COMPOSITIO MATHEMATICA

B. MAZUR
A. WILES

On p-adic analytic families of Galois representations

Compositio Mathematica, tome 59, nº 2 (1986), p. 231-264
<http://www.numdam.org/item?id=CM_1986__59_2_231_0>

Compositio Mathematica 59 (1986) 231–264

ON p-ADIC ANALYTIC FAMILIES OF GALOIS REPRESENTATIONS

B. Mazur and A. Wiles

Contents

Introduction

Hida has produced interesting examples of continuous Galois representations

$$\rho_p : G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p[[T]]) \tag{1}$$

which are unramified outside the prime number p, where $G_{\mathbf{Q}}$ is the absolute Galois group of an algebraic closure to $\mathbf{Q}$. These are obtained as applications of the theory he has developed in [Hi 1], [Hi 2].

By composition with the homomorphisms

$$\mathbf{Z}_p[[T]] \xrightarrow{s_k} \mathbf{Z}_p$$

$$1 + T \mapsto (1+p)^{k-1}$$

ρ_p gives rise to a p-adic analytic family of Galois representations

$$\rho_p^{(k)}: G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p)$$

parametrized by k in $\mathbf{Z}_p$.

Hida has shown that for the integer values $k = 2, 3, 4, \ldots$ the specialized representations $\rho_p^{(k)}$ are isomorphic (over $\mathbf{Q}_p$) to the Deligne p-adic representations attached to cuspidal newforms of weight k. Thus one may view his p-adic analytic families of Galois representations as being p-adic "interpolations" of Deligne representations.

An interesting special case of Hida's construction is obtained in connection with the unique cuspform Δ of level 1 and weight 12. He obtains a representation

$$\rho_{p,\Delta}: G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p[[T]]) \tag{2}$$

as an example of his general theory, for some prime numbers p such that the Ramanujan function $\tau(p)$ is not divisible by p. The specialization $\rho_{\mathrm{p},\Delta}^{(12)}$ to weight $k = 12$ is the p-adic Deligne representation attached to Δ. See §13 below.

The object of this paper is to study the geometry of Hida's general construction. We connect his theory with the theory of Igusa Towers developed in [M-W 2]. We also obtain control of the action of the inertia group at p in Hida's representation. In particular, we analyze the p-adic Hodge structure of the representations $\rho_p^{(k)}$. As an application of this theory, together with results due to Nigel Boston (see Appendix), we obtain reasonably general results indicating that the image of ρ_p is large. For example, in the case of the representations $\rho_{p,\Delta}$, the image of $\rho_{p,\Delta}$ contains all of $\mathrm{SL}_2(\mathbf{Z}_p[[T]])$ provided $p > 11$, p is different from 23 and 691, and $\tau(p) \not\equiv 0 \bmod p$. In these cases, the specialization to weight one $\rho_{p,\Delta}^{(1)}$ is not the Deligne-Serre representation attached to a classical newform of weight one. Indeed we show that for $p = 13$, 17 and 19 (cf. §12, §13 below) that the p-adic Hodge structure of $\rho_{p,\Delta}^{(1)}$ is not even semi-simple (and hence is not of Hodge-Tate type!). Our proof makes it seem to us that the phenomenon of non-semi-simplicity will persist for many $\rho_p^{(1)}$. Note that when $\rho_p^{(1)}$ is not semi-simple it follows from recent work of Faltings (cf. [Fa] and future publications) on the conjecture of Tate regarding p-adic Hodge structure, that the restriction to the decomposition group at p of the representation $\rho_p^{(1)}$ cannot occur in the étale cohomology of any smooth projective variety over a finite extension field of $\mathbf{Q}_p$ which possess good reduction at p.

In our examples (§13) as in general, the representations obtained by specializing to weight 1 (and weight 0, $-1, \ldots$) deserve to be studied further. Do they occur in compatible families? For a prime number $l \neq p$, are the traces of Frobenius elements at l algebraic?

We fix p a prime number $\geqslant 5$, but since our theory will be trivial for $p \leqslant 11$, we lose no generality by supposing $p \geqslant 13$.

If K is a field, G_K refers to the Galois group of an algebraic closure $\overline{K}$ over K. For the standard fields with which we shall be dealing, i.e., $\mathbf{Q}$, $\mathbf{Q}_p$, and $\mathbf{F}_p$ we suppose that algebraic closures $\overline{\mathbf{Q}}$, $\overline{\mathbf{Q}}_p$, $\overline{\mathbf{F}}_p$ have been chosen, indeed, with compatibilities made explicit when needed (cf. proof of proposition 2 in §4 below). A primitive p^n-th root of unity in $\overline{\mathbf{Q}}$ or in $\overline{\mathbf{Q}}_p$ will be denoted ζ_{p^n}, or sometimes just ζ if no confusion can arise.

If X is an S-scheme, we will indicate this by sometimes writing $X_{/S}$. For $S'_{/S}$ the base change of $X_{/S}$ to S' will be denoted $X_{/S'}$. If $S = \mathrm{Spec}(A)$ is an affine scheme we will sometimes denote $X_{/S}$ as $X_{/A}$.

§1. Good quotients of $J_1(p^n)$:

In this section we shall be dealing with curves and abelian varieties over $\mathbf{Q}$. Set:

$$X_n = X_1(p^n) \quad \text{and} \quad Z_n = X_1(p^n, p^{n-1})$$

using the notation of [M-W 1] Chap. 3. Thus, Z_n is the canonical model over $\mathbf{Q}$ whose associated Riemann surface is the completion of the quotient of the upper half-plane by the action of the group

$$\Gamma_0(p^n) \cap \Gamma_1(p^{n-1}).$$

We have natural mappings

$$X_n \xrightarrow{\pi} Z_n \xrightarrow{\rho} X_{n-1} \quad (n \geqslant 1)$$

which induce mappings on jacobians,

$$JX_n \xleftarrow{\pi^*} JZ_n \xrightarrow{\rho_*} JX_{n-1} \quad (n \geqslant 1).$$

We now define quotient abelian varieties,

$$J_1(p^n) = JX_n \overset{\alpha_n}{\twoheadrightarrow} A_n$$

by the following inductive procedure: $A_0 = 0$; $A_1 = J_1(p)/\text{image } J_0(p)$ with α_1 the natural projection. For $n \geqslant 1$, A_{n+1} is linked to A_n by the diagram below, whose horizontal lines are exact sequences of commutative group schemes over **Q**.

$$\begin{array}{ccccccc} \mathscr{K}_{n+1} & \to & JX_{n+1} & \xrightarrow{\alpha_{n+1}} & A_{n+1} & \to & 0 \\ \uparrow = & & \uparrow \pi^* & & & & \\ 0 \to \mathscr{K}_{n+1} & \to & JZ_{n+1} & \xrightarrow{\alpha_n \rho_*} & A_n. & & \end{array}$$

A fairly complete account of the basic properties of these quotients A_n is given in [M-W 1] Chap. 3. The cotangent space of A_n may be identified (via α_n) with the subspace of cuspforms of weight 2 on $\Gamma_1(p^n)$ generated by (new) forms of primitive nebentypus, i.e., new forms on $\Gamma_1(p^i)$ (for $i \leqslant n$) with nebentypus character of conductor p^i. By a theorem of Langlands (see discussion in [M-W 1] Chap. 3 or [K-M]) it follows that A_n achieves "everywhere good reduction" over the field $\mathbf{Q}(\zeta_{p^n})$.

Using the n distinct "degeneracy operators" (cf. [M1] §2; these are the operators denoted B_d) from $J_0(p)$ to $J_0(p^n)$ and then mapping $J_0(p^n)$ to $J_1(p^n)$ in the natural way, we obtain a mapping

$$\underbrace{J_0(p) \times J_0(p) \times \ldots \times J_0(p)}_{n} \xrightarrow{\beta_n} J_1(p^n)$$

with finite kernel.

Let $U_p: J_1(p^n) \to J_1(p^n)$ denote the Atkin operator ([M-W 1]) and let the superscript ^{0} denote the connected component containing the identity.

Proposition: *The mapping α_n factors as indicated in the diagram of commutative group schemes over **Q** below, and the horizontal line is a "complex, with finite homology" (Note: it is not necessarily exact).*

$$\begin{array}{ccccc} & \overset{\beta_n}{\nearrow} & J_1(p^n) & \overset{\alpha_n}{\searrow} & \\ & & \downarrow & & \\ 0 \to J_0(p)^n & \to & J_1(p^n)/(\ker U_p^{n-1})^0 & \to & A_n \to 0 \end{array}$$

Proof: The cusp forms of weight 2 on $\Gamma_1(p^n)$ decompose into the direct sum of subspaces $C(\phi)$ where ϕ runs through the newforms (cuspidal, of weight 2) on $\Gamma_1(p^i)$ for $i \leqslant n$. If ϕ is new on $\Gamma_1(p^i)$, then $C(\phi)$ is of dimension $n-i+1$, the minimal polynomial of the operator U_p on $C(\phi)$

is equal to its characteristic polynomial, and, moreover, has the form $x^{n-i}(x-a_p)$ where a_p is the eigenvalue of U_p acting on ϕ. By a result of Ogg and Li, [O], [Li], a_p is zero if and only if $i \geqslant 2$, and ϕ is not of primitive nebentypus. The proposition follows.

§2. Models of modular curves

In this section, we shall be recalling constructions made in [K-M] and [M-W 1]. The basic diagram of modular schemes which we shall need and which deserves some explanation, is:

$$\begin{array}{l} \mathrm{Ig}(p^n)_{/\mathbf{F}_p} \hookleftarrow \mathscr{X}_1(p^n)_{/\mathbf{F}_p} \hookrightarrow \mathscr{X}_1(p^n)_{/\mathbf{Z}[\zeta]} \hookrightarrow X_1(p^n)_{\mathbf{Z}[\zeta]} \\ \mathrm{Ig}(p^n)_{/\mathbf{F}_p} \hookleftarrow \mathscr{X}_1(p^n)_{/\mathbf{F}_p} \hookrightarrow \mathscr{X}_1(p^n)_{/\mathbf{Z}} \hookrightarrow X_1(p^n)_{\mathbf{Z}}. \end{array} \qquad (D_n)$$

The curve $\mathscr{X}_1(p^n)_{/S}$ (the "incomplete" model) is the fine moduli scheme ($n \geqslant 1$) attached to the problem of classifying isomorphism classes $(E, \alpha_n : \boldsymbol{\mu}_{p^n} \hookrightarrow E)_{/S'}$ over S-schemes S' of pairs consisting of $E_{/S'}$, an elliptic curve over S' and isomorphisms α_n of $\boldsymbol{\mu}_{p^n/S'}$ onto closed finite flat subgroup schemes of E (over S').

The formation of $\mathscr{X}_1(p^n)_{/S}$ commutes with base change over S (in conformity with our notational convention for the subscript $_{/S}$) and $\mathscr{X}_1(p^n)_{/\mathbf{F}_p}$ may be viewed as the fiber in characteristic p of either $\mathscr{X}_1(p^n)_{/\mathbf{Z}}$ or $\mathscr{X}_1(p^n)_{/\mathbf{Z}[\zeta]}$, its base change to $\mathbf{Z}[\zeta]$.

The curve $\mathrm{Ig}(p^n)_{/\mathbf{F}_p}$ (the "Igusa curve of level p^n") is the complete smooth model of the incomplete curve $\mathscr{X}_1(p^n)_{/\mathbf{F}_p}$. For a detailed treatment of Igusa curves, see Chap. 12 of [K-M].

The proper scheme $X_1(p^n)_{\mathbf{Z}}$ may be briefly described as the normalization of $\mathscr{X}_1(p^n)_{/\mathbf{Z}}$ over the j-line over $\mathbf{Z}$, and $X_1(p^n)_{\mathbf{Z}[\zeta]}$ may be described similarly, with $\mathbf{Z}$ replaced by $\mathbf{Z}[\zeta]$. As explained in the introduction to [K-M] this terse description tells us very little about these proper schemes. Nevertheless, much of their structure is made explicit in [K-M] (cf. also Chap. 2 of [M-W 1]). Note that the scheme $X_1(p^n)_{\mathbf{Z}[\zeta]}$ is *not* the base change to $\mathbf{Z}[\zeta]$ of the scheme $X_1(p^n)_{\mathbf{Z}}$ (which is the reason why we have not written the subscripts with a "/").

Indeed, there is a natural morphism

$$X_1(p_n)_{\mathbf{Z}[\zeta]} \to X_1(p^n)_{\mathbf{Z}} \otimes \mathbf{Z}[\zeta] \qquad (1)$$

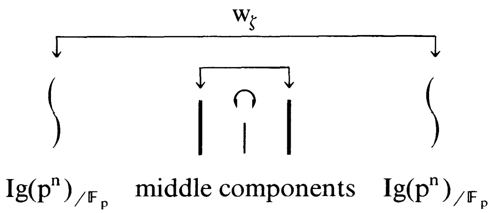
which is an isomorphism on the incomplete moduli scheme, but not, in fact, an isomorphism if $n \geqslant 1$. Recall, also, the involution w_ζ of the scheme $X_1(p^n)_{\mathbf{Z}[\zeta]}$ ([M-W 1] chap. 2). Note that there is *no* involution of the scheme $X_1(p^n)_{\mathbf{Z}} \otimes \mathbb{Z}[\zeta]$ compatible with w_ζ via (1).

The normalization,

$$X_1\widetilde{(p^n)_{\mathbf{Z}[\zeta]} \otimes \mathbf{F}_p} \qquad (2)$$

of the characteristic p fibre of $X_1(p^n)_{\mathbf{Z}[\zeta]}$ has the property that the natural inclusion of the incomplete moduli space $\mathscr{X}_1(p^n)_{/\mathbf{F}_p}$ in it extends to an isomorphism i_1 from $\mathrm{Ig}(p^n)_{/\mathbf{F}_p}$ to *one* connected component of (2). Let i_2 denote the composition of i_1 with the involution w_ζ. Then i_2 identifies $\mathrm{Ig}(p^n)_{/\mathbf{F}_p}$ with another component of (2). These two components are referred to as the "*good*" components of (2); all the other components are called "*middle*" components.

A schematic picture of (2) is then:



(In our picture we have supposed n to be odd, but consult [K-M] and [M-W 1] for a more detailed picture).

One other structure to be made explicit is the "*geometric inertial action*" on the characteristic p fibre. Let

$$I = \mathrm{Gal}\big(\mathbf{Q}_p(\zeta)/\mathbf{Q}_p\big) = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \underset{\cong}{\to} (\mathbf{Z}/p^n\mathbf{Z})^*$$

where the right-most isomorphism is the standard one: $g \in I$ is sent to $a_g \in (\mathbf{Z}/p^n\mathbf{Z})^*$ such that $g \cdot \zeta = \zeta^a g$.

Consider the obvious action of I on $X_1(p^n)_{\mathbf{Z}} \otimes \mathbf{Z}[\zeta]$, i.e. $g \in I$ acts via $1 \otimes g$. There is a natural action of I on the scheme $X_1(p^n)_{\mathbf{Z}[\zeta]}$ so that the morphism (1) is I-equivariant (cf. [K-M], [M-W 1]). The action of I on (1) induces a geometric action on characteristic p fibers:

$$X_1(p^n)_{\mathbf{Z}[\zeta]} \otimes \mathbf{F}_p \to X_1(p^n)_{\mathbf{Z}} \otimes \mathbf{F}_p. \qquad (3)$$

Since I acts trivially on the range of (3), and since (3) is I-equivalent, we have that the induced action of I on the normalization (2) has the following properties:

$$\begin{cases} \text{(a) I acts as the identity on the good component } i_1 \cdot \mathrm{Ig}(p^n)_{/\mathbf{F}_p}. \\ \text{(b) I preserves the set of middle components.} \\ \text{(c) I preserves the good component } i_2 \cdot \mathrm{Ig}(p^n). \end{cases} \qquad (4)$$

We may sharpen (c): Since, for $g \in I$, and $x \in i_1 \cdot \mathrm{Ig}(p^n)(\tilde{\mathbf{F}}_p)$,

$$g \cdot w_\zeta(x) = w_{g \cdot \zeta} g \cdot x = w_{g \cdot \zeta} x = w_{\zeta a_g} x = \langle a_g \rangle w_\zeta(x),$$

we see that $g \in I$ acts like the diamond operator $\langle a_g \rangle$ on $i_2 \cdot \mathrm{Ig}(p^n)_{/\mathbf{F}_p}$.

There is a natural morphism of the diagram (D_{n+1}) onto the diagram (D_n) induced by sending $\mathscr{X}_1(p^{n+1})_{/S}$ to $\mathscr{X}(p^n)_{/S}$ in the following way: a pair $(E, \alpha_{n+1} : \boldsymbol{\mu}_{p^{n+1}} \hookrightarrow E)$ is sent to the pair $(E, \alpha_n : \boldsymbol{\mu}_{p^n} \hookrightarrow E)$ simply by setting α_n to be the restriction of α_{n+1} to $\boldsymbol{\mu}_{p^n} \subset \boldsymbol{\mu}_{p^{n+1}}$.

In this way the system of Igusa curves is seen to form a "tower"

$$\cdots \to \mathrm{Ig}(p^{n+1})_{/\mathbf{F}_p} \to \mathrm{Ig}(p^n)_{/\mathbf{F}_p} \to \cdots \to \mathrm{Ig}(p)_{/\mathbf{F}_p},$$

in the notation of [M-W 2].

§3. The smooth commutative group schemes

Set:

$$J_n := \mathrm{Pic}^0(X_1(p^n)_{\mathbf{Z}[\zeta]}),$$

which is a smooth commutative group scheme over $\mathbf{Z}[\zeta]$. Using Raynaud's theorem ([M-W 1] Chap. 2 §1 Prop. 1) and the structure of the scheme $X_1(p^n)_{\mathbf{Z}[\zeta]}$) one knows that J_n is the connected component of the Néron model of $J_1(p^n)_{/\mathbf{Q}}$ over the base $\mathbf{Z}[\zeta]$.

Set:

$A_n :=$ the Néron model of the abelian variety $A_{n/\mathbf{Q}}$ over the base $\mathbf{Z}[\zeta]$.

We know (cf. [M-W1] Chap. 3) that A_n is an abelian scheme. The surjection

$$J_{n/\mathbf{Q}} \overset{\alpha_n}{\to} A_{n/\mathbf{Q}}$$

extends to a canonical surjection of commutative group schemes over $\mathbf{Z}[\zeta]$, which we denote by the same letter,

$$J_n \overset{\alpha_n}{\to} A_n.$$

Set:

$$j_n := \text{the jacobian of } \mathrm{Ig}(p^n)_{/\mathbf{F}_p}.$$

There is a canonical surjection

$$J_{n/\mathbf{F}_p} \twoheadrightarrow \mathrm{av}(J_{n/\mathbf{F}_p})$$

to the "abelian variety part" of $J_{n/\mathbf{F}_p}$ (cf. [M-W 1] Chap. 2. §1), and we have that $\mathrm{av}(J_{n/\mathbf{F}_p})$ is the direct product of the jacobians of the irreducible components of the $\mathbf{F}_p$-scheme (2). Write:

$$\mathrm{av}\left(J_{n/\mathbf{F}_p}\right)=j_n\times\mathscr{B}\times j_n \tag{5}$$

where the "first" j_n is the jacobian of the good component $i_1\cdot\mathrm{Ig}(p^n)_{/\mathbf{F}_p}$, $\mathscr{B}$ is the product of the jacobians of the middle components, and the final j_n is the jacobian of the good component $i_2\cdot\mathrm{Ig}(p^n)_{/\mathbf{F}_p}$.

Define

$$\sigma_n: j_n\times j_n\to A_{n/\mathbf{F}_p}$$

as the composition of the imbedding $j_n\times j_n\hookrightarrow j_n\times\mathscr{B}\times j_n=\mathrm{av}(J_n/\mathbf{F}_p)$ [given by $(x,\ y)\mapsto(x,0,\ y)$] with the induced mapping

$$\mathrm{av}(\alpha_{n/\mathbf{F}_p}):\mathrm{av}\left(J_{n/\mathbf{F}_p}\right)\to A_{n/\mathbf{F}_p}. \tag{6}$$

Recall that since A_n is an abelian scheme over $\mathbf{Z}[\zeta]$ which is the Néron model over that base of the abelian variety $A_{n/\mathbf{Q}}$, there is a natural "geometric inertia group action" on the characteristic p fiber of A_n (cf. [S-T] and especially [Gr] exp. IX §4).

Note that the relevant inertia group is the one denoted I above, and the "geometric inertia group action" yields an action of the group I on both domain and range of (6), and moreover, the morphism (6) is I-equivariant. It is also immediate that the "geometric inertia group action" on $\mathrm{av}(J_{n/\mathbf{F}_p})$ is the one induced from the previously described action of I on $X_1(p^n)_{\mathbf{Z}[\zeta]}\otimes\mathbf{F}_p$.

PROPOSITION: *The morphism*

$$\sigma_n: j_n\times j_n\to A_{n/\mathbf{F}_p}$$

is an isogeny of abelian varieties. We have commutative diagrams:

$$\begin{array}{ccc} j_n\times j_n & \xrightarrow{\sigma_n} & A_{n/F_p}\\ \mathrm{F}\times\mathrm{V}\downarrow & & \downarrow U_p\\ j_n\times j_n & \xrightarrow{\sigma_n} & A_{n/F_p}\end{array}\qquad\qquad \begin{array}{ccc} j_n\times j_n & \xrightarrow{\sigma_n} & A_{n/F_p}\\ 1\times\langle a_g\rangle\downarrow & & \downarrow g\\ j_n\times j_n & \xrightarrow{\sigma_n} & A_{n/F_p}\end{array}$$

where F *is the Frobenius endomorphism*, V *the Verscheibung*, $g\in I$ *and its action on* A_n *is via the "geometric inertia group action".*

PROOF: That σ_n is an isogeny is the proposition on page 267 of [M-W 1]. The first commutative diagram comes from loc. cit., the Proposition 2 on page 271 (where the formulas have simplified a bit since our "auxiliary level" a is 1). The second commutative diagram comes from (4); a, b, c.

§4. The projector associated to U

Let $\mathscr{C}$ denote a $\mathbf{Z}_p$-additive category where morphisms have kernels. Let A denote any object of $\mathscr{C}$ such that End(A) is a $\mathbf{Z}_p$-module of finite type. Let $U: A \to A$ be an endomorphism of A. Then there is a unique direct product decomposition

$$A = A_U \times A_U^{nil}$$

such that U preserves this decomposition, and the endomorphism U on A_U is an isomorphism while the endomorphism U on A_U^{nil} is topologically nilpotent (e.g., as an element in the finite $\mathbf{Z}_p$-algebra End(A_U^{nil})). To see this, simply let R denote the $\mathbf{Z}_p$-subalgebra of End(A) generated by U. Then R is a commutative, finite $\mathbf{Z}_p$-algebra. Consequently, R is a finite product of local rings $R = \prod_{\mathfrak{m}} R_{\mathfrak{m}}$ where $\mathfrak{m}$ ranges through the (finitely many) maximal ideals of R.

Let $\epsilon_{\mathfrak{m}}: R \to R_{\mathfrak{m}}$ denote the projector to the $\mathfrak{m}$-th factor, and define the following "orthogonal commuting idempotent decomposition of the identity" in R:

$$\epsilon_U = \sum_{U \notin \mathfrak{m}} \epsilon_{\mathfrak{m}}; \quad \epsilon_U^{nil} = \sum_{U \in \mathfrak{m}} \epsilon_{\mathfrak{m}}.$$

Then $A_U = \epsilon_U \cdot A$ while $A_U^{nil} = \epsilon_U^{nil} \cdot A$. We will often apply this construction in the following situation.

Let $V_{/S}$ be an abelian scheme over a base S. Let $V_{p/S}$ denote the p-divisible group scheme over S associated to V. Let $U: V_{/S} \to V_{/S}$ be an endomorphism of abelian S-schemes. Then set

$$V_{U/S} := V_{p,U/S}.$$

We have that $V_{U/S}$ is a p-divisible group scheme over S and U operates on V_U as an isomorphism.

As an example, let us take $U = U_p$ acting on the abelian varieties of the proposition in §1. We have that the ϵ_U-projection of the finite complex in the proposition yields a complex of p-divisible groups over $\mathbf{Q}$, with finite homology:

$$0 \to J_0(p)_U^n \to J_1(p^n)_U \to A_{n,U} \to 0. \tag{7}$$

Applying our construction to the abelian scheme A_n over the base $S = \text{Spec}\,\mathbf{Q}$ or $S = \text{Spec}\,\mathbf{Z}[\zeta]$ with $U = U_p$ $(= U_{p*})$, we obtain a p-divisible group scheme $A_{n,U/\mathbf{Q}}$ which "prolongs" (in the sense of the word introduced in [M-W 1]) to a p-divisible group scheme $A_{n,U/\mathbf{Z}[\zeta]}$.

Denote, as usual, the characteristic p fiber of $A_{n,U/\mathbf{Z}[\zeta]}$ by $A_{n,U/\mathbf{F}_p}$.

PROPOSITION 1: *The isogeny σ_n induces an isogeny of p-divisible group schemes over $\mathbf{F}_p$:*

$$j_{n,p}^{\text{ét}} \times j_{n,p}^{\text{m.t.}} \to A_{n,U/\mathbf{F}_p}$$

where the superscript $^{\text{ét}}$ *and* $^{\text{m.t.}}$ *refer to the étale and multiplicative type parts of a p-divisible group scheme.*

PROOF: This comes directly from the Proposition in §3.

Let

$$\sigma_n^{\text{ét}} : j_{n,p}^{\text{ét}} \to A_{n,U/\mathbf{F}_p}^{\text{ét}}$$

denote the composition of σ_n with the injection $j_{n,p}^{\text{ét}} \hookrightarrow j_{n,p}^{\text{ét}} \times j_{n,p}^{\text{m.t.}}$ as "first coordinate".

PROPOSITION 2: *The morphism*

$$\sigma_n^{\text{ét}} : j_{n,p}^{\text{ét}} \to A_{n,U/\mathbf{F}_p}^{\text{ét}}$$

is an isogeny, and the "geometric inertia group action" of I on $A_{n/\mathbf{F}_p}$ induces the trivial action on $A_{n,U/\mathbf{F}_p}^{\text{ét}}$.

PROOF: The first assertion is immediate from Proposition 1, while the second comes from the first, together with the right-hand commutative diagram in the Proposition of §3.

Now choose compatible algebraic closures to obtain the following exact sequence of Galois groups:

$$\begin{array}{ccccccc} 1 \to & \mathscr{I}_{\mathbf{Q}_p} & \to & G_{\mathbf{Q}_p} & \to & G_{\mathbf{F}_p} & \to 1 \\ & \uparrow & & \uparrow & & \uparrow = & \\ 1 \to & \mathscr{I}_{\mathbf{Q}_p(\zeta)} & \to & G_{\mathbf{Q}_p(\zeta)} & \to & G_{\mathbf{F}_p} & \to 1 \end{array}$$

so that $\mathscr{I}_{\mathbf{Q}_p} = \mathscr{I}$ is the inertia group, and the Galois group denoted I in §2 may be identified with the quotient,

$$I = \mathscr{I}_{\mathbf{Q}_p} / \mathscr{I}_{\mathbf{Q}_p(\zeta)}.$$

We may view $A_{n,U}^{\text{ét}}(\overline{\mathbf{Q}}_p)$ as a $G_{\mathbf{Q}_p}$-module, and $j_{n,p}(\overline{\mathbf{F}}_p)$ as a $G_{\mathbf{F}_p}$-module. By virtue of the fact that we have chosen compatible algebraic closures, the mapping $\sigma_n^{\text{ét}}$ induces an isogeny

$$\sigma_n^{\text{ét}}: j_{n,p}(\overline{\mathbf{F}}_p) \to A_{n,U}^{\text{ét}}(\overline{\mathbf{Q}}_p) = A_{n,U}(\overline{\mathbf{Q}}_p)_{\mathscr{I}_{\mathbf{Q}_p(\zeta)}}$$

(when $A_{n,U}(\overline{\mathbf{Q}}_p)_{\mathscr{I}_{\mathbf{Q}_p(\zeta)}}$ denotes the group of coinvariants under $\mathscr{I}_{\mathbf{Q}_p(\zeta)}$ which is compatible with the natural actions of $G_{\mathbf{Q}_p(\zeta)}$ on domain and range – both actions factoring, of course, through actions of $G_{\mathbf{F}_p}$.

But by virtue of Proposition 2 (i.e., the "geometric inertia group action" on $A_{n,U/\mathbf{F}_p}^{\text{ét}}$ is trivial) we may identify $A_{n,U}^{\text{ét}}(\overline{\mathbf{Q}}_p)$ as the coinvariant elements under the action of the *full* inertia group $\mathscr{I}_{\mathbf{Q}_p}$. Thus:

COROLLARY: *The mapping $\sigma_n^{\text{ét}}$ is an isogeny of $G_{\mathbf{F}_p}$-modules,*

$$\sigma_n^{\text{ét}}: j_{n,p}(\overline{\mathbf{F}}_p) \to A_{n,U}(\overline{\mathbf{Q}}_p)_{\mathscr{I}_{\mathbf{Q}_p}}$$

§5. Λ'-modules

Let $\mathbf{Z}_p^* = \mathbf{F}_p^* \times \Gamma$ denotes the natural factorization, where Γ is the subgroup of p-adic units congruent to 1 modulo p. Let $\omega: \mathbf{F}_p^* \to \mathbf{Z}_p^*$ denote the Teichmüller homomorphism, i.e., the unique homomorphism whose composition with reduction mod p is the identity homomorphism of $\mathbf{F}_p^*$. Define:

$$\Lambda := \mathbf{Z}_p[[\mathbf{Z}_p^*]], \quad \Lambda_n := \mathbf{Z}_p[(\mathbf{Z}/p^n\mathbf{Z})^*],$$

$$\wedge := \mathbf{Z}_p[[\Gamma]], \quad \wedge_n := \mathbf{Z}_p[\Gamma/\Gamma_n],$$

where $\Gamma_n \subset \Gamma$ is the unique closed subgroup of index p^{n-1}, so that we have natural ring homomorphisms $\wedge \hookrightarrow \Lambda \twoheadrightarrow \Lambda_n$. For each j mod $p-1$ we have a $\wedge$-homomorphism

$$\Lambda \overset{\omega^j}{\twoheadrightarrow} \wedge$$

characterized by the property that $\mathbf{F}_p^* \hookrightarrow \mathbf{Z}_p^*$ maps to the scalar subring $\mathbf{Z}_p \subset \wedge$ via ω^j. We have an isomorphism of $\wedge$-algebras

$$\Lambda \underset{\substack{\Pi\omega^j \\ j \bmod p-1}}{\cong} \underbrace{\wedge \times \wedge \times \cdots \times \wedge}_{\leftarrow p-1 \rightarrow}.$$

Define:

$$\Lambda' :\cong \underbrace{\Lambda \times \Lambda \times \cdots \times \Lambda}_{\leftarrow p-2 \rightarrow} \quad \left(\text{resp. } \Lambda'_n \cong \underbrace{\Lambda_n \times \Lambda_n \times \cdots \times \Lambda_n}_{\leftarrow p-2 \rightarrow}\right)$$

viewed as quotient of the ring Λ (resp. Λ_n) via the mapping $\prod_{\substack{j \bmod p-1 \\ j \not\equiv 0(p-1)}} \omega^j$.

Given a Λ-module M, we shall denote by M' the Λ'-module

$$M' = M \otimes_\Lambda \Lambda'.$$

Thus, the superscript $'$ denotes "removing the trivial tame character".

For example, the diamond operators (cf. [M-W 1], Chap. 2, §5.1) give a natural action of $(\mathbf{Z}/p^n\mathbf{Z})^*$ on $X_1(p^n)$ and on the abelian varieties occurring in the proposition of §1. We may thus view the p-divisible groups occurring in (7) as Λ-modules. It is immediate that we have the following isomorphisms of Λ'-modules:

$$J_0(p)'_U = 0 \quad A'_{n,U} = A_{n,U}$$

and therefore the proposition of §1 yields

PROPOSITION: *The mapping $J_1(p^n) \to A_n$ induces an isogeny*

$$J_1(p^n)'_U \to A_{n,U}.$$

REMARK: To recapitulate what has been achieved at this point, on the level of $G_{\mathbf{Q}_p}$-modules, we have the following diagram of natural morphisms of $G_{\mathbf{Q}_p}$-modules, where the horizontal maps are isogenies:

$$\begin{array}{ccccc} J_1(p^n)'_U(\overline{\mathbf{Q}}_p) & \tilde{\rightarrow} & A_{n,U}(\overline{\mathbf{Q}}_p) & & \\ \downarrow & & \downarrow & & \\ J_1(p^n)'_U(\overline{\mathbf{Q}}_p)_{\mathscr{I}_{\mathbf{Q}_p}} & \tilde{\rightarrow} & A_{n,U}(\overline{\mathbf{Q}}_p)_{\mathscr{I}_{\mathbf{Q}_p}} & \tilde{\leftarrow} & j_{n,p}(\overline{\mathbf{F}}_p). \end{array}$$

Specifically, we have that the quotient of $J_1(p^n)'_U(\overline{\mathbf{Q}}_p)$ consisting of the group of coinvariants under inertia ($\mathscr{I}_{\mathbf{Q}_p}$) is isogenous to $j_{n,p}(\overline{\mathbf{F}}_p)$.

§6. Duality

Let $\mathscr{T}a_p(M) = \mathrm{Hom}(M, \mathbf{Q}_p/\mathbf{Z}_p)$ denote the *contravariant* Tate module of a p-torsion group of finite corank, M. If R is a ring of operators on

M, $\mathcal{T}a_p(M)$ inherits a natural R-action by the formula $rf(m)=f(rm)$ for $r\in R$, $m\in M$, $f\in\mathcal{T}a_p(M)$.

The Weil pairing for the jacobian of $X_1(p^n)$ induces a nondegenerate bilinear skew-symmetric pairing

$$\mathcal{T}a_p(J_1(p^n)(\overline{\mathbf{Q}}))\times\mathcal{T}a_p(J_1(p^n)(\overline{\mathbf{Q}}))\to\mathbf{Z}_p(-1)$$
$$(x,y)\mapsto\langle x,y\rangle$$

where $\mathbf{Z}_p(-1)=\mathcal{T}a_p(\mu_{p^\infty}(\overline{\mathbf{Q}}))$.

If r is any Hecke operator T_l $(l\neq p)$ or any diamond operator $\langle a\rangle$ for $a\in\mathbf{Z}_p^*$, or U_p, and if r_* and r^* are the endomorphisms induced by direct and inverse images, respectively, then we have the adjoint law:

$$\langle x,\ r_*y\rangle=\langle r^*x,\ y\rangle.$$

Moreover, the Weil pairing commutes with the action of $G_{\mathbf{Q}}$ in the sense that $g\langle x,\ y\rangle=\langle gx,\ gy\rangle$ for $g\in G_{\mathbf{Q}}$.

Let W_n denote the direct factor of $\mathcal{T}a_p(J_1(p^n)(\overline{\mathbf{Q}}))$ defined by:

$$W_n:=\mathcal{T}a_p(J_1(p^n)'_U(\overline{\mathbf{Q}})).$$

Define a pairing, (the "*twisted Weil pairing*")

$$W_n\times W_n\to\mathbf{Z}_p(-1)$$
$$(x,y)\mapsto[x,y]$$

by the rule

$$[x,\ y]:=\langle x,\ w_\zeta y\rangle.$$

The twisted Weil pairing is bilinear and nondegenerate. It commutes with the action of $G_{\mathbf{Q}(\zeta)^+}$, and satisfies the agreeable law:

$$[x,\ r_*y]=[r_*x,\ y],$$

for r as above, and $x,\ y\in W_n$.

As for the action of $G_{\mathbf{Q}}$, one computes:

$$\left[gx,\ \langle a_g\rangle^{-1}\cdot gy\right]=a_g^{-1}\cdot[x,\ y] \tag{8}$$

for $g\in G_{\mathbf{Q}}$, and $x,\ y\in W$, where a_g is as in §2.

PROPOSITION: *The subspace $W_n^{\mathcal{I}}$ of invariant elements under the action of inertia ($\mathcal{I}=\mathcal{I}_{\mathbf{Q}_p}$) is isotropic for the twisted Weil pairing. The induced pairing*

$$W_n^{\mathcal{I}}\times W_n/W_n^{\mathcal{I}}\to\mathbf{Z}_p(-1)$$

is nondegenerate.

PROOF: The first assertion is evident, since the twisted Weil pairing commutes with the action of $G_{\mathbf{Q}(\zeta)^+}$. The second assertion follows from the fact that the $\mathscr{I}_{\mathbf{Q}_p}$-invariants in W_n are equal to the $\mathscr{I}_{\mathbf{Q}_p(\zeta)^+}$ invariants (as follows from Proposition 2 of §4) and W_n is the (contravariant) Tate module of a p-divisible group over $\mathbf{Q}_p(\zeta)$ which prolongs to an *ordinary* p-divisible group scheme over $\mathbf{Z}_p[\zeta]$.

Set

$$M_n := \mathscr{T}a_p\big(j_{n,p}(\overline{\mathbf{F}}_p)\big).$$

A corollary of the remark at the end of §5 is the following equalities of ranks:

$$\operatorname{rank}_{\mathbf{Z}_p}(M_n) = \operatorname{rank}_{\mathbf{Z}_p}\big(W_n^{\mathscr{I}}\big) = \tfrac{1}{2}\cdot \operatorname{rank}_{\mathbf{Z}_p}(W_n).$$

REMARK: One has the analogous equalities of the ranks of the ω^j-parts of the Λ'-modules involved, for each j mod $p-1$.

§7. Hecke modules

Let

$$\mathscr{H} = \Lambda'\big[U_p,\dots, T_l,\ \dots (l \neq p)\big]$$

denote the polynomial algebra over Λ' in the infinitely many commuting variables U_p and T_l for $l \neq p$. We view $J_1(p^n)'_{U/\mathbf{Q}}$ as $\mathscr{H}$-module (where the Λ'-action is the natural one, and U_p and T_l act as the Atkin and Hecke operators U_{p*} and T_{l*} respectively.

The contravariant Tate module W_n inherits an $\mathscr{H}$-module structure. We have the Hermitian property of the twisted Weil pairing:

$$[x,\ h\cdot y] = [h\cdot x,\ y]$$

for $h \in \mathscr{H}$.

We may endow $j_{n,p}(\tilde{\mathbf{F}}_p)$ and hence also M_n with an $\mathscr{H}$-module structure by letting T_l act as the Hecke operator T_{l*} and U_p act as *Frobenius*.

There is a canonical $\mathscr{H}\otimes\mathbf{Q}$-isomorphism

$$M_n \otimes \mathbf{Q} \xrightarrow{\sim} W_n^{\mathscr{I}} \otimes \mathbf{Q},$$

coming from the end of §5.

LEMMA: *The annihilator ideal in $\mathscr{H}$ of M_n is equal to the annihilator ideal of W_n.*

PROOF: Let $r \in \mathscr{H}$ be such that $r \cdot m = 0$ for all $m \in M_n$. Then multiplication by r induces a homomorphism from $W_n/W_n^{\mathscr{I}}$ into W_n, and hence by projection, into $W_n/W_n^{\mathscr{I}}$. By virtue of the duality expressed in the previous proposition, this homomorphism

$$W_n/W_n^{\mathscr{I}} \to W_n/W_n^{\mathscr{I}}$$

is dual (via the twisted Weil pairing) to multiplication by r in $W_n^{\mathscr{I}}$, and hence zero by assumption. Consequently, multiplication by r induces a homomorphism from $W_n/W_n^{\mathscr{I}}$ into $W_n^{\mathscr{I}}$. Since this homomorphism must also be compatible with the action of $\mathscr{I}$, it is zero.

DEFINITION: *By the Hecke algebra (at "level n") $\mathbf{T}_n$ we shall mean the quotient of $\mathscr{H}$ by the common annihilator ideal of M_n and W_n.*

The Hecke algebra acts faithfully, then, on $j^{\text{ét}}_{n,p/\mathbf{F}_p}$, on $J_1(p^n)'_{U/\mathbf{Q}}$, on M_n and on W_n.

§8. Passage to the limit

If B_{n+1}, B_n are Λ_{n+1}- and Λ_n-modules respectively, say that $f: B_{n+1} \to B_n$ is a *perfect surjection* if it is a Λ_{n+1}-homomorphism of the Λ_{n+1}-module B_{n+1} onto B_n given its induced Λ_{n+1}-module structure, and the natural mapping

$$B_{n+1} \otimes_{\Lambda_{n+1}} \Lambda_n \to B_n$$

is an isomorphism of Λ_n-modules.

The natural projection of diagram (D_{n+1}) to (D_n) discussed at the end of §2 induces $\mathscr{H}$-module homomorphisms,

$$M_{n+1} \to M_n; \quad W_{n+1} \to W_n; \quad W_{n+1}^{\mathscr{I}} \to W_n^{\mathscr{I}};$$

$$W_{n+1}/W_{n+1}^{\mathscr{I}} \to W_n/W_n^{\mathscr{I}}. \tag{9}$$

PROPOSITION 1: *There is an integer r (independent of n) such that M_n, $W_n^{\mathscr{I}}$, and $W_n/W_n^{\mathscr{I}}$ are free Λ_n-modules of* rank r. *The Λ_n-module W_n is free of* rank $2r$. *All the morphisms of* (9) *are perfect surjections. The $\mathbf{T}_n$-module M_n is free of* rank 1.
The $\mathscr{H}$-module homomorphism $\mathbf{T}_{n+1} \to \mathbf{T}_n$ is a perfect surjection. The $\mathbf{T}_n$-module $W_n^{\mathscr{I}}$ is free of rank 1. The $\mathbf{T}_n$-module $W_n/W_n^{\mathscr{I}}$ is the dualizing module for $\mathbf{T}_n$, (hence faithful).

PROOF: The statements about M_n follow essentially immediately from the propositions proven in [M-W 2]. We say "essentially immediately" because, in that paper, we completed M_n to the part on which U_p acted with eigenvalue a p-adic "1-unit". But all the proofs go over unchanged to the full M_n.

Since $M_{n+1} \to M_n$ is a perfect surjection, and M_n is free (of rank 1) over $\mathbf{T}_n$, it follows that $\mathbf{T}_{n+1} \to \mathbf{T}_n$ is a perfect surjection.

Now consider the diagram

$$\begin{array}{ccccccc} 0 \to W_{n+1}^{\mathscr{I}} \otimes_{\Lambda_{n+1}} \Lambda_n & \to & W_{n+1} \otimes_{\Lambda_{n+1}} \Lambda_n & \to & W_{n+1}/W_{n+1}^{\mathscr{I}} \otimes_{\Lambda_{n+1}} \Lambda_n \to 0 \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ 0 \to W_n^{\mathscr{I}} & \longrightarrow & W_n & \longrightarrow & W_n/W_n^{\mathscr{I}} \to 0. \end{array}$$

In [Hi2], Hida shows that W_n is free of some rank, say r' (independent of n) over Λ_n and that β is an isomorphism. But the snake-lemma mapping $\delta: \ker(\gamma) \to \operatorname{cok}(\alpha)$ is compatible with the action of $\mathscr{I}_{\mathbf{Q}(\zeta_{p^{n+1}})^+}$ and consequently $\delta = 0$ because $\mathscr{I}_{\mathbf{Q}(\zeta_{p^{n+1}})^+}$ acts trivially on $\operatorname{cok}(\alpha)$ and "like $\mathbf{Z}_p(-1)$" on $\ker(\gamma)$. Consequently both α and γ are isomorphisms.

From the fact that M_n is isogenous to $W_n^{\mathscr{I}}$ and $W_n^{\mathscr{I}}$ is in duality with $W_n/W_n^{\mathscr{I}}$ we can now compute the $\mathbf{Z}_p$-ranks of all the modules involved, in terms of the quantity r, i.e.,

$$r \cdot p^n = \operatorname{rank}_{\mathbf{Z}_p} M_n = \operatorname{rank}_{\mathbf{Z}_p} W_n^{\mathscr{I}} = \operatorname{rank}_{\mathbf{Z}_p} W_n/W_n^{\mathscr{I}}.$$

and (consequently) $r' = 2r$.

From the fact that α and β are isomorphisms, we have natural isomorphisms

$$W_n^{\mathscr{I}} \otimes_{\Lambda_n} \mathbf{Z}_p \xrightarrow{\cong} W_1^{\mathscr{I}} \quad \text{and} \quad \left(W_n/W_n^{\mathscr{I}}\right) \otimes_{\Lambda_n} \mathbf{Z}_p \xrightarrow{\cong} \left(W_1/W_1^{\mathscr{I}}\right),$$

the $\mathbf{Z}_p$-ranks of these modules being all equal to r.

Choose Λ_n-homomorphisms $\Lambda_n^r \to W_n^{\mathscr{I}}$, $\Lambda_n^r \to W_n/W_n^{\mathscr{I}}$ projecting surjectively to the modules in (9). These Λ_n-homomorphisms are surjections, then, by Nakayama's lemma, and injections as well by counting $\mathbf{Z}_p$-ranks. Hence both $W_n^{\mathscr{I}}$ and $W_n/W_n^{\mathscr{I}}$ are Λ_n-free of rank r.

It remains to show that $W_n^{\mathscr{I}}$ is $\mathbf{T}_n$-free of rank 1. All assertions of the proposition will then have been proved, since $W_n/W_n^{\mathscr{I}}$ isomorphic as $\mathbf{T}_n$-module to the $\mathbf{Z}_p$-dual of $W_n^{\mathscr{I}}$.

We first show that $W_n^{\mathscr{I}}$ is $\mathbf{T}_n$-free (of rank 1) when $n = 1$. For this, we return to an analysis of $\alpha_n: J_n \to A_n$ when $n = 1$. Note that α_1 identifies $J_1(p)/J_0(p)$ with A_1 and hence

$$J_1(p)'_p = A_{1,p}.$$

Moreover, by [M-W 1] Chap. 2 Prop. 4, the natural isogeny,

$$\sigma_1 : j_{1,p} \times j_{1,p} \to A_{1,p/\mathbf{F}_p}$$

is an isomorphism.

It follows that we may identify M_1 and $W_1^{\mathscr{I}}$ as $\mathbf{T}_1$-modules. Consequently $W_1^{\mathscr{I}}$ is $\mathbf{T}_1$-free of rank 1. Since $\mathbf{T}_n \to \mathbf{T}_1$ is a perfect surjection, its kernel is contained in its radical. We may then take any $w \in W_n^{\mathscr{I}}$ whose projection of $W_1^{\mathscr{I}}$ is a $\mathbf{T}_1$-generator, and Nakayama's lemma gives us that w is a $\mathbf{T}_n$-generator of $W_n^{\mathscr{I}}$. Since both $\mathbf{T}_n$ and $W_n^{\mathscr{I}}$ are $\mathbf{Z}_p$-free of the same rank, w is a free $\mathbf{T}_n$-generator of $W_n^{\mathscr{I}}$. q.e.d.

REMARK: Our argument gives the further fact that the exact sequence of $\mathbf{T}_n[G_{\mathbf{Q}_p}]$-modules

$$0 \to W_n^{\mathscr{I}} \to W_n \to W_n/W_n^{\mathscr{I}} \to 0$$

splits (noncanonically) as an exact sequence of $\mathbf{T}_n$-modules.

PROOF: Let $\tau \in \mathscr{I}_{\mathbf{Q}_p(\zeta_{p^n})^+}$ be an element inducing the nontrivial involution of $\mathbf{Q}_p(\zeta_{p^n})$. Then τ acts as the identity on $W_n^{\mathscr{I}}$ and induces, by passage to the quotient, the scalar homomorphism, multiplication by -1 on $W_n/W_n^{\mathscr{I}}$. Since $p \neq 2$, $(\tau - 1)W_n$ is a lifting of $W_n/W_n^{\mathscr{I}}$ to W_n, and gives us a $\mathbf{T}_n$-splitting of the above exact sequence.

Note that since M_n is Λ_n-free of rank r, so is $\mathbf{T}_n$.

Now set:

$$\mathbf{T} = \varprojlim_n \mathbf{T}_n; \quad M = \varprojlim_n M_n; \quad W = \varprojlim_n W_n,$$

where the limits are compiled with respect to the natural maps of $\mathbf{T}_{n+1}$ to $\mathbf{T}_n$, etc.

The Λ'-algebra $\mathbf{T}$ we shall call the *Hecke algebra*. Both M and W are faithful $\mathbf{T}$-modules since M_n, W_n are faithful over $\mathbf{T}_n$ for each n.

PROPOSITION 2: *The* $\mathbf{T}$*-module* M *is free of rank* 1. *The* Λ*-modules* M *and* W *are free of ranks* r *and* $2r$ *respectively. The* Λ*-algebra* $\mathbf{T}$ *is finite and flat of rank* r. *The ring* $\mathbf{T}$ *is semi-local, complete, noetherian, Cohen-Macaulay of dimension two. We have the exact sequence of* $\mathbf{T}[G_{\mathbf{Q}_p}]$*-modules,*

$$0 \to W^{\mathscr{I}} \to W \to W/W^{\mathscr{I}} \to 0 \tag{10}$$

where $W^{\mathscr{I}}$, *the invariants under inertia, is free of rank* 1 *over* $\mathbf{T}$. *Its cokernel,* $W/W^{\mathscr{I}}$ *is a free* Λ*-module of rank* r, *isomorphic as* $\mathbf{T}$*-module to* *the dualizing module of* $\mathbf{T}$. *The above exact sequence splits (noncanonically) as an exact sequence of* $\mathbf{T}$*-modules. The natural projections to finite layers compile to produce isomorphisms,*

$$W^{\mathscr{I}} \cong \varprojlim_n W_n^{\mathscr{I}} \quad \text{and} \quad W/W^{\mathscr{I}} \cong \varprojlim_n W_n/W_n^{\mathscr{I}}.$$

Formation of inertial invariants commutes with "arbitrary" change of rings, in the sense that if $\mathbf{T} \to R$ *is a nontrivial homomorphism to a ring* R, *then the natural homomorphisms*

$$W^{\mathscr{I}} \otimes R \to (W \otimes R)^{\mathscr{I}} \quad \text{and} \quad W/W^{\mathscr{I}} \otimes R \to (W \otimes R)/(W \otimes R)^{\mathscr{I}}$$

are isomorphisms.

PROOF: The first two sentences follow directly from the previous proposition. The third sentence follows from the first two. The structure of the ring $\mathbf{T}$ comes from the fact that it is finite and flat over Λ which is a complete local regular noetherian ring of dimension 2.

There is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & W^{\mathscr{I}} & \to & W & \to & W/W^{\mathscr{I}} & \to & 0 \\ & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & & \\ 0 & \to & \varprojlim W_n^{\mathscr{I}} & \to & \varprojlim W_n & \underset{\pi}{\to} & \varprojlim W_n/W_n^{\mathscr{I}} & \to & 0 \end{array}$$

where the horizontal lines are exact (surjectivity of the map labeled γ is established by the standard compactness argument).

It has already been shown that β is an isomorphism. Therefore α is an isomorphism (kernels commute with inverse limits) and consequently so is γ.

The fact that $W^{\mathscr{I}}$ is free of rank 1 over $\mathbf{T}$ follows from the previous proposition together with the fact that α above is an isomorphism. Similarly, that $W/W^{\mathscr{I}}$ is free of rank r over Λ comes from the previous proposition together with the fact that γ above is an isomorphism. That $W/W^{\mathscr{I}}$ is the dualizing module for $\mathbf{T}$ comes from nondegeneracy of the twisted Weil pairings, and the lemma below concerning the dualizing modules of Cohen Macaulay rings. To see the noncanonical splitting of the exact sequence (10), we repeat the argument already given at finite levels. Namely, take an element $\tau \in \mathscr{I}_{\mathbf{Q}_p(\zeta_{p^\infty})^+}$ which induces the nontrivial involution of $\mathbf{Q}_p(\zeta_{p^\infty})$. Then, using the twisted Weil pairing dualities at finite level, one sees that τ induces the identity mapping on $W^{\mathscr{I}}$ and multiplication by -1 on $W/W^{\mathscr{I}}$. Again $(\tau - 1)W$ yields a lifting of $W/W^{\mathscr{I}}$. The final fact concerning formation of inertial invariants under nontrivial base change can be seen using the properties of this element τ.

Namely, since $p \neq 2$, for any nontrivial ring R admitting a homomorphism from $\mathbf{T}, +1$ differs from -1.

Remarks concerning dualizing modules

The following lemma was explained to us by David Eisenbud.

LEMMA: *Let Λ be a complete, noetherian regular local ring. Let R be a finite flat Λ-algebra. Let $\gamma \in \Lambda$ be a nonzero divisor contained in the maximal ideal of Λ. Then if W is an R-module which is finite and flat over Λ, these are equivalent*:

(&) *W is the dualizing module for R*

(2) *$W/\gamma W$ is the dualizing module for $R/\gamma R$.*

PROOF: A general reference for dualizing modules is [Har]. If $\Omega = \mathrm{Hom}(R, \Lambda)$ is the dualizing module for R, then $\Omega/\gamma\Omega = \mathrm{Hom}_{\Lambda/\gamma\Lambda}(R/\gamma R, \Lambda/\gamma\Lambda)$ is the dualizing module for $R/\gamma R$ (since $\Lambda/\gamma\Lambda$ is Gorenstein, and R is free of finite rank as Λ-module). Hence (1) $\Rightarrow$ (2).

To see that (2) $\Rightarrow$ (1), let W be as in the statement of the proposition, and let Ω be the dualizing module for R. Let $\phi: W/\gamma W \to \Omega/\gamma\Omega$ be an $R/\gamma R$-isomorphism.

Local duality ([Har] Ch. V) enables us to identify $\mathrm{Ext}^1_R(W, \Omega)$ with $H^{d-1}_{\mathrm{local}}(W)$ where $d = \mathrm{depth}(R)$ and where H_{local} refers to local cohomology supported at the closed point of Spec R. But since W is Cohen-Macaulay, $H^{d-1}_{\mathrm{local}}(W)$ vanishes, and hence so does $\mathrm{Ext}^1_R(W, \Omega)$.

It follows that the obstruction to lifting ϕ to an R-homomorphism $\Phi: W \to \Omega$, which lies in $\mathrm{Ext}^1_R(W, \Omega)$, vanishes, i.e. such a Φ exists. By Nakayama's lemma, Φ is an isomorphism, establishing the lemma.

Remarks concerning the Hecke algebra

The fact that $\mathbf{T}$ acts faithfully on M shows that $\mathbf{T}$ is the Hecke algebra attached to the "Igusa Tower" (See [M-W 2], with the reminder that the difference between the algebra defined there and here is that there we considered only the part where the "eigenvalues of U_p are 1-units"). The fact that $\mathbf{T}$ acts faithfully on W shows that $\mathbf{T}$ is *also* the Hecke algebra as appears in Hida's theory (see [Hi1,2] with the reminder that we have only considered the case of "tame level" $N_0 = p$ and we have localized away from the trivial character). Hida has shown the following other equivalent descriptions of $\mathbf{T}$.

If $\mathscr{C}$ is a collection of $\mathscr{H}$-modules, say that a quotient algebra of $\mathscr{H}$ is *cut out* by $\mathscr{C}$ if it is the quotient by the intersection of the annihilator ideals of all elements of $\mathscr{C}$. Equivalently, it is the smallest quotient algebra of $\mathscr{H}$ acting naturally on all the modules in $\mathscr{C}$.

PROPOSITION 3 (Hida): *The Hecke algebra* $\mathbf{T}$ *is the quotient algebra of* $\mathcal{H}$ *cut out by any one of the following collections* $\mathcal{C}$ *described below*:

$$\mathcal{C} = (a), \quad (b_k) \quad \text{for } k = 2, 3, 4, \ldots,$$

$$(c_\kappa) \quad \text{for } \kappa \in \mathbb{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}_p \text{ with 1-st coordinate different from 2 mod } p$$

where:

$$(a) = \{ J_1(p^n)'_U(\overline{\mathbf{Q}});\ \textit{for all } n \},$$

$$(b_k) = \left\{ \begin{array}{l} \textit{the spaces of classical } (\mathbf{C}_p\textit{-valued}) \textit{ p-ordinary modular} \\ \textit{forms on } \Gamma_1(p^n) \textit{ of weight } k \in \mathbf{N}, \textit{ whose nebentyus} \\ \textit{character is different from } \omega^{k-2};\ \textit{for all } n \end{array} \right\},$$

$$(c_\kappa) = \left\{ \begin{array}{l} \textit{the space of p-adic (in the sense of Katz [Ka])} \\ \mathbf{C}_p\textit{-valued} \\ \textit{p-ordinary modular forms } (N_0 = 1) \textit{ of weight } \kappa \in \\ \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}_p \textit{ (such that the projection of } \kappa \textit{ to} \\ \mathbf{Z}/(p-1)\mathbf{Z} \textit{ differs from 2 mod } p-1) \end{array} \right\}.$$

NOTE: Hida also shows that $\mathbf{T}$ can be cut out by appropriate (p-ordinary) parts of parabolic cohomology of weights $k \geqslant 2$.

Remarks on the action of the decomposition group

Since $W^{\mathcal{I}}$ is free of rank one over $\mathbf{T}$, and the decomposition group $G_{\mathbf{Q}_p}$ leaves $W^{\mathcal{I}}$ stable and commutes with the action of $\mathbf{T}$, the action of $G_{\mathbf{Q}_p}$ on $W^{\mathcal{I}}$ is given by a $\mathbf{T}$-valued character on $G_{\mathbf{Q}_p}$

$$\eta : G_{\mathbf{Q}_p} \twoheadrightarrow G_{\mathbf{Q}_p}/\mathcal{I}_{\mathbf{Q}_p} \simeq \hat{\mathbf{Z}} \to \mathbf{T}$$
$$1 \mapsto U_p$$

That it is the character determined by the property that $1 \in \hat{\mathbf{Z}}$ is sent to $U_p \in \mathbf{T}$ follows easily from the proposition of §3.

Using formula (8) we can also calculate the action of $G_{\mathbf{Q}_p}$ on $W/W^{\mathcal{I}}$. Namely:

$$g \cdot w = \eta^{-1}(g) \cdot a_g^{-1} \langle a_g \rangle w \tag{11}$$

for $w \in W/W^{\mathcal{I}}$ and $g \in G_{\mathbf{Q}_p}$.

§9. p-adic Hodge structure

We rely on [Ta] and [Sen] for the basic theory used in this section. Let $\mathbf{C}_p$ denote the completion of $\overline{\mathbf{Q}}_p$. Fix $K \subset \overline{\mathbf{Q}}_p$ a finite field extension of $\mathbf{Q}_p$ and consider the natural continuous action of G_K on $\mathbf{C}_p$. A *semi-linear G_K-representation* will mean a finite dimensional $\mathbf{C}_p$-vector space V with a continuous G_K-action satisfying the law $g(c \cdot v) = g(c) \cdot g(v)$ for $g \in G_K$, $C \in \mathbf{C}_p$, $v \in V$.

By $\mathbf{C}_p(-1)$ we mean $\mathcal{T}a_p(\mu_{p^\infty}) \otimes_{\mathbf{Z}_p} \mathbf{C}_p$ viewed as semi-linear vector space with the diagonal action of G_K. For any p-adic integer k we can define $\mathbf{C}_p(K)$ (the "k-twisted" $\mathbf{C}_p$) such that $\mathbf{C}_p(k_1) \otimes_{\mathbf{C}_p} \mathbf{C}_p(k_2)$ is canonically isomorphic to $\mathbf{C}_p(k_1 + k_2)$.

If a semi-linear G_K-representation V of dimension n has a filtration by semi-linear subspaces whose successive quotients are 1-dimensional and isomorphic to $\mathbf{C}_p(k_i)$ for p-adic integers $k_1, k_2, \ldots, k_n$, then we shall say that the (unordered) set $(k_1, k_2, \ldots, k_n)$, counted with multiplicities, is the set of *twists* of V. If V is isomorphic, as semi-linear G_K-representation, to $\mathbf{C}_p(k_1) \oplus \mathbf{C}_p(k_2) \oplus \ldots \oplus \mathbf{C}_p(k_n)$, then we shall say that V is *semi-simple, with set of twists* $(k_1, \ldots, k_n)$.

The "status" of a semi-linear G_K-representation vis a vis semi-simplicity, and its set of twists is insensitive to finite base change in the sense that, firstly, it is independent of the filtration: given two filtrations, as above, of the same semi-linear G_k-representation, the set of twists computed from each are equal. Secondly, if $K' \subset \overline{\mathbf{Q}}_p$ is a finite field extension of K, and V a semi-linear G_K-representation, Let V' denote the semi-linear $G_{K'}$-representation obtained by restriction to $G_{K'}$. Then V has a set of twists if and only if V' does, and the set of twists are equal; V is semi-simple if and only if V' is.

A theorem of Tate [Ta] guarrantees that if V is a G_K-representation with twists $(k_1, k_2, \ldots, k_n)$ with the k_i's all distinct, then V is semi-simple.

Now let W be an R-module of finite type, where R is a complete noetherian ring. Suppose that a G_K-action is given on W, i.e., by a continuous homomorphism $G_K \to \mathrm{Aut}_R(W)$. Suppose also that we are given a continuous homomorphism

$$\lambda : R \to \overline{\mathbf{Q}}_p$$

such that the image of λ lies in a finite field extension of $\mathbf{Q}_p$.

Define

$$W_\lambda = W \otimes_R \mathbf{C}_p$$

where $\mathbf{C}_p$ is viewed as R-algebra via λ. If K contains the image of λ, then we may view W_λ as semi-linear G_K-representation, by letting G_K act in the natural "diagonal" way on W_λ. In general, we replace K by a finite field extension, if necessary, so that K does contain image (λ), and give W_λ this diagonal semi-linear G_K-action.

If W_λ has a set of twists $(k_1, \ldots, k_n)$ we shall refer to them as the *λ-adic (Hodge) twists* of W. If W_λ is semi-simple, we shall say that W has *semi-simple λ-adic Hodge structure.*

By a theorem of Sen one knows that the following statements are equivalent, for the G_K-module W, in the case where R is a field:

(a) *The inertia group $\mathscr{I}_K$ acts on W through a finite quotient.*

(b) *The λ-adic Hodge structure of W is semi-simple, with twists* $(0, 0, \ldots, 0)$.

We now apply this theory to the case of $R = \mathbf{T}$, the Hecke Algebra, and W the $\mathbf{T}[G_{\mathbf{Q}}]$-module of §8.

For $k \in \mathbf{Z}_p$, let $\chi_k : \Lambda \to \mathbf{Z}_p$ denote the continuous homomorphism which sends $[x] \in \Gamma \subset \Lambda^*$ to $x^{k-1} \in \mathbf{Z}_p$ for x a 1-unit.

A continuous homomorphism

$$\lambda : \mathbf{T} \to \overline{\mathbf{Q}}_p$$

is said to be of *weight* $k \in \mathbf{Z}_p$ if the restriction of λ to Λ is equal to χ_k. Note that any continuous homomorphism λ as above has the property that its image is contained in a finite extension of $\mathbf{Q}_p$.

Set $d_\lambda = \dim_{\mathbf{C}_p}(W_\lambda)$. By Proposition 2 of §8 we see that $d_\lambda \geqslant 2$.

PROPOSITION: *If λ is of weight $k \in \mathbf{Z}_p$. then the set of twists of W_λ is $(0, k-1, k-1, \ldots k-1)$, where the twist $k-1$ occurs with multiplicity $d_\lambda - 1$. If $k \neq 1$, then W has semi-simple λ-adic Hodge structure.*

PROOF: This follows from Proposition 2 of §8 and formula (11).

REMARK: We have no example of a λ with d_λ different from 2. Prop. 2 below guarantees that $d_\lambda = 2$ except possibly if the attached residual representation is reducible.

Let $F \subset \overline{\mathbf{Q}}_p$ be a finite extension of $\mathbf{Q}_p$ containing the image of λ. From the theorem of Sen quoted above, and from the previous proposition, we have that the action of $I_{\mathbf{Q}_p}$ on $W \otimes_{\mathbf{T}} F$ (where F is given a $\mathbf{T}$-algebra structure via λ) factors through a finite quotient if and only if

(a) $k = 1$ and

(b) the λ-adic Hodge structure of W is semi-simple.

We are thankful to Hida for the proof of the following proposition:

PROPOSITION 1: *Given any prime ideal $P \subset \mathbf{T}$ a residual representation attached to P exists, and is unique (up to F-equivalence).*

PROOF: Uniqueness is clear by the theorem of Brauer-Nesbitt [C-R] 30.16. We concentrate on existence below.

Step 1: Minimal ideals

Use Hida's ([Hi2] Cor. 1.3) together with Proposition 2 of §8 to see that $W \otimes_{\mathbf{T}} F$ is a residual representation attached to P, where P is any minimal prime ideal and F is the field of fraction of $\mathbf{T}/P$.

Step 2: Prime ideals P which are neither minimal nor maximal

Let $\mathscr{T}$ denote the total quotient ring of $\mathbf{T}$, which is semi-simple by [Hi1] Cor. 3.3. Let $\mathscr{L}$ denote the quotient field of Λ. Then $\mathscr{T} = \mathbf{T} \otimes \mathscr{L}$ is a finite-dimensional (semi-simple) $\mathscr{L}$-algebra. Put $\mathscr{W} = W \otimes_{\mathbf{T}} \mathscr{T} = W \otimes_{\Lambda} \mathscr{L}$. Then $\mathscr{W}$ is free of rank 2 over $\mathscr{T}$ ([Hi 2], lemma 8.1). Let $\tilde{\mathbf{T}}$ be the integral closure of Λ in $\mathscr{T}$ and let Ω be the image of $W \otimes_{\mathbf{T}} \tilde{\mathbf{T}}$ in $\mathscr{W}$. By definition, Ω contains W, and is finitely generated over $\tilde{\mathbf{T}}$. Hence Ω is a $\tilde{\mathbf{T}}$-lattice, and is, by construction, stable under the action of Galois. Let P be any prime ideal in $\mathbf{T}$, which is neither minimal nor maximal. By the lying-over theorem, there exists a prime ideal $\tilde{P}$ in $\tilde{\mathbf{T}}$ which is again neither minimal nor maximal, and such that $\tilde{P} \cap \mathbf{T} = P$. Since $\tilde{\mathbf{T}}$ is a sum of Krull domains of dimension 2, the completion $\tilde{\mathbf{T}}_{\tilde{P}}$ at $\tilde{P}$ is a discrete valuation ring. Thus $\Omega_{\tilde{P}} = \Omega \otimes_{\tilde{\mathbf{T}}} \tilde{\mathbf{T}}_{\tilde{P}}$ is free of rank two over $\tilde{\mathbf{T}}_{\tilde{P}}$.

Put $F = \mathbf{T}/P \cdot \mathbf{T}$ and $\tilde{F} = \tilde{\mathbf{T}}_{\tilde{P}}/\tilde{P} \cdot \tilde{T}_{\tilde{P}}$. Then $\tilde{F}$ is a finite extension of F, and $\Omega_{\tilde{P}}/\tilde{P} \cdot \Omega_{\tilde{P}}$ is a vector space of dimension 2 over $\tilde{F}$. Consequently, the action of $G_{\mathbf{Q}}$ on $\Omega_{\tilde{P}}/\tilde{P} \cdot \Omega_{\tilde{P}}$ gives a representation $\pi : G_{\mathbf{Q}} \to GL_2(\tilde{F})$. The characteristic polynomial for Frobenius ϕ_l at $l \neq p$ for the Galois representation on $\Omega_{\tilde{P}}$ (into $GL_2(\tilde{\mathbf{T}}_{\tilde{P}})$) is given by $1 - t(l)X + [l]X^2 \in \mathbf{T}[X] \subset \tilde{\mathbf{T}}_{\tilde{P}}[X]$, where $t(l)$ and $[l]$ are the images of T_l and $l \in \mathbf{Z}_p^*$ in $\mathbf{T} \subset \tilde{\mathbf{T}}_{\tilde{P}}$. Therefore the characteristic polynomial of $\pi(\phi_l)$ is the image in $\tilde{F}[X]$ of the above characteristic polynomial under the natural homomorphism $\mathbf{T} \to F \subset \tilde{F}$. By the Cebotarev density theorem, the characteristic polynomial of $\pi(g)$ lies in $F[X]$ for all $g \in G_{\mathbf{Q}}$. Note that the representation π is odd, and consequently if c is a "complex conjugation" involution in $G_{\mathbf{Q}}$, $\pi(c)$ is not a scalar matrix. It follows from these facts applied to ([Sch] IXa) that the representation π can be descended to a representation $G_{\mathbf{Q}} \to GL_2(F)$, whose semi-simplification gives the residual representation attached to P. The problem of descent of coefficients from $\tilde{F}$ to F is connected to the notion of "Schur index" for which a general reference is [Serre 3] 12.2.

Step 3: Maximal ideals

If P is a maximal ideal, there are two (closely related) ways to proceed. One may find a nonminimal prime ideal P' properly contains in P. Use the residual representation attached to P' (constructed in Step 2) and an argument analogous to the argument of Step 2 to construct the residual representation attached to P. More succinctly, however, we may find such a P' which is the kernel of a specialization homomorphism $s_k : \mathbf{T} \to \mathbf{C}_p$ of weight k, where k is an integer $\geqslant 2$. One can then just apply [D-S], 6b to the newform attached to s_k. q.e.d.

Let $\mathbf{T}_P$ denote the completion of the localization of $\mathbf{T}$ at the prime ideal P. Thus, if P is a minimal prime, then $\mathbf{T}_P$ is a factor of the total quotient ring of $\mathbf{T}$; if P is a maximal prime, then $\mathbf{T}_P$ is a factor of the semi-local ring $\mathbf{T}$; if P is an "intermediary" prime, then $\mathbf{T}_P$ is an order in complete discrete valuation ring whose residue field is F.

Let $W_P = W \otimes_{\mathbf{T}} \mathbf{T}_P$. Define

$$d_P := \dim_F(W \otimes_{\mathbf{T}} F) = \dim_F(W_P \otimes_{\mathbf{T}_P} F).$$

The following statements are equivalent:

(a) $d_{\mathrm{p}} = 2$.

(b) *The semi-simplification of the* $F[G_{\mathbf{Q}}]$*-module* $W \otimes_{\mathbf{T}} F$ *is a residual representation attached to* P.

(c) W_P *is free of rank* 2 *over* $\mathbf{T}_p$.

(d) $\mathbf{T}_P$ *is Gorenstein.*

This follows from Proposition 2 of §8 together with standard arguments in commutative algebra.

QUESTION: *Do the equivalent statements* (a)–(d) *always hold*?

PROPOSITION 2: *Suppose that the residual representation attached to P is irreducible. Then the equivalent assertions* (a), (b), (c), *and* (d) *all hold.*

PROOF: Let V be a two-dimensional vector space over F and $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{Aut}(V)$ a residual representation attached to P. Denote $W \otimes_{\mathbf{T}} F$ by $\overline{W}$, and let

$$0 \subset \overline{W}_1 \subset \overline{W}_2 \subset \cdots \subset \overline{W}_s$$

denote a $G_{\mathbf{Q}}$-stable filtration each of those successive quotients is a residual representation attached to P, i.e., $\overline{W}_j / \overline{W}_{j-1} = V$ as $G_{\mathbf{Q}}$-modules for $j = 1, 2, \ldots, s$. There is such a filtration since ρ is irreducible and consequently one can make use of the argument [M2] or [W] which brings the Eichler-Shimura relations, the Cebotarev theorem and Brauer-Nesbitt to bear on the situation. New let $I = I_{\mathbf{Q}_p}$ and note that the inertial invariants V^I in the residual representation form an F-vector space of dimension 1. It follows from the Proposition of §9 that $\overline{W}^I = \overline{W}_1^I$ and consequently that the action of the element τ (cf. the proof of proposition 2 of §8) which acts like the scalar -1 on $\overline{W}/\overline{W}^I$ also acts like the scalar -1 on $\overline{W}_j/\overline{W}_{j-1}$ for $j \geqslant 2$. But this is impossible. Hence $s = 1$. Consequently (a) holds.

COROLLARY 1: *Let* $\mathfrak{m} \subseteq \mathbf{T}$ *be a maximal ideal. Suppose the residual representation attached to* $\mathfrak{m}$ *is irreducible. Then the assertions* (a), (b), (c) *and* (d) *all hold for any prime ideal P contained in* $\mathfrak{m}$.

COROLLARY 2: *Let* $\lambda : \mathbf{T} \to \overline{\mathbf{Q}}_P$ *be a continuous homomorphism and let* $P \subset \mathbf{T}$ *be the kernel of* λ. *Suppose that* λ *has weight k for* $k \in \mathbf{Z}_p$. *Then if the attached residual representation to P is irreducible* (*e.g., if the attached residual representation to the maximal ideal containing P is irreducible*), *we have that the twists of W are* $(0,\ k-1)$.

§10. Full representations

Let G be a compact topological group and $\rho : G \to GL_2(R)$ a continuous homomorphism, where R is a topological ring. Say that ρ is *full* if the image of ρ contains $SL_2(R)$. Clearly, fullness depends only upon the R-equivalence class of the representation ρ.

PROPOSITION: *Let* $P \subset \mathfrak{m}$ *be ideals in* $\mathbf{T}$ *with* $\mathfrak{m}$ *maximal. Suppose that the residual representation attached to* $\mathfrak{m}$ *is full. Then* $\mathbf{T}_P$ *is Gorenstein,* W_P *is free of rank two over* $\mathbf{T}_P$, *the action of* $G_{\mathbf{Q}}$ *on* W_P *determines a* $\mathbf{T}_P$*-equivalence class of representations*

$$\rho_P : G_{\mathbf{Q}} \to GL_2(\mathbf{T}_P).$$

Suppose that $p \geqslant 5$ *and* $\Lambda \to \mathbf{T}_{\mathfrak{m}}$ *is an isomorphism. Then* $\rho_{\mathfrak{m}}$ *is full.*

PROOF: Since the residual representation attached to $\mathfrak{m}$ is full, it is irreducible, and hence we may apply the Proposition of §10. This defines ρ_P. To see that ρ_P is full, we use the Proposition of §9 together with a result of Nigel Boston (Proposition 3 of the appendix).

§11. Specialization to weight one

Let $\lambda : \mathbf{T} \to \overline{\mathbf{Q}}_P$ be a continuous homomorphism, with kernel P. Then $\mathcal{O} = \mathbf{T}/P$ is an order in a complete discrete valuation ring which is a finite extension of $\mathbf{Z}_P$. Denote by F the field of fractions of $\mathcal{O}$. Supose that λ has weight k. Suppose that the residual representation attached to P is irreducible. Thus we have the representation $\rho_P : G_{\mathbf{Q}} \to GL_2(\mathcal{O})$. By passage to the field of fractions we have an F-valued two-dimensional representation denoted ρ_F of $G_{\mathbf{Q}}$. Hida has shown that when k is a natural number $\geqslant 2$, this F-valued representation is a Deligne representation attached to a cuspidal newform of weight k (of level a power of p). What happens when $k = 1$?

Suppose that $k = 1$. By the corollary of §10 the λ-adic Hodge twists of ρ_F are (0, 0). Let e be the largest natural number such that $\mathcal{O}$ contains a primitive p^{e-1}-st root of 1. By what has been already demonstrated one easily sees that the action of $I_{\mathbf{Q}_p(\zeta_{p^e})}$ via ρ_P is unipotent. It follows that ρ_F falls into one of these two (mutually exclusive) cases:

(I) (*the case of semi-simple* λ*-adic Hodge structure*) In this case the restriction of the representation ρ_P to $G_{\mathbf{Q}_p(\zeta_{p^e})}$ is everywhere unramified.

(II) (*the case of non semi-simple* λ*-adic Hodge structure*) In this case the action of $I_{\mathbf{Q}_p(\zeta_{p^e})}$ via ρ_P is infinite and unipotent.

REMARKS: It can happen that the representation ρ_{P} is a Deligne representation attached to a classical cuspidal newform of weight one. In this case, by the theorem of Deligne-Serre [D-S], the representation ρ_P factors through a finite quotient group of $G_{\mathbf{Q}}$, and consequently we are in case (I).

We do not know whether it can happen that we are in case (I) and yet the representation ρ_{P} does not factor through a finite quotient group of $G_{\mathbf{Q}}$. Indeed, to our knowledge, it is an open question to determine whether or not there are everywhere unramified l-adic representations of G_K for K a number field, such that G_K acts infinitely. As we shall presently see, there *are* examples of case II.

PROPOSITION: *Suppose that these further hypotheses hold*:

(1) $G_{\mathbf{Q}}$ *does not act* (*via* ρ_{P}) *through a finite quotient group*.

(2) $e=1$ *and* $p \leqslant 19$.

Then we are in case (*II*), *i.e., the* λ*-adic Hodge structure is non semi-simple*.

PROOF: Since $e=1$ we have that $G_{\mathbf{Q}(\zeta_p)}$ acts in an everywhere unramified manner, via ρ_{P}. Let $L/\mathbf{Q}$ be the (infinite) Galois field extension cut out by ρ_{P}. But Odlyzko [Od] (*On conductors and discriminants*) has results which, in efffect, put an upper bound on the degree of any normal extension $L/\mathbf{Q}$ which contains $\mathbf{Q}(\zeta_p)$ and is everywhere unramified over $\mathbf{Q}(\zeta_p)$, provided $p \leqslant 19$. Specifically, let $K=\mathbf{Q}(\zeta_p)$, and let D_L, D_K denote the discriminants of L and K; let n_L, n_K denote their degrees over $\mathbf{Q}$. Then,

$$D_L^{1/n_L} = D_K^{1/n_K} = p^{(p-2)/(p-1)}.$$

But by Odlyzko (loc. at. (1.10)),

$$D_L^{1/n_L} > 22.2\ \mathrm{e}^{-254/n_L}$$

and consequently, if $p \leqslant 19$, we have:

$$n_L < 254/\left(\log 22.2 - \frac{p-2}{p-1}\log p\right).$$

REMARK: By loc. cit. (1.13), if the Generalized Riemann Hypothesis holds (for L) then one can improve the above corollary by weakening the hypothesis $p \leqslant 19$ to $p \leqslant 41$.

§12. Numerical examples

Consider the unique cuspidal newform of level 1 and weight 12,

$$\Delta = q \cdot \prod_{n \geqslant 1} (1 - q^n)^{24} = \sum_{n \geqslant 1} \tau(n) q^n$$

($q = e^{2\pi i z}$, where z is the uniformizing parameter of the upper half plane).

Fix p a prime number such that

$$\tau(p) \not\equiv 0 \bmod p \tag{$*$}$$

(e.g., the only prime numbers $< 2{,}041$ such that $\tau(p) \equiv 0 \bmod p$ are $p = 2$, 3, 5 and 7).

For any such prime number $p \leqslant 19$, and for any natural number $j \geqslant 2$, there is a unique cuspidal newform $\phi_p^{(j)}$ with Fourier coefficients in $\mathbf{Z}_p$ which is on $\Gamma_1(p)$, is of weight j with nebentypus character ω^{12-j}, and is p-ordinary (*note*: A modular form with Fourier coefficients in $\mathbf{Z}_p$ is *p-ordinary* if it is an eigenform for the operator U_p with eigenvalue a p-adic unit).

The l-th Fourier coefficient of $\phi_p^{(j)}$ is congruent to $\tau(l)$ modulo p.

Now suppose that p is *different from* 11, and consequently the modular form $\phi_p^{(2)}$ of weight 2 has *nontrivial* nebentypus character ω^{10}.

Let $\mathbf{T}$ denote the Hecke algebra attached to p, as in §7. It follows from Hida's theory (Prop. 3 of §8) that there is a maximal ideal $\mathfrak{m} \subseteq \mathbf{T}$ with residue field $\mathbf{F}_p$ such that the natural projection

$$\mathbf{T} \to \mathbf{T}/\mathfrak{m} = \mathbf{F}_p$$

sends the Hecke operator T_l to $\tau(l) \bmod p$ for $l \neq p$, and U_p to $\tau(p) \bmod p$. Suppose, the completion of $\mathbf{T}$ with respect to the maximal ideal $\mathfrak{m}$ is a (finite flat) Λ-algebra *of rank* 1, i.e., the natural mapping

$$\Lambda \to \mathbf{T}_{\mathfrak{m}} \tag{$**$}$$

is an isomorphism.

It follows that $\mathbf{T}_{\mathfrak{m}}$ is Gorenstein and consequently, by the discussion in §10, we have that $W_{\mathfrak{m}}$ is free over $\mathbf{T}_{\mathfrak{m}}$ of rank 2. We thus have a natural representation

$$\rho_{\mathfrak{m}} : G_{\mathbf{Q}} \to \mathrm{Aut}(W_{\mathfrak{m}}) = GL_2(\mathbf{T}_{\mathfrak{m}}).$$

We may identify $\mathbf{T}_{\mathfrak{m}}$ with $\mathbf{Z}_p[[T]]$, the power series ring in one variable T over the p-adic integers:

$$\mathbf{T}_{\mathfrak{m}} = \Lambda \cong \mathbf{Z}_p[[T]]$$

$$[1+p] \in \Gamma \longleftrightarrow 1 + T \in \mathbf{Z}_p[[T]]$$

and view the representation $\rho_{\mathfrak{m}}$ as giving a homomorphism

$$\rho_{p,\Delta} : G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p[[T]]).$$

This is the homomorphism alluded to as an example of Hida's theory, in the Introduction. To simplify notation we refer to $\rho_{\mathrm{p},\Delta}$ simply as ρ_p in what follows. Note that for any $k \in \mathbf{Z}_p$, we have the specialization homomorphism

$$\mathbf{Z}_p[[T]] \underset{s_k}{\to} \mathbf{Z}_p$$

$$1 + T \to (1+p)^{k-1}.$$

Composition of ρ_p with the homomorphism $GL_2(\mathbf{Z}_p[[T]]) \to GL_2(\mathbf{Z}_p)$ induced from s_k yields a representation

$$\rho_p^{(k)} : G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p); \quad k \in \mathbf{Z}_p.$$

For $k = j$, a natural number $\geqslant 2$, the specialized representation $\rho^{(j)}$ is the p-adic representation attached (by Deligne) to the cuspidal newform $\phi_p^{(j)}$; in particular we have that $\rho_p^{(12)}$ is the p-adic representation attached to Δ.

PROPOSITION 1: *Let p be a prime number such satisfying* $(**)$ *that* $\tau(p) \not\equiv 0 \bmod p$, *and suppose that* $p \neq 11$, 23, *and* 691. *Then the representation*

$$\rho_{p,\Delta} : G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p[[T]])$$

is full, i.e., its image contains $SL_2(\mathbf{Z}_p[[T]])$.

PROOF: We use the results of Serre and Swinnerton-Dyer ([SwD] §4, Cor. to Thm. 4; [Serre 2] 3.3) which guarantee that the residual representation

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

(which is the representation attached to Δ mod p) is full if $p \geqslant 11$ and

$p \neq 23$, 691. Then apply the Proposition of §11. Now consider the specialization of ρ_p to weight 1,

$$\rho_p^{(1)}: G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p).$$

If $p = 23$, this representation factors through a subgroup of $GL_2(\mathbf{Z}_p)$ isomorphic to the symmetric group on three letters; in this case the representation $\rho_p^{(1)}$ is the representation attached by Serre and Deligne to a cuspform of weight 1 (the unique such cuspform of level 23). If, however, p is such that $\tau(p) \not\equiv 0 \bmod p$ and $p \neq 11, 23, 691$, then the homomorphism $\rho_p^{(1)}$ is full; consequently it cannot be the p-adic representation attached to a (classical) modular form of weight one.

PROPOSITION 2: *If $p = 13, 17, 19$, then the p-adic Hodge structure of the representation $\rho_p^{(1)}$ (restricted to the decomposition group at p) is non-semi-simple.*

PROOF: In these cses $\rho_p^{(1)}$ satisfies the hypotheses of the Proposition of §12.

REMARKS: (1) Under the Generalized Riemann Hypothesis we would obtain that $\rho_p^{(1)}$ has non-semi-simple p-adic Hodge structure for $29 \leqslant p \leqslant 41$ (cf. the discussion at the end of §12). Is the p-adic Hodge structure of $\rho_{\mathrm{p}}^{(1)}$ non-semi-simple for all $p > 23$, with $\tau(p) \not\equiv 0 \bmod p$?

(2) Fix $p \geqslant 13$, $p \neq 23$, $\tau(p) \not\equiv 0 \bmod p$ and consider the representation $\rho_p^{(1)}$. Does $\rho_p^{(1)}$ fit into a compatible family of representations (cf. [Serre 1] for a discussion of the notion of compatible families)? Presumably not, but we have not been able to rule the possibility out. For ϕ_l, $l \neq p$, an l-Frobenius element in $G_{\mathbf{Q}}$, what sort of numbers are the eigenvalues of $\rho_p^{(1)}(\phi_l)$?

(3) One may also consider the representations $\rho_p^{(k)}$ for nonpositive integers $k = 0, -1, -2, \ldots$. It follows from the Corollary in §10 that these representations are of Hodge-Tate type. The representation $\rho_p^{(k)}$ with $p = 13$, $k = 0$ is worth singling out (see Prop. 3 below).

(4) Atkin has proved that there is a 13-adic integer u_{13} uniquely characterized by the property that

$$\lim_{m \to \infty} U_{13}^m \cdot (j - 744)/u_{13}^m$$

converges (indeed: to a 13-adic modular form in the sense of Katz cf. [Ka] 3.13), where j is the elliptic modular function.

Denote by j^0 the 13-adic modular form given as the above limit. One knows that j^0 is an eigenform for the Hecke operators T_l $(l \neq 13)$. It follows from the result of Atkin that j^0 is a p-ordinary, p-adic modular form (of weight 0 and trivial character) for $p = 13$. But (up to scalar multiple) there is only one such form (of p-power level) as follows from the Proposition of Hida (Prop. 3 of §8) plus the fact that our $\mathbf{T}_{\mathfrak{m}}$ is equal to Λ (i.e. it is of rank 1 over Λ). Thus, we have:

PROPOSITION 3: *Let $\rho_p^{(k)}$ be as above, and let $\rho_{13}^{(0)}$ denote its specialization to $p = 13$ and weight $k = 0$. For any prime number $l \neq 13$, let $t_l \in \mathbf{Z}_{13}$ denote the eigenvalue of T_l acting on j^0, and let $\phi_l \in G_{\mathbf{Q}}$ be a choice of Frobenius element at l. Then*:

$$\text{Trace } \rho_{13}^{(0)}(\phi_l) = t_l \in \mathbf{Z}_{13}.$$

(5) In studying ρ_p we have considered only the "simplest" specializations to each weight k. But for any primitive p^m-th root of 1, η, in $\mathbf{C}_p$, we have the "η-twisted specialization to weight k" which is a continous homomorphism of $\mathbf{Z}_p[[T]]$ to $\mathbf{Z}_p[\eta] \in \mathbf{C}_p$ given by sending the element $1 + T$ to $\eta(1+p)^{k-1}$. Given any prime number p such that $\tau(p) \not\equiv 0 \bmod p$ (i.e., so that we have ρ_p) we may compose ρ_p with the induced homomorphism coming from the "η-twisted specialization to weight k" to obtain a representation which we might denote

$$\rho_p^{(k,\eta)} : G_{\mathbf{Q}} \to GL_2\big(\mathbf{Z}_p[\eta]\big).$$

It would be interesting to study the η-twisted specializations to *weight one* in detail. For example, how often do they have non-semi-simple p-adic Hodge structure?

References

[At] O, ATKIN: Congruences for modular forms. Proceedings of the IBM Conference on Computers in Mathematical Research, Blaricium, 1966. North-Holland (1968) 8–19.

[C-R] C. CURTIS and I. REINER: *Representation theory of finite groups and associative algebras*. Interscience, New York (1962).

[D-S] P. DELIGNE and J.-P. SERRE: Formes modulaires de poids 1. *Ann. Sci. Ecole Norm. Sup*. 7 (1974) 507–730.

[Fa] G. FALTINGS: Report on Hodge-Tate-Structures. (preprint. Princeton U. 1985).

[Gr] A. GROTHENDIECK: *Groupes de Monodromie en Géométrie Algébrique. Lecture Notes in Mathematics*, 288. Springer-Verlag, Berlin-Heidelberg-New York (1972).

[Har] R. HARTSHORNE: *Residues and Duality. Lecture Notes in Mathematics*, 20 Springer-Verlag, Berlin-Heidelberg-New York (1966).

[Hi 1] H. HIDA: Iwasawa modules attached to congruences of cusp forms. To appear in *Ann. Sci. E.N.S.*

[Hi 2] H. HIDA: Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms (preprint).

[Ka] N. KATZ: P-adic properties of modular schemes and modular forms. *Modular Functions of One Variable III. Lecture Notes in Mathematics*, 350. Springer Verlag, Berlin-Heidelberg-New York (1973) 69–141.

[K-M] N. KATZ and B. MAZUR: Arithmetic moduli of elliptic curves. *Annals of Math. Studies*, 108. Princeton Univ. Press (1985).
[Li] W. LI: Newforms and functional equations. *Math. Ann.* 212 (1975) 285–315.
[M1] B. MAZUR: Isogenies of prime degree. *Inv. Math.* 44 (1978) 129–162.
[M2] B. MAZUR: Modular curves and the Eisenstein ideal. *Publ. Math. IHES* 47 (1978) 33–186.
[M-W 1] B. MAZUR and A. WILES: Classfields of abelian extensions of **Q**. *Inv. Math.* 76 (1984) 179–330.
[M-W 2] B. MAZUR and A. WILES: Analogies between function fields and number fields. *Amer. J. Math.* 105 (1983) 507–521.
[Od] A. ODLYZKO: On conductors and discriminants.
[O] A. OGG: On the eigenvalues of Hecke operators. *Math. Ann.* 179 (1969) 101–108.
[Sch] I. SCHUR: Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen, Sitzungsberichte Preuss. Ak. der Wiss. (1906) pp. 164–184. In: *Gesammelte Abhandlungen* I. Springer-Verlag, Berlin-Heidelberg-New York (1973) 177–197.
[Sen] S. SEN: Continuous cohomology and p-adic Galois representations. *Inv. Math.* 62 (1981) 89–116.
[Serre 1] J.-P. SERRE: Représentations l-adiques. Kyoto Int. Symp. on Algebraic Number Theory (1977) 177–193.
[Serre 2] J.-P. SERRE: Congruences et formes modulaires [d'après H.P.F. Swinnerton-Dyer] Sém. Bourbaki exp. 416. *Lecture Notes in Mathematics* 317. Springer-Verlag, Berlin-Heidelberg-New York (1973) 319–338.
[Serre 3] J.-P. SERRE: *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg-Berlin (1977).
[S-T] J.-P. SERRE and J. TATE: Good reduction of abelian varieties, *Ann. of Math.* 88 (1968) 492–517.
[SwD] H.P.F. SWINNERTON-DYER: On l-adic representations and congruences for coefficients of modular forms. *Modular Functions of One Variable* III. *Lecture Notes in Mathematics*, 350. Springer-Verlag, Berlin-Heidelberg-New York (1973) 1–56.
[Ta] J. TATE: p-divisible groups. Proceedings of a conference on local fields (Driebergen 1966). Berlin-Heidelberg-New York, Springer-Verlag (1967) 158–183.
[W] A. WILES: Modular curves and the class group of $\mathbf{Q}(\zeta_p)$. *Inv. Math.* 58 (1980) 1–35.

Appendix (by Nigel Boston)

The center and the commutator subgroup of a group G are denoted by $Z(G)$ and G' respectively.

PROPOSITION 1: *Let* $1 \to \Gamma \to G \to Q \to 1$ *be an exact sequence of groups, Γ abelian. Let H be a subgroup of G projection onto Q. Let $V_1, \dots, V_d$ be minimal Q-invariant subgroups of Γ that generate Γ. If for $1 \leqslant i \leqslant d$, $\exists x_i \in V_i \setminus Z(G)$ normalizing H, then $H = G$.*

PROOF: Suppose $H \neq G$. Since each $H \cap V_j$ is Q-invariant, $H \cap V_i = 1$ for some i. Consider $[x_i, H]$, the group generated by all $x_i h x_i^{-1} h^{-1}$ $(h \in H)$. Since x_i normalizes H and V_i is Q-invariant, $[x_i, H] \subseteq H \cap V_i = 1$. Since $[x_i, \Gamma] = 1$ and $H\Gamma = G$, $[x_i, G] = 1$, i.e., $x_i \in Z(G)$, a contradiction.

Let R be a complete noetherian local ring, maximal ideal $\mathfrak{m}$, with $R/\mathfrak{m}$ finite, $\mathrm{char}(R/\mathfrak{m}) = p \neq 2$.

PROPOSITION 2: *Let H be a closed subgroup of $SL_n(R)$ projecting onto $SL_n(R/\mathfrak{m}^2)$. Then $H = SL_n(R)$.*

For this we need the following definition. The *Frattini subgroup*. $\Phi(G)$, of a group G is the intersection of the maximal subgroups of G. We shall use:

LEMMA: *If J is a subgroup of the finite group G projecting onto G/K, and if $\Phi(G) \supseteq K$, then $J = G$.*

PROOF: If $J \neq G$, then J lies in some maximal subgroup M. Since $K \supseteq \Phi(G)$, $K \supseteq M$ and so $JK \supseteq M$, contradicting $JK = G$.

The only properties of $\Phi(G)$ we need are (see [1], Chapter 11):

(i) if K is a normal subgroup of the finite group G, then $\Phi(K) \supseteq \Phi(G)$;

(ii) If G is a finite p-group, then $\Phi(G) = G' \cdot G^p$ (i.e., generated by commutators and p^{th} powers).

For future use, if I is an ideal of the ring A, define $\Gamma(I) = \ker(SL_n(A) \to SL_n(A/I))$ (the choice of n will be clear from the context).

PROOF OF PROPOSITION 2: We apply the lemma with $G = SL_n(R/\mathfrak{m}^r)$ and $G/K = SL_n(R/\mathfrak{m}^{r-1})$ to show by induction that H projects onto $SL_n(R/\mathfrak{m}^r)$ for each $r \geqslant 2$.

Each $\Gamma(\mathfrak{m}^t/\mathfrak{m}^{t+1})$ is an elementary abelian p-group since its multiplication is given by componentwise addition. Thus $\Gamma(\mathfrak{m}/\mathfrak{m}^r)$ is a p-group and so by properties (i) and (ii)) $\Phi SL_n(R/\mathfrak{m}^r)) \supseteq \Phi\Gamma(\mathfrak{m}/\mathfrak{m}^r)) \supseteq \Gamma(\mathfrak{m}/\mathfrak{m}^r)'$. To apply the lemma we just need $\Gamma(\mathfrak{m}/\mathfrak{m}^r)' \supseteq \Gamma(\mathfrak{m}^{r-1}/\mathfrak{m}^r)$, which is easily checked using $(1+u)(1+v)(1+u)^{-1}(1+v)^{-1} = 1 + [u, v] +$ higher terms, choosing $u, v \in M_n(\mathfrak{m}/\mathfrak{m}^r)$ to produce generators of $\Gamma(\mathfrak{m}^{r-1}/\mathfrak{m}^r)$.

REMARK: Is this true with SL_n replaced by any semisimple group? Sample calculations suggest this is the case.

Suppose now $p \geqslant 5$ and $p \nmid n$. Let $I_1, \dots, I_d$ be minimal ideals of $R/\mathfrak{m}^2$ that generate $\mathfrak{m}/\mathfrak{m}^2$, where $d = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

COROLLARY: *Let H be a closed subgroup of $SL_n(R)$ projecting onto $SL_n(R/\mathfrak{m})$, such that for $1 \leqslant i \leqslant d$, $\exists x_i \in \Gamma(I_i) \setminus Z(SL_n(R/\mathfrak{m}^2))$ normalizing the image of H in $SL_n(R/\mathfrak{m}^2)$. Then $H = SL_n(R)$.*

PROOF: By the work of Klingenberg [2] (see [3], pp. 84, 245 for a summary), the $\Gamma(I_i)$ are minimal $SL_n(R/\mathfrak{m})$-invariant subgroups of

$\Gamma(\mathfrak{m}/\mathfrak{m}^2)$ since they are minimal normal subgroups of $SL_n(R/\mathfrak{m}^2)$. By Proposition 1, H projects onto $SL_n(R/\mathfrak{m}^2)$ and by Proposition 2, $H = SL_n(R)$.

To apply this corollary to the proposition in §11, we now suppose R has Krull dimension 2 and $\mathfrak{m} = (p, \tau)$ $(p \geqslant 5)$, so R is regular and $p \notin \mathfrak{m}^2$.

PROPOSITION 3: *Let* $\rho: \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to Gl_2(R)$ *be a continuous representation, inducing* $\bar{\rho}: \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(R/\mathfrak{m})$. *Let* I_p *be the inertia subgroup at* p. *Suppose*

(*i*) $\bar{\rho}$ *is full, i.e.,* Im $\bar{\rho}$ *contains* $SL_2(R/\mathfrak{m})$;

(*ii*) $\exists$ *a matrix* $\begin{pmatrix} 1 & * \\ 0 & 1+\tau \end{pmatrix}$ *in* $\rho(I_p)$,

(*iii*) *for each* $b \in (R/\mathfrak{m})^*$, $\exists$ *a matrix* $\begin{pmatrix} 1 & * \\ 0 & b \end{pmatrix}$ *in* $\bar{\rho}(I_p)$,

(*iv*) $\rho(I_p) \subseteq \left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\}$.

Then ρ *is full, i.e.,* Im ρ *contains* $SL_2(R)$.

PROOF: We apply the last corollary with $H = \mathrm{Im}\ \rho \cap SL_2(R)$. Let H_2 be the image of H in $SL_2(R/\mathfrak{m}^2)$ and $J_1 = (p, \mathfrak{m}^2)/\mathfrak{m}^2$, $J_2 = (\tau, \mathfrak{m}^2)/\mathfrak{m}^2$.

We first see that $\Gamma(J_1) \subseteq H_2$. If $1 + u \in H_2$ is an inverse image of a transvection in $SL_2(R/\mathfrak{m})$, then $(1+u)^p = 1 + pu$. This produces a nontrivial $x_1 \in H_2 \cap \Gamma(J_1)$, so by minimality of $\Gamma(J_1)$, $H_2 \cap \Gamma(J_1) = \Gamma(J_1)$.

Now we just need a noncentral $x_2 \in \Gamma(J_2)$ normalizing H_2. Consider the set of $r \in R$ such that $\begin{pmatrix} 1 & r \\ 0 & 1+\tau \end{pmatrix} \in \rho(I_p)$ (nonempty by (ii)). If one such r lies in $\mathfrak{m}$, then adjusting by an element of $\Gamma(J_1)$ and multiplying by $(1+\tau)^{-1/2}$ produces the desired x_2.

Thus we asume that no such r lies in $\mathfrak{m}$.

Let $U = \left\{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in R/\mathfrak{m},\ \ b \in (R/\mathfrak{m})^*\right\}$ and consider $V = U \cap \bar{\rho}(I_p)$. By our assumption V contains a matrix $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $a \neq 0$, but by (iii) V projects onto $\left\{\begin{pmatrix} 1 & 0 \\ 1 & b \end{pmatrix} : b \in (R/\mathfrak{m})^*\right\}$ which acts irreducibly on the kernel. Thus $V = U$, and in particular $V' = \left\{\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in R/\mathfrak{m}\right\}$.

Now all elements of $\rho(I_p')$ have determinant 1, so by (iv) and the last paragraph, for each $a \in R/\mathfrak{m}$, $\rho(I_p')$ contains an element $\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$ where $v \mapsto a$.

Thus we can adjust the element produced by (ii) so that $r \in \mathfrak{m}$, contradicting our earlier assumption.

References

[1] J. Rose: *A Course on Group Theory*. Cambridge Univ. Press, London/New York (1978).
[2] W. Klingenberg: Lineare Gruppen über lokalen Ringen, *Amer. J. Math.* 83 (1961) 137–153.
[3] B.R. McDonald: *Geometric Algebra over Local Rings*. Marcel Dekker Inc., New York and Basel (1976).

(Oblatum 15-IX-1985)

B. Mazur
Department of Mathematics
Harvard University
1 Oxford Street
Cambridge, MA 02138
USA

A. Wiles
Department of Mathematics
Princeton University
Princeton, NJ 08540
USA