(p)}$ denote the restriction of ρ_x to the decomposition subgroup $G_{\mathbb{Q}_p}$ and let V_x be $\mathbb{Q}_p \times \mathbb{Q}_p$, viewed as representation space for $\rho_x^{(p)}$. By the theory of Sen, ([Sen 1]) we can associate to the two-dimensional $\mathbb{Q}_p$-representation $\rho_x^{(p)}$ a (monic, quadratic) "characteristic polynomial" $T^2\text{-}dT + c$ with coefficients in $\mathbb{Q}_p$(cf. [Sen 1], for its definition) with these properties:

(a) Writing $d = d(x)$ and $c = c(x)$ to indicate dependence upon x, we have that $d(x) = \delta(x)$.

(b) Letting $x' := b*X$ we have

$$d(x') = d(x) + 2b$$
$$c(x') = c(x) + b \cdot d(x) + b^2.$$

(c) If $\mathbb{C}_p$ is the completion of $\bar{\mathbb{Q}}_p$, viewed as $G_{\mathbb{Q}_p}$-module, and if $V_p \otimes \mathbb{C}_p$ is given the diagonal $G_{\mathbb{Q}_p}$ structure, then the characteristic polynomial of $\rho_{x,p}$ depends only on the isomorphism class of the $\mathbb{C}_p$-vector space $V_p \otimes \mathbb{C}_p$ endowed with its semi-linear $G_{\mathbb{Q}_p}$-action.

(d) If the $G_{\mathbb{Q}_p}$-module $V_p \otimes \mathbb{C}_p$ has a two-stage filtration with successive quotients isomorphic to the $G_{\mathbb{Q}_p}$-modules $\mathbb{C}_p(r)$ and $\mathbb{C}_p(s)$ for $r, s \in \mathbb{Z}_p$, i.e., if $\rho_{x,p}$ has "p-adic Hodge twists r and s" (cf. [Sen 1] for a definition of these "p-adic Tate twist" modules) then r, s are the two roots of the characteristic polynomial of $\rho_{x,p}$, and conversely, if the roots of the characteristic polynomial of $\rho_x^{(p)}$ are p-adic integers r, s, then the $G_{\mathbb{Q}_p}$-module $V_p \otimes \mathbb{C}_p$ has a two-stage filtration whose two successive quotients are isomorphic to the $G_{\mathbb{Q}_p}$-modules

$\mathbb{C}_p(r)$ and $\mathbb{C}_p(s)$.

(c) Let $\mathscr{S}: X \to \mathbb{Q}_p \times \mathbb{Q}_p$ be the mapping which associates to each point $x \in X$ the coefficients (d, c) of the characteristic polynomial $T^2 - dT + c$ of $\rho_{x,p}$. Th $\mathscr{S}$ is a locally analytic mapping of p-adic analytic manifolds.

For proofs of the above statements, see [Sen 1, 2] and compare the discus given in [M].

PROPOSITION. *Let $\bar{\rho}$ satisfy our running hypotheses, and suppose furth has a cleanly unobstructed deformation theory. Then the jacobian $d\mathscr{S}$ mapping*

$$\mathscr{S}: X \to \mathbb{Q}_p \times \mathbb{Q}_p$$

has maximal rank at any point $x \in X$ which is

(i) *ordinary (i.e, such that $x \in X^\circ$), and such that*
(ii) $\delta(x) \neq 0$ *(equivalently, such that* $\det(\rho_x)$ *is not of finite order, i.e., such that ρ_x is not of "weight one").*

Proof. Since we have an isomorphism of Λ-algebras, $\Lambda \cong R^\circ$, one has that δ is an identification of X° with the p-adic analytic manifold $\mathbb{Z}_p$. Now consider the locally analytic mapping $\Sigma: \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Q}_p \times \mathbb{Q}_p$ given by the composition:

$$\mathbb{Z}_p \times \mathbb{Z}_p \xrightarrow[1 \times \delta^{-1}]{} \mathbb{Z}_p \times X^0 \subset \mathbb{Z}_p \times X \underset{\mathscr{S}}{\to} \mathbb{Q}_p \times \mathbb{Q}_p.$$

From the above discussion we have that

$$\Sigma(b, a) = (2b + a, b^2 + ab),$$

and one immediately calculates that the jacobian matrix $d\Sigma$ is of maximal rank (i.e., rank two) if $a \neq 0$. □

Now for a pair of elements $(d, c) \in \mathbb{Q}_p \times \mathbb{Q}_p$, let $X_{d,c} \subset X$ denote the locally analytic subspace which is $\mathscr{S}^{-1}(c, d)$, i.e., which consists of those $x \in X$ such that the characteristic polynomial of $\rho_{x,p}$ is $T^2 - dT + c$. Note that if $X_{d,c}$ contains an ordinary point, we must have $c = 0$ and $d \in \mathbb{Z}_p$, and furthermore the ordinary point it contains is unique. Let, then $c = 0$ and $d \in \mathbb{Z}_p$, and denote by x_0 the unique ordinary point in $X_{d,0}$. The subspace $X_{d,0} \subset X$ consists of all points x such that the representation space V_p attached to $\rho_x^{(p)}$ has the property that its associated $G_{\mathbb{Q}_p}$-module $V_p \otimes \mathbb{C}_p$ has a two-stage filtration with successive quotients isomorphic to the $G_{\mathbb{Q}_p}$-modules $\mathbb{C}_p = \mathbb{C}_p(0)$ and $\mathbb{C}_p(d)$ (coming in either order).

COROLLARY. *Let $\bar{\rho}$ satisfy our running hypotheses and suppose further that it has a cleanly unobstructed deformation theory. Let d be a nonzero p-adic integer and* [illegible]*et $X_{d,0}$ be the locally analytic subspace of X as above, which consists in those $x \in X$* [illegible] *"p-adic Hodge twists" 0 and d. Then there is a neighborhood U of the unique* [illegible]*inary point x_0 in $X_{d,0}$ which is a p-adic analytic manifold (over $\mathbb{Q}_p$) of dimension* [illegible] *particular, we may parametrize a suitable such neighborhood U by $t \in p^M\mathbb{Z}_p$* [illegible]*n appropriate positive integer M) to obtain an analytic family of inequivalent* [illegible]*entations unramified outside p lifting $\bar{\rho}$, having p-adic Hodge twists 0 and d,*

$$[illegible] \to GL_2(\mathbb{Z}_p). \qquad (*)$$

The [illegible]*ix coefficients of the analytic family of representations are power series in* [illegible] *unique ordinary representation in $X_{d,0}$ occurs for the value $t = 0$ (where $\rho_0 =$* [illegible]*).*

Proof. This follows immediately from the previous proposition and the implicit function theorem (in the context of p-adic analytic manifolds). □

REMARKS. (1) Any point x such that ρ_x is attached to a modular form of weight $k \geqslant 1$ must lie in the analytic space $X_{k-1,0}$. If $\bar{\rho}$ satisfies the hypotheses of the corollary we then have, for any $k > 1$, an analytic family (*) lying in $X_{k-1,0}$. How many members of that family can come from modular forms? See subsequent joint work with Carayol, Fontaine, and the author for results bearing on this question.

(2) Do we have an analytic family of the form (*) in $X_{0,0}$, i.e., in weight one?

5. Universal Hecke operators

One can define "*Hecke operators*" $T_l \in R$ ($l \neq p$) by the formula

$$T_l := \text{trace}_R\{\rho(\varphi_l)\}$$

where φ_l is the *geometric* Frobenius element at l. One can define an "*Atkin operator*" $U_p \in R^\circ$ as follows: restricting the universal ordinary deformation $\boldsymbol{\rho}^\circ$ to the decomposition group G_{Q_p} and to the submodule of inertial invariants in the universal ordinary representation, we obtain an unramified representation of $G_{\mathbf{Q}_p}$ on a free R°-module of rank one. If $\varphi_p \in G_{\mathbf{Q}_p}$ is a choice of geometric Frobenius, then the action of $\rho^\circ(\varphi_p)$ on this free R°-module of rank one is via a scalar in R°, which we define to be U_p. Since the $G_{\mathbf{Q}_p}$-representation on inertial invariants is unramified, this scalar is well-defined, and is independent of the choice of φ_p.

6. Relation between ordinary Galois representations and p-adic ordinary modular eigenforms

Consider pairs (f, v), where the first object of the pair, f, is a classical cuspidal modular form on $\Gamma_0(p^\nu)$ for some $\nu \geqslant 1$, with character ε and weight $w \geqslant 1$ and which is an eigenform for the Hecke operators T_l for prime numbers $l \neq p$ and for the Atkin operator U_p. Let $\mathcal{O}_f$ denote the ring generated by the Fourier coefficients $a_n(f)$ for $n \geqslant 1$. We suppose that $a_1(f) = 1$ so that $a_l(f)$ is the eigenvalue of T_l acting on f ($l \neq p$) and $a_p(f)$ is the eigenvalue of U_p. The second object of the pair, $v\colon \mathcal{O}_f \to k$ is a homomorphism from $\mathcal{O}_f$ to a finite field k.

Let $\mathcal{O}_{f,v}$ denote the completion of $\mathcal{O}_f$ with respect to the kernel of v, and for $a \in \mathcal{O}_{f,v}$, let $\bar{a}$ denote the projection of a to k.

We say that f is *ordinary* at v, or (f, v) is *ordinary*, if a_p is a unit in $\mathcal{O}_{f,v}$, or equivalently if $\bar{a}_p$ is a nonzero element of k.

We say that (f, v) *belongs to* $\bar{\rho}$ if for all prime numbers $l \neq p$, we have:

$$\det\{X - \bar{\rho}(\varphi_l)\} = X^2 - \bar{a}_l X + \bar{\varepsilon}(l) l^{w-1}$$

where φ_l is a (*geometric*) Frobenius element. Note that we have chosen to work with the *geometric* rather than the *arithmetic* Frobenius, and therefore our representations are *not* the same as in, e.g., [D]. Having made our choice, *ordinary* modular forms belong to *ordinary* representations, as defined in Section 2. Had we made the other choice, they would correspond to *co-ordinary* representations.

Let $\mathscr{K}_{f,v}$ denote the field of fractions of $\mathcal{O}_{f,v}$ and let

$$r: G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathscr{K}_{f,v})$$

denote the representation unramified outside p (unique up to $\mathscr{K}_{f,v}$-equivalence) such that

$$\det\{X - r(\varphi_l)\} = X^2 - a_l X + \varepsilon(l) l^{w-1}$$

for all prime numbers $l \neq p$. Such a representation has been shown to exist by the work of Shimura ($w = 2$), Deligne ($w \geqslant 2$), and Deligne-Serre ($w = 1$), (cf. [Sh], [D], [D-S]).

Recall that we have supposed $\bar{\rho}$ to be absolutely irreducible with determinant different from ω and ω^{-1}. Under this hypothesis, if (f, v) is ordinary and belongs to $\bar{\rho}$, it has been shown in [M-W] (and see [M-T] for a more general result valid in the context where there is an auxiliary level) that there is an ordinary representation,

$$\rho_{f,v}: G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_{f,v}),$$

unramified outside p, equivalent over $\mathscr{K}_{f,v}$ to r and which is a lifting of $\bar{\rho}$, with respect to the natural homomorphism $\mathrm{GL}_2(\mathcal{O}_{f,v}) \to \mathrm{GL}_2(k)$ induced by v. The strict equivalence class of the lifting $\rho_{f,v}$ is uniquely determined and therefore $\rho_{f,v}$ gives us an ordinary deformation of $\bar{\rho}$ to $\mathcal{O}_{f,v}$, i.e., it is induced by a unique homomorphism

$$h_{f,v}: R^{\circ} \to \mathcal{O}_{f,v}.$$

We now *suppose that there exists an ordinary pair* (f, v) *belonging to* $\bar{\rho}$.

Let $\mathscr{H}$ denote the commutative polynomial algebra over Λ generate by the symbols T_l for $l \neq p$ and by U_p. For each pair (f, v) belonging to $\bar{\rho}$, consider the homomorphism of Λ-algebras $\varphi(f, v): \mathscr{H} \to \mathcal{O}_{f,v}$ which takes T_l to $a_l(f) \in \mathcal{O}_{f,v}$ for all $l \neq p$ and U_p to $a_p(f)$. Let $\mathscr{C}$ denote a set of ordinary pairs (f, v) belonging to $\bar{\rho}$, and let $I_{\mathscr{C}} \subset \mathscr{H}$ denote the ideal

$$I_{\mathscr{C}} = \bigcap \ker \varphi_{f,v} \subset \mathscr{H}$$

where the intersection is taken over all pairs (f, v) in $\mathscr{C}$.

Let $\mathbf{T}_{\mathscr{C}}$ denote the quotient Λ-algebra, $\mathbf{T}_{\mathscr{C}} := \mathscr{H}/I_{\mathscr{C}}$. For w an integer, let $\mathscr{C}_w$ denote the set of all ordinary pairs (f, v) as above, belonging to $\bar{\rho}$, where f is of weight w.

THEOREM (Hida). *The ideal* $I_{\mathscr{C}_w}$, *and therefore the quotient algebra* $\mathbf{T}_{\mathscr{C}_w}$, *is independent of* w, *provided that* $w \geqslant 2$.

Proof. See [H1], [H2], and [G2]. □

DEFINITION. By Hilda's Hecke algebra $\mathbf{T}$, we mean $\mathbf{T}_{\mathscr{C}_w}$, for any $w \geqslant 2$.

To indicate dependence upon $\bar{\rho}$, we sometimes denote $\mathbf{T}$ by $\mathbf{T}(\bar{\rho})$. From the construction of $\mathbf{T}$, we obtain a mapping $R^\circ \to \mathbf{T}$ which 'factors' any of the $h_{f,v}$, where (f, v) is an ordnary pair belonging to $\bar{\rho}$, with f of weight $\geqslant 2$. Let $\eta_{f,v}\colon \mathbf{T} \to \mathcal{O}_{f,v}$ be the homomorphism whose composition with $R^\circ \to \mathbf{T}$ yields $h_{f,v}$. Let $\tau_l \in \mathbf{T}(l \neq p)$ denote the image of $T_l \in R$ and $u_p \in \mathbf{T}$ the image of $U_p \in R^\circ$.

It follows from [M-W], that for every ordinary pair (f, v) belonging to $\bar{\rho}$, the homomorphism $\eta_{f,v}$ brings the "Hecke operator" $\tau_l \in \mathbf{T}$ to the l-th Fourier coefficient $a_l(f)$ and it brings the "Atkin operator" $u_p \in \mathbf{T}$ to $a_p(f)$, the eigenvalue of U_p acting on the modular form f, in $\mathcal{O}_{f,v}$.

Concerning the structure of the Λ-algebra $\mathbf{T}$, we have:

PROPOSITION. (Hida). *The ring* $\mathbf{T}$ *is a finite flat* Λ*-algebra* [*generated by the elements* τ_l *for* $l \neq p$ *and by* u_p].

Proof. See [H1], [H2]. □

REMARKS. The ring $\mathbf{T}$ occurs in various notations in a number of articles: in [H1, 2], [T], and [M-T] it occurs as a localization of a ring denoted h_∞^{ord}, and it itself is denoted R; in [M-W] it is denoted $\mathbf{T}_{\mathfrak{m}}$.

CONJECTURE. *The homomorphism* $R^\circ \to \mathbf{T}$ *is an isomorphism.*

REMARKS. From the previous discussion it follows from the above conjecture that every ordinary representation of $G_{\mathbf{Q}}$ to $\mathrm{GL}_2(\mathcal{O})$ unramified outside p, where $\mathcal{O}$ is a finite discrete valuation ring extension of $\mathbb{Z}_p$ which is a lifting of $\bar{\rho}$ belongs to a p-adic p-ordinary modular eigenform with Fourier coefficients in $\mathcal{O}$. This conjecture is then a partial "complement" to the conjectures of Serre [Se]. See forthcoming joint work with J. Tilouine, [M-T], in which a more general version of this conjecture, involving auxiliary level, is discussed.

7. Residual representations attached to fixed weight and varying prime p:

For a choice of weight w in the set $\{12, 16, 18, 20, 22, 26\}$ let $f(=f_w)$ denote the unique cuspidal newform on $SL_2(\mathbf{Z})$ of that weight w. For any prime number p, let $\bar{\rho}_{f,p}$ denote the unique (semi-simple) representation mod p belonging to the newform f, i.e.,

$$\bar{\rho}_{f,p}: G_{\mathbf{Q}} \to GL_2(\mathbf{F}_p)$$

is unramified outside p, has the property that

$$\text{trace} \circ \bar{\rho}_{f,p}(\varphi_l) \equiv a_l(f) \bmod p, \quad \text{and} \quad \det \bar{\rho}_{f,p}(\varphi_l) \equiv l^{w-1} \bmod p$$

for all prime numbers $l \neq p$, where φ_l is the Frobenius element at l.

For each such choice of f and p, we have the Λ-algebras

$$\Lambda \to R(\bar{\rho}_{f,p}) \to R^\circ(\bar{\rho}_{f,p}) \to \mathbf{T}(\bar{\rho}_{f,p}).$$

Since these newforms f have weight > 2, a result implicit in the work of Hida (See Gouvêa [G1]) yields

PROPOSITION 1 (Hida, Gouvêa). *If the newform f is ordinary at p, i.e., if $a_p(f)$ is not divisible by p, then:*

$$\Lambda = \mathbf{T}(\bar{\rho}_{f,p}). \qquad \square$$

We now make the stipulations needed to guarantee that $\bar{\rho}_{f,p}$ satisfies our running hypotheses for $\bar{\rho}$, namely, *we suppose that*:

(1) $\bar{\rho}_{f,p}$ is absolutely irreducible,

(2) The weight w is congruent to neither $0, 2$ nor $(p-1)/2 \bmod p-1$, and

(3) $\bar{\rho}_{f,p}$ is ordinary, i.e., $a_p(f) \not\equiv 0 \bmod p$; equivalently, the pair (f, v) is an ordinary pair, where $v: \mathcal{O}_f = \mathbb{Z} \to \mathbb{F}_p$ is reduction mod p.

A consequence of the Conjecture of Section 6, the main proposition (Section 3), and the above proposition, is the following:

PROPOSITION 2. *Let $f(=f_w)$ be a newform as above* (*i.e.*, $w = 12, 16, 18, 20, 22,$ *or* 26) *and let p be a prime number such that (f, p) satisfies conditions* (1), (2), *and* (3) *above. Then if the conjecture of Section* 6 *holds, the deformation theory for $\bar{\rho}_{f,p}$ is cleanly unobstructed, i.e., $R(\bar{\rho}_{f,p})$ is a power series ring on 2 parameters over Λ and the Λ-algebra $R^\circ(\bar{\rho}_{f,p})$ is equal to Λ.* $\square$

EXAMPLE. Taking $w = 12$, $f = f_{12}$ is the modular form usually denoted Δ, whose Fourier expansion is given by

$$\Delta = q\prod(1 - q^n)^{24} = \sum\tau(n)q^n$$

where the infinite product and sum above is taken over all $n \geqslant 1$.

Using the known results about the image of $\bar{\rho}_{\Delta,p}$ for varying p ([Sw-D]), Conjecture 1 then specializes to

PROPOSITION 2. *If the conjecture of Section* 6 *holds, the deformation theory for* $\bar{\rho}_{\Delta,p}$ *is cleanly unobstructed, i.e.,* $R(\bar{\rho}_{\Delta,p})$ *is a power series ring on* 2 *parameters over* Λ *and* $\Lambda = R^{\circ}(\bar{\rho}_{\Delta,p})$, *for all prime numbers p different from* 11, 13, *and* 691, *and such that* $a_p(\Delta)$ $(= \tau(p))$ *is not congruent to* 0 *modulo p.* □

Notes. (1) We have excluded 691 as being the only prime number for which $\tau(p)$ is non-zero mod p and for which $\bar{\rho}_{\Delta,p}$ is not absolutely irreducible. It is the case, however, that the (*versal*) deformation theory for all the prime numbers p for which $\bar{\rho}_{\Delta,p}$ is not absolutely irreducible (i.e., $p = 2, 3, 5, 7$, and 691) has been worked out by Nigel Boston [B1]: for $p = 2$, the versal deformation ring $R(\bar{\rho}_{\Delta,p})$ is *not* smooth, while for $p = 3, 5, 7$, and 691 it is; for $p = 691$ the versal deformation theory is cleanly unobstructed. We have included the prime 23 in proposition 3 because although the assertion that the deformation theory for $p = 23$ is cleanly obstructed is *not* a formal consequence of the Conjecture in Section 6 and our main proposition, the deformation theory for $p = 23$ has in fact been *proven* to be cleanly obstructed in [M], and again in [B-M]. The requirement that p be ordinary for Δ does not appear to be terribly restrictive. For example, all primes p in the range $7 < p < 2411$ are ordinary for Δ.

(2) There is some reason to hope for a close connection between the question of whether the deformation theory at p for an eigenform is obstructed and the question of whether p divides a certain special value of a normalized L function of the symmetric square automorphic representation attached to the eigenform. See forthcoming work of Coates and Flach (in a slightly different context) which lends support to this hope. The fact that the relevant L function "special value" is nonzero for Δ we take as a fact compatible with the picture painted by the conjecture of Section 6. See also [C-S] for the construction of a p-adic L function attached to symmetric squares of certain modular forms, and [M-T] for related matters.

(3) It would be helpful to have a numerical clarification of the cases $p = 11$ and 13 (and $f = \Delta$). Nigel Boston tells me that the answer for $p = 11$ may be particularly interesting. See his future publications for a discussion of this case.

(4) A theorem of Gross ([Gr]), completed by numerical data obtained by Elkies and Atkin, shows that for all primes p in the range $11 \leqslant p \leqslant 3500$, and $p \neq 23, 691$, the representation $\bar{\rho}_{\Delta,p}$ has the property that the image of an inertia group at p has order divisible by p. This fact may easily be shown to imply, for this range of primes p, that for any point x in $X = \mathrm{Hom}(R(\bar{\rho}_{\Delta,p}), \mathbb{Z}_p)$ there are only two possibilities:

(i) The point x is *twist-ordinary* in the sense that an appropriate twist $x' = b*x$ of x by a one-dimensional character (cf. Section 4 above) is in the ordinary locus $X^\circ = \mathrm{Hom}(R^\circ(\bar{\rho}_{\Delta,p}), \mathbb{Z}_p)$.

(ii) The point x is *inertially ample* in the sense that the image of the inertia group at p under the representation $\rho_{x,p}$ contains an open subgroup in $SL_2(\mathbb{Z}_p)$.

In contrast to $\Delta\,(=f_{12})$, there are a few primes $p < 3{,}500$, and $w\,(> 12)$ as above such that f_w is ordinary at p and such that the image of inertia at p under $\bar{\rho}_{f_w,p}$ is of order *prime to p*. Specifically, in the terminology of [Gr], Atkin and Elkies found *companion forms* for certain f_w and p. It then follows by results of Serre that the image of inertia at p under $\bar{\rho}_{f_w,p}$ is tame. The complete list of such primes p (See [Gr]) is: for f_{16}, $p = 397$; for f_{18}, $p = 271$; for f_{20}, $p = 139$ and 379; for f_{22}, no such p; for f_{26}, $p = 107$. It would be interesting to know what the inertially ample locus is, in the universal deformation space, for the residual representations in these instances.

8. A good system of generators for the decomposition group

Let S be the set $\{p, \infty\}$, $G_{\mathbb{Q},S}$ the Galois group of the maximal subfield of $\bar{\mathbb{Q}}$ which is unramified outside S, and let $\bar{\rho}\colon G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ be an absolutely irreducible ordinary residual representation, with k a finite field of characteristic p. Let $L/\mathbb{Q}$ be the splitting field of $\bar{\rho}$, so that $G := \mathrm{Gal}(L/\mathbb{Q})$ may be identified, via $\bar{\rho}$, with a subgroup of $\mathrm{GL}_2(k)$. Let Π denote the "p-completion of $G_{\mathbb{Q},S}$ relative to $\bar{\rho}$" (see [B1] or [B-M]. Thus we have a short exact sequence,

$$1 \to P \to \Pi \to G \to 1,$$

where P is a normal pro-p subgroup of Π. The "*deformation theory*" of $\bar{\rho}\colon G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ factors through Π (for a discussion of this, see [B1]). Fix an imbedding $v\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ and consider the associated inertia and decomposition groups, relative to v, $I \subset D \subset \Pi$, so that I is the image of the inertia subgroup of $G_{\mathbb{Q}_p}$ in Π (via the map induced by v) and D is the image of the full group $G_{\mathbb{Q}_p}$.

Let $I^\circ \subset I$ and $D^\circ \subset D$ denote pro-p Sylow subgroups in I and in D respectively. Since $\bar{\rho}$ is ordinary one sees that I° is normal in I and D° is normal in D. Moreover put $A := I/I^\circ$ and $B := D/D^\circ$. Then B is an abelian group of order prime to p, and A is a cyclic group of order prime to p. The natural inclusion $I \subset D$ induces an injection $A \hookrightarrow B$.

Using the Schur-Zassenhaus theorem (cf. Proposition 2.1 of [B1]) we may find a lifting $A \hookrightarrow I$ and a compatible lifting $B \hookrightarrow D$. Fix such liftings, and identify A with its image in I and B with its image in D. We then have semi-direct product decompositions: $I = A \ltimes I^\circ$ and $D = B \ltimes D^\circ$.

Let K_v denote the intermediate field in the extension $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$ which is fixed by the kernel of the natural mapping $G_{\mathbb{Q}_p} \twoheadrightarrow B$, so that $\mathrm{Gal}(K_v/\mathbb{Q}_p) \cong B$.

LEMMA: *There are elements $x, y \in I^\circ$ and $z \in D^\circ$ with the following properties:*

(1) *The subgroup $B \hookrightarrow D$ is in the centralizer of z.*

(2) *If K_v contains no primitive* pth *root of* 1, *the element y is trivial. Otherwise, it satisfies the following commutation relation with elements of B: For $g \in B$,*

$$gyg^{-1} = y^{e(g)},$$

where $e: B \to \mathbb{Z}_p^*$ is the Teichmüller lifting of the cyclotomic character $\chi: B \to \mathbb{F}_p^*$ which defines the natural action of B on the subgroup of p-th roots of unity in K_v. Exponentiation above refers to the operation of raising an element in a pro-p-group to a p-adic unit power.

(3) *The elements $\{x^g = gxg^{-1}$ (for $g \in B$), y, and $z\}$ generate D° as a pro-p-group.*

(4) *The closed normal subgroup generated by the elements $\{x^g$ (for $g \in B$) and $y\}$ is equal to I°.*

Proof. Here we use the techniques of [B1] but see also: [B2], [B-M]). The lemma will follow directly from a computation of the structure of the p-Frattini quotient groups of the local Galois group G_{K_v} and its inertia subgroup $\mathrm{I}_{K_v} \subset G_{K_v}$ viewed as B-modules via the natural action ($B = \mathrm{Gal}(K_v/\mathbb{Q})$). But the p-Frattini quotient of G_{K_v} is isomorphic, as B-module, to $(K_v^*)/(K_v^*)^p$ and the image of I_{K_v} in it is equal to the subgroup $(\mathcal{O}_v^*)/(\mathcal{O}_v^*)^p$, giving us an exact sequence of B-modules,

$$0 \to (\mathcal{O}_v^*)/(\mathcal{O}_v^*)^p \to (K_v^*)/(K_v^*)^p \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

The action of B on $\mathbb{Z}/p\mathbb{Z}$ above is trivial, and the exact sequence of B-modules splits. The B-module $(\mathcal{O}_v^*)/(\mathcal{O}_v^*)^p$ is isomorphic to the direct sum of the regular representation, $\mathbb{F}_p[B]$, and $\mu_p(K_v)$ where the action of B on $\mu_p(K_v)$ is the natural action of $\mathrm{Gal}(K_v/\mathbb{Q})$. Thus this module is just the regular representation if K_v contains no nontrivial pth roots of unity. It follows that we can find three elements $\bar{x}, \bar{y}, \bar{z}$ in the p-Frattini quotient of G_{K_v} [we view this p-Frattini quotient as $(K_v^*)/(K_v^*)^p$], with the following properties:

(i) the element $\bar{z}$ is fixed under the action of B,

(ii) the elements $\bar{x}$ and $\bar{y}$ are in the subspace $(\mathcal{O}_v^*)/(\mathcal{O}_v^*)^p$, and that subspace is generated by

$$\{g \cdot \bar{x}\ (g \in B) \text{ and } \bar{y}\},$$

(iii) the element $\bar{y}$ is trivial if K_v contains no nontrivial pth roots of 1; otherwise it is an eigenvector for the action of B, which acts as the cyclotomic character χ on it,

(iv) the p-Frattini quotient $(K_v^*)/(K_v^*)^p$ can be generated by the elements $\{g \cdot \bar{x}(\text{for } g \in B), \bar{y}, \text{ and } \bar{z}\}$.

By [B1] Proposition 2.3, we may find liftings y, z in D°, of $\bar{y}$, $\bar{z}$, respectively, which satisfy property (1) and the commutation law part of property (2), i.e. $gyg^{-1} = y^{e(g)}$ for $g \in B$. Since $\det(\bar{\rho})$ is nontrivial, it immediately follows that y is in fact in I°, because D°/I° is fixed under the action of B and consequently the projection of y to D°/I° is both fixed under B and subject to the commutation law described above. Thus property (2) holds. Now choose any lifting x of $\bar{x}$ to I°. By Burnside's theorem (cf. [B1] Proposition 2.2), the set of elements $\{x^g\ (g \in B), y, \text{and } z\}$ generate D°, giving property (3).

As for property (4), let $J \lhd D^\circ$ denote the closed normal subgroup generated by the set of elements $\{x^g\ (g \in B), \text{ and } y\}$. Then J is contained in I°. Also, D°/J is generated by a single element (the image of z); therefore $D^\circ/J \twoheadrightarrow D^\circ/I^\circ \cong \mathbb{Z}_p$ is an isomorphism, and $J = I^\circ$. □

9. Proof of the main proposition

Recall its statement, from Section 3 above.

PROPOSITION: *If the (ordinary) residual representation $\bar{\rho}$ has the property that its determinant is neither trivial nor of order two nor ω nor ω^{-1}, then the natural homomorphism $R \to R^\circ$ is surjective and its kernel is an ideal that can be generated by two elements.*

Proof. After conjugating $\bar{\rho}$, if necessary, we may assume that the image of $B \hookrightarrow D$ under $\bar{\rho}$ is a subgroup of diagonal matrices in $\mathrm{GL}_2(k)$ and that $A \subset B$ maps to matrices of the form

$$\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}. \qquad (*)$$

Now we introduce the universal deformation of $\bar{\rho}$, which may be viewed as a homomorphism

$$\rho: \Pi \to \mathrm{GL}_2(R)$$

where R is the universal deformation ring of $\bar{\rho}$, and where ρ is determined only up to strict equivalence. We can, and do, choose ρ in its strict equivalence class so that the image of B lies in the image in $\mathrm{GL}_2(R)$ of the subgroup of diagonal matrices of $\mathrm{GL}_2(W(k))$–the mapping $\mathrm{GL}_2(W(k)) \to \mathrm{GL}_2(R)$ being induced from the natural homomorphism $W(k) \to R$. We may (and do) arrange it, furthermore, so that the image of A lies in the image of the subgroup of diagonal matrices of

$GL_2(W(k))$ of the form

$$\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}.$$

Let x, y, z be elements of D° having the properties stipulated in the lemma. We consider, in turn, the images of these elements under ρ.

Since $\det(\bar{\rho}) = \omega^j$, with $j \not\equiv 0 \mod p-1$, $\det(\bar{\rho})$ is also nontrivial when restricted to A. It then follows from property (1) that $\rho(z)$ is a diagonal matrix in $GL_2(R)$.

Claim. $\rho(y) = 1$.

Proof of claim. Let $u = \rho(y) \in GL_2(R)$, and let $\bar{u} \in GL_2(k)$ be its reduction modulo the mapping induced by $R \to k$. Since y is in I°, it follows that $\bar{u}$ is either trivial or of order p; it is, in particular, unipotent. Suppose that $\bar{u}$ is not the identity. Then its eigenspace in $V = k \times k$ is one-dimensional, and by property (2) its eigenspace must be stabilized by the action of B. Consequently, it must also be stabilized by the action of A. Since $\det(\bar{\rho})$ is nontrivial when restricted to A, which is a subgroup of matrices of the form (∗), it immediately follows from property (2) that $\bar{u}$ is either upper or lower triangular in $GL_2(k)$. But now, since $\det(\bar{\rho})$ is neither ω nor ω^{-1}, a simple matrix calculation shows that property (2) is contradictory. Therefore $\bar{u} = 1$.

To deduce that $u = 1$, we work inductively: Let $I_2 \subset I_1$ be ideals in R, put $R_j := R/I_j$ $(j = 1, 2)$ and let $u_j \in R_j$ denote the projection of u to R_j. We suppose that $\mathfrak{m} \cdot I_1 \subset I_2$, where $\mathfrak{m}$ is the maximal ideal in R. The kernel, then, of the projection $R_2 \twoheadrightarrow R_1$ is naturally endowed with the structure of vector space over k; we suppose it to be of dimension 1, and therefore generated by a single element, call it ε, such that $\mathfrak{m} \cdot \varepsilon = 0$. We suppose that $u_1 = 1$. We shall prove that u_2 is also 1.

Write $u_2 = 1 + \varepsilon \cdot M$, where M is a 2×2 matrix with entries in k. Find an element $g \in A$ such that $\chi(g) \neq \pm 1$ in $\mathbb{F}_p^*$. By property (2) we have that $\bar{\rho}(g) \cdot M \cdot \bar{\rho}(g)^{-1} = \chi(g) \cdot M$, from which we get that M has trace and determinant zero. But then $1 + M$ is unipotent, and so by the argument already given (for $\bar{u}$ above), M must vanish. Since we can find a countable sequence of ideals $\mathfrak{m} = \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots$ such that $\mathfrak{a}_j \supset \mathfrak{a}_{j+1}$ has the properties required of $I_1 \supset I_2$ above, and such that $\cap \mathfrak{a}_j = 0$, we conclude that $u = 1$. □

As for $\rho(x) \in GL_2(R)$, write it out as a matrix,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

with entries a, b, c, d, in R. Since $\bar{\rho}$ is ordinary and we have normalized things so that the image of I under $\bar{\rho}$ is in (*) above, $a - 1$ and c lie in the maximal ideal $\mathfrak{m} \subset R$. Form the quotient ring $R' := R/(a - 1, c)$, and let

$$\rho' : \Pi \to \mathrm{GL}_2(R')$$

be the homomorphism induced from ρ by projection. By brutal design, x then maps to the semi-Borel subgroup of the form

$$\begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}$$

in $\mathrm{GL}_2(R')$, under the homomorphism ρ'. But it is also the case that B and z map to diagonal matrices in $\mathrm{GL}_2(R')$ and y maps to the identity. From property (4) it then follows that I° also maps to the above semi-Borel subgroup, and from property (3) that D° maps to the Borel subgroup

$$\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}.$$

As a consequence we have that ρ' is an ordinary deformation of $\bar{\rho}$. There is therefore a unique local ring homomorphism $R^\circ \to R'$ such that composition of it with the natural homomorphism $R \to R^\circ$ yields the projection $R \twoheadrightarrow R'$. If $\rho^\circ : \Pi \to \mathrm{GL}_2(R^\circ)$ denotes the homomorphism induced from ρ, i.e., ρ° is a representative for the universal ordinary deformation of $\bar{\rho}$, then ρ' is induced from ρ° via $R^\circ \to R'$. Our proposition would follow if we show that a maps to 1 and c to 0 under the homomorphism $R \to R^\circ$, for then we would have that $R' \subset R^\circ$ and the representation ρ', which has already been shown to be ordinary, induces ρ°. By universality of ρ°, we would have $R' = R^\circ$ and $\rho' = \rho^\circ$.

Let $M^\circ = R^\circ \times R^\circ$ be given a Π-module structure via composition of ρ° with the standard action of $\mathrm{GL}_2(R^\circ)$ on M°[M° is viewed as 1×2 column vectors with entries in R°]. Now note that the sub-module in M° consisting of vectors fixed under the action of A is the free R°-module of rank 1, $R^\circ \times 0 \subset M^\circ$. Since ρ° is ordinary, it then follows that $R^\circ \times 0$ must be fixed by all of I°, and in particular, by x. This certainly gives us that the element $a \in R$ is sent to 1 and c to 0 under the homomorphism $R \to R^\circ$. □

10. References

[B1] N. Boston, Explicit deformations of Galois representations. IHES preprint (1988). To appear.

[B2] N. Boston, Deformations of Galois representations associated to the cusp form Δ. IHES preprint (1988). To appear.

[B-M] N. Boston and B. Mazur, Explicit universal deformations of Galois representations. *Algebraic Number Theory in honor of K. Iwasawa.* Advanced Studies in Pure Mathematics series, *17*. Academic Press (1989) 1–21.

[C-S] J. Coates and C-G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve. *J. Reine Angew. Math.* 375/376 (1987) 104–156.

[D] P. Deligne, Formes modulaires et représentations l-adiques. Séminaire Bourbaki 68/69 no. 355. *Lecture Notes in Mathematics* 179 pp. 136–172. Springer-Verlag, Berlin-Heidleberg-New York 1971.

[D – S] P. Deligne and J.-P. Serre, Formes modulaires de poids 1. *Ann. Sci. Ec. Norm. Sup.* 7 (1974), 507–530 [Republished in J.-P. Serre *Oeuvres. Collected Papers* Vol. III pp. 193–216, Springer-Verlag, New York-Heidleberg-Berlin-Tokyo 1986].

[G1] F. Gouvêa, On the ordinary Hecke algebra. IHES Preprint. 1988. To appear.

[G2] F. Gouvêa, Arithmetic of p-adic Modular Forms. *Lecture Notes in Mathematics* 1304. Springer Verlag, Berlin-Heidleberg-New York 1988.

[Gr] B. Gross, The Galois representations associated to modular forms (mod p). Preprint 1988. To appear.

[H1] H. Hida, Galois representations in $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms. *Inv. Math.* 85 (1986) 545–613.

[H2] H. Hida, Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. Ec. Norm. Sup.* 19 (1986) 231–273.

[M] B. Mazur, Deforming Galois representations. In Y. Ihara, K. Ribet, and J.-P. Serre, eds., *Galois Groups over* **Q**, Proceedings of a workshop held at MSRI in March 1987. Springer-Verlag (1989) 385–437.

[M-T] B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler, et conjectures principales. To appear.

[M-W] B. Mazur and A. Wiles, On p-adic analytic families of Galois representations. *Comp. Math.* 59 (1986) 231–264.

[Se] J.-P. Serre, Valeurs propres des opérateurs de Hecke modulo l. Journées arith. Bordeaux, Astérisque 24–25 (1975), 109–117 [Republished in J.-P. Serre *Oeuvres. Collected Papers* Vol. III pp. 226–234, Springer-Verlag New York Heidleberg Berlin Tokyo 1986].

[Sen 1] S. Sen, Continuous cohomology and p-adic Galois representations. *Inv. Math.* 62 (1980) 87–116.

[Sen 2] S. Sen, The analytic variation of p-adic Hodge structure. *Annals of Math.* 127 (1988) 647–661.

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic forms. Publ. Math. Soc.* Japan II Tokyo Princeton (1971).

[Sw-D] P. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms. *Lecture Notes in Mathematics* 350 pp. 1–55. Springer-Verlag, Berlin-Heidleberg-New York (1973).

[T] J. Tilouine, Un sous-groupe p-divisible de la jacobienne de $X_1(N_p^r)$ comme module sur l'algèbre de Hecke. *Bull. Math. Soc. Fr.* 115 (1987) 329–360.