Katz p-adic L-functions, congruence modules and deformation of Galois representations

H. HIDA* AND J. TILOUINE

0. Although the two-variable main conjecture for imaginary quadratic fields has been successfully proven by Rubin [R] using brilliant ideas found by Thaine and Kolyvagin, we still have some interest in studying the new proof of a special case of the conjecture, i.e., the anticyclotomic case given by Mazur and the second named author of the present article ([M-T], [T1]). Its interest lies firstly in surprizing amenability of the method to the case of CM fields in place of imaginary quadratic fields and secondly in its possible relevance for non-abelian cases. In this short note, we begin with a short summary of the result in [M-T] and [T1] concerning the Iwasawa theory for imaginary quadratic fields, and after that, we shall give a very brief sketch of how one can generalize every step of the proof to the general CM-case. At the end, coming back to the original imaginary quadratic case, we remove some restriction of one of the main result in [M-T]. The idea for this slight amelioration to [M-T] is to consider deformations of Galois representations not only over finite fields but over any finite extension of $\mathbf{Q}_p$. Throughout the paper, we assume that $p > 2$.

1. Let M be an imaginary quadratic field and p be an odd prime which splits in M; i.e., $p = \overline{\mathfrak{p}}\mathfrak{p}(\mathfrak{p} \neq \overline{\mathfrak{p}})$. We always fix the algebraic closures $\overline{\mathbf{Q}}$ and $\overline{\mathbf{Q}}_p$ and embeddings of $\overline{\mathbf{Q}}$ into $\mathbf{C}$ and $\overline{\mathbf{Q}}_p$. Any algebraic number field will be considered to be inside $\overline{\mathbf{Q}}$. Suppose the factor $\mathfrak{p}$ of p is compatible with this embedding M into $\overline{\mathbf{Q}}_p$. The scheme of the new proof of the main conjecture for the anti-cyclotomic $\mathbf{Z}_p$-tower of M consists in proving two divisibility theorems between the following three power series:

$$(1.1) \qquad L^-|H|Iw^-,$$

where

* The first named author is supported in part by an NSF grant

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

(i) L^- is the Katz–Yager p-adic L-function (which interpolates p-adically Hurwitz–Damerell numbers) projected to one branch of the anti-cyclotomic line of the imaginary quadratic field M;

(ii) H is the characteristic power series of the congruence module attached to M (and the branch in (i)) constructed via the theory of Hecke algebras for $GL(2)_{/\mathbf{Q}}$;

(iii) Iw^- is the characteristic power series (of the branch in (i)) of the maximal $\mathfrak{p}$-ramified extension of the anti-cyclotomic $\mathbf{Z}_p^\times$-tower over M.

Once these divisibilities are assumed, the proof is fairly easy: Under a suitable branch condition, we know from the analytic class number formula that the λ and μ-invariants of G and Iw^- are the same and hence

(1.2) $$Iw^- = L^- \quad \text{up to a unit power series}$$

as the anticyclotomic main conjecture predicts.

Strictly speaking, the equality (1.2) is proven in [M-T] and [T] under the assumption that the class number of M is equal to 1. In fact, if the class number h of M is divisible by p, we need to modify (1.1) as

(1.3) $$h \cdot L^- | H | h \cdot Iw^- \quad \text{for the class number } h \text{ of } M.$$

In [M-T], the second divisibility assertion: $H \mid Iw^-$ is proven under the milder assumption that h is prime to p but there is another assumption that the branch character ψ of L^- must be non-trivial on the inertia group $I_\mathfrak{p}$ at $\mathfrak{p}$. We will prove the divisibility (1.3) outside the trivial zero of L^- (if any) without hypothesis in Appendix.

2. In this section, we deal with the generalization of the first divisibility result: $L^- \mid H$ in the general CM case. The second divisibility: $H \mid Iw^-$ will be dealt with in the following paragraphs. To state the result precisely, we fix a prime p and write the fixed embeddings as $\iota_p : \overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$ and $\iota_\infty : \overline{\mathbf{Q}} \to \mathbf{C}$. We consider $\overline{\mathbf{Q}}$ as a subfield of $\overline{\mathbf{Q}}_p$ and $\mathbf{C}$ by these embeddings. Let F be a totally real number field with class number $h(F)$ and M/F be a totally imaginary quadratic extension whose class number is denoted by $h(M)$. Let c be the complex conjugation which induces the unique non-trivial automorphism of M over F. We assume the following ordinarity condition:

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

Ordinarity hypothesis All prime factor $\mathfrak{p}$ of p in F splits in M.

Thus we can write the set of prime factors of p in M as a disjoint union $S \cup S^c$ of two subsets of prime ideals so that $\mathfrak{P} \in S$ if and only if $\mathfrak{P}^c \in S^c$. If a is the number of prime ideals in F over p, there are 2^a choices of such subset S. Such an S will be called a p-adic CM-type. Considering S as a set of p-adic places of M, let Σ be the set of embeddings of M into $\overline{\mathbf{Q}}$ which give rise to places in S after combining with ι_p. Then $\Sigma \cup \Sigma \circ c$ is the total set of embeddings of M into $\overline{\mathbf{Q}}$ and hence gives a complex CM-type of M. Hereafter we fix a p-adic CM-type S and compatible complex CM-type Σ. Let $\mathbf{G}$ be the Galois group of the maximal p-ramified abelian extension M_∞ of M. Then we fix a decomposition $\mathbf{G} = \mathbf{G}_{tor} \times \mathbf{W}$ for a finite group $\mathbf{G}_{tor}$ and a $\mathbf{Z}_p$-free module $\mathbf{W}$. Let $K/\mathbf{Q}_p$ be a p-adically complete extension in the p-adic completion Ω of $\overline{\mathbf{Q}}_p$ containing all the images $\sigma(M)$ for $\sigma \in \Sigma$ and $\mathfrak{O} = \mathfrak{O}_K$ be the p-adic integer ring of K. We now consider the continuous group algebras $\Lambda = \mathfrak{O}[[\mathbf{W}]]$ and $\mathfrak{O}[[\mathbf{G}]] = \Lambda[\mathbf{G}_{tor}]$. By choosing a basis of $\mathbf{W}$, we have $\mathbf{W} \cong \mathbf{Z}_p^r$ and $\Lambda \cong \mathfrak{O}[[X_1, \ldots, X_r]]$. Here $r = [F : \mathbf{Q}] + 1 + \delta$, where δ is the defect of the Leopoldt conjecture for F; i.e., $\delta \geq 0$ and $\delta = 0$ if and only if the Leopoldt conjecture holds for F and p. Fix a character $\lambda : \mathbf{G}_{tor} \to \mathfrak{O}^\times$ and define the projection $\lambda_* : \mathfrak{O}[[\mathbf{G}]] \to \mathfrak{O}[[\mathbf{W}]] = \Lambda$ by $\lambda_*(g, w) = \lambda(g)[w]$ for the group element $[w]$ in Λ for $w \in \mathbf{W}$ and $g \in \mathbf{G}_{tor}$. We consider two anti-cyclotomic characters of $\mathbf{G}$ given by $\lambda_- = \lambda(\lambda^c)^{-1}$ and $\alpha = \lambda_*(\lambda_*^c)^{-1}$, where $\lambda^c(\sigma) = \lambda(c\sigma c^{-1})$ and $\lambda_*^c(\sigma) = \lambda_*(c\sigma c^{-1})$. Let $M^-(\lambda_-)$ be the subfield of M_∞ fixed by $\mathrm{Ker}(\alpha)$. Let $\mathbf{M}_S(\lambda_-)/M^-(\lambda_-)$ be the maximal p-abelian extension unramified outside S. Naturally $X_S = \mathrm{Gal}(\mathbf{M}_S(\lambda_-)/M^-(\lambda_-))$ is a continuous module over $\mathbf{Z}_p[[\mathbf{H}]]$ of $\mathbf{H} = \mathrm{Im}(\alpha)$. We consider the λ_--branch of X_S defined by

$$X_S(\lambda_-) = X_S \otimes_{\mathbf{Z}_p[\mathbf{G}_{tor}]} \mathfrak{O}(\lambda^-)$$

where $\mathfrak{O}(\lambda_-)$ is the $\mathfrak{O}$-free module of rank one on which $\mathbf{G}_{tor}$ acts via λ_-. Once we are given a p-adic CM-type S, we have the following 3 objects as in the imaginary quadratic case:

(i) The λ_--branch of the projection L^- of the Katz p-adic L-function $L \in \mathfrak{O}_\Omega[[\mathbf{G}]]$ to the anti-cyclotomic tower $M^-(\lambda_-)$;

(ii) The congruence power series $H \in \Lambda$ attached to the λ-branch of the nearly ordinary Hecke algebra of CM-type S;

(iii) The characteristic power series Iw^- of $X_S(\lambda_-)$ in Λ.

Note that $\mathrm{Ker}(\alpha)$ contains $\mathbf{G}_+ = \{x \in \mathbf{G} \mid cxc^{-1} = x\}$ and we can realize the quotient $\mathbf{G}/\mathbf{G}_+$ inside $\mathbf{G}$ by the subgroup of commutators $[x, c] = xcx^{-1}c^{-1}$.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721267.013
Cambridge Books Online © Cambridge University Press, 2009

Especially the maximal torsion-free quotient $\mathbf{W}^-$ of $\mathbf{H}$ can be thought of a direct factor of $\mathbf{W}$ via this map. For a technical reason (namely, H resides in Λ), we regard L^- and Iw^- as elements in Λ via this inclusion although they belong to $\Lambda_- = \mathfrak{O}[[\mathbf{W}^-]]$. Moreover, to have a non-zero Iw^-, we need to suppose a weak version of the Leopoldt conjecture (depending on S) for the anti-cyclotomic tower. This weak form of Leopoldt's conjecture holds true if the CM field M is abelian over $\mathbf{Q}$. On the other hand, one can prove unconditionally (i.e. without supposing the weak Leopoldt conjecture) the non-vanishing of the characteristic power series Iw of the maximal S-ramified abelian extension over the full $\mathbf{Z}_p^r$-tower of M. Before giving the precise definition of L^- and H, we state the first theorem:

Theorem 2.1 L^- divides H in $\mathfrak{O}_\Omega[[\mathbf{W}]] \otimes_{\mathbf{Z}} \mathbf{Q}$. Moreover if the μ-invariant of every branch of the Katz p-adic L-function of M vanishes, then we have the strong divisibility:

$$(h(M)/h(F))L^- \mid H \text{ in } \mathfrak{O}_\Omega[[\mathbf{W}]].$$

The following conjecture is obviously motivated by (1.1):

Conjecture 2.2 $H = (h(M)/h(F))L^-$ up to a unit in $\mathfrak{O}_\Omega[[\mathbf{W}]]$ if $p > 2$, where $h(M)$ (resp. $h(F)$) is the class number of M (resp. F).

This conjecture is known to be true if $F = \mathbf{Q}$, $p \geq 5$ and the class number $h(M)$ of M is prime to p under a certain branch condition.

First, let us explain the definition of L^-. Although we will not make the identification with the power series ring due to the lack of canonical coordinates of $\mathbf{W}$, we may regard any element of Λ as a p-adic analytic function of several variables. There are two different ways of viewing $\Phi \in \Lambda$ as an analytic object: For $G = \mathbf{G}$ or $\mathbf{W}$, let $\mathfrak{X}(G)$ be the set of all continuous characters of G with values in $\overline{\mathbf{Q}}_p$. If one fixes a $\mathbf{Z}_p$-basis (w_i) of $\mathbf{W}$, then each character $P \in \mathfrak{X}(\mathbf{W})$ is determined by its value $(P(w_i)) \in D^r$, where $D = \{x \in \overline{\mathbf{Q}}_p \mid |x-1|_p < 1\}$. Thus $\mathfrak{X}(\mathbf{W}) \cong D^r$. Each character $P : G \to \overline{\mathbf{Q}}_p^\times$ induces an $\mathfrak{O}$-algebra homomorphism $P : \mathfrak{O}[[\mathbf{G}]] \to \overline{\mathbf{Q}}_p$ such that $P|_G$ is the original character of G. In this way, we get an isomorphism:

$$\mathfrak{X}(G) \cong \mathrm{Spec}(\mathfrak{O}[[\mathbf{G}]])(\overline{\mathbf{Q}}_p) = \mathrm{Hom}_{\mathfrak{O}\text{-alg}}(\mathfrak{O}[[\mathbf{G}]], \overline{\mathbf{Q}}_p).$$

Then

(A1) Φ is an analytic function on $\mathfrak{X}(G)$ whose value at P is $P(\Phi) \in \overline{\mathbf{Q}}_p$.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

On the other hand, we can view Λ as a space of measures on G in the sense of Mazur so that

$$\text{(A2)} \qquad \int_G P(g)\, d\Phi(g) = P(\Phi) = \Phi(P).$$

By class field theory, we can identify, via the Artin symbol, the group $\mathbf{G}$ with the quotient of the idele group $M_A^\times$. For a given A_0-type Hecke character $\varphi : M_A^\times/M^\times \to \mathbf{C}^\times$ of p-power conductor whose infinity type is given by

$$\varphi(x_\infty) = x_\infty^{-\xi} = \Pi_{\sigma\in\Sigma\cup\rho\Sigma}(x_\infty^\sigma)^{-\xi_\sigma} \text{ for } \xi = (\xi_\sigma)_{\sigma\in\Sigma\cup\rho\Sigma} \in \mathbf{Z}^{\Sigma\cup\rho\Sigma},$$

as shown by A. Weil in 1955, φ has values in $\overline{\mathbf{Q}}$ on finite ideles and we have a unique p-adic avatar $\hat{\varphi} : \mathbf{G} \to \overline{\mathbf{Q}}_p^\times$ which satisfies $\hat{\varphi}(x) = \varphi(x)$ if $x_p = x_\infty = 1$, and if $x_p \in M_p^\times$ is close enough to 1, then

$$\hat{\varphi}(x_p) = x_p^{-\xi} = \Pi_{\sigma\in\Sigma\cup\rho\Sigma}(x_p^\sigma)^{-\xi_\sigma}.$$

In 1978, Katz showed in [K] the existence of a unique p-adic L-function given by an element L of $\mathfrak{O}_\Omega[[\mathbf{G}]]$ such that

$$\frac{L(\hat{\varphi})}{\text{suitable } p\text{-adic period}} = c(\varphi)\frac{L(0,\varphi)}{\text{suitable complex period}}$$

whenever φ is critical at 0 (i.e. if either $\xi_{\sigma\rho} \geq \xi_\sigma + \xi_{\sigma\rho} + 1 \geq 0$ or $\xi_\sigma + 1 \leq \xi_\sigma + \xi_{\sigma\rho} + 1 \leq 0$ for all $\sigma \in \Sigma$). Here, $c(\varphi)$ is a simple constant including a modifying Euler p-factor, local Gauss sum, Γ-factor and a power of π. See [K, (5.3.0), (5.7.8-9)] for details. To define L^-, we first project Katz's L to Λ. Namely, we fix once and for all a finite order character $\lambda : \mathbf{G}_{\mathrm{tor}} \to \mathfrak{O}^\times$. Then we have a continuous character $\lambda_* : \mathbf{G} = \mathbf{G}_{\mathrm{tor}} \times \mathbf{W} \to \mathfrak{O}[[\mathbf{W}]]$ given by

$$\lambda_*(g,w) = \lambda(g)w \in \mathfrak{O}[[\mathbf{W}]],$$

where we consider $\lambda(g)$ for $g \in \mathbf{G}_{\mathrm{tor}}$ as a scalar in $\mathfrak{O}$ but w as a group element in $\mathbf{W}$. This character induces the projection to Λ

$$\lambda_* : \mathfrak{O}[[\mathbf{G}]] = \Lambda[\mathbf{G}_{\mathrm{tor}}] \to \Lambda.$$

Then for any point $P \in \mathfrak{X}(\mathbf{W})$, $\lambda_P = P \circ \lambda_* : \mathbf{G} \to \overline{\mathbf{Q}}_p$ is a p-adic character of $\mathbf{G}$. When λ_P is the avatar of an A_0-type Hecke character, we say that P is arithmetic (this notion of arithmeticity is independent of the choice of λ). Let c denote the complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/F)$ and write $\lambda^c(x) = \lambda(cxc^{-1})$. We then consider the anti-cyclotomic character α attached to λ_* given by

$$\alpha(x) = \lambda_*^{-1}\lambda_*^c(x) = \lambda_*(cxc^{-1}x^{-1})$$

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721267.011
Cambridge Books Online © Cambridge University Press, 2009

and the corresponding Λ-algebra homomorphism

$$\alpha_* : \mathfrak{O}[[\mathbf{G}]] \to \mathfrak{O}[[\mathbf{W}]].$$

This α_* actually has values in the anti-cyclotomic part $\mathfrak{O}[[\mathbf{W}^-]]$, where

$$\mathbf{W}^- = \{w \in \mathbf{W} \mid w^c = cwc^{-1} = w^{-1}\}.$$

Then we define

$$L^- = \alpha_*(L) \in \mathfrak{O}_\Omega[[\mathbf{W}^-]].$$

Although the divisibility of Theorem 2.1 is stated as taking place in the bigger ring $\mathfrak{O}[[\mathbf{W}]] \supset \mathfrak{O}[[\mathbf{W}^-]]$, actually the congruence power series H itself also falls in the subring $\mathfrak{O}[[\mathbf{W}^-]]$. However we will know this fact *after* proving the second divisibility: $H \mid (h(M)/h(F))Iw^-$ and we do not know this fact *a priori.* Thus we continue to formulate our result using $\mathfrak{O}_\Omega[[\mathbf{W}]]$ as the base ring. This power series L^- satisfies the following interpolation property:

$$\frac{L^-(P)}{p\text{-adic period}} = c(\lambda_P^c\lambda_P^{-1})\frac{L(0,\lambda_P^c\lambda_P^{-1})}{\text{complex period}}$$

whenever P is arithmetic and $\lambda_P^c\lambda_P^{-1}$ is critical at P.

We now define the p-adic Hecke algebra and the congruence power series and then give a sketch of the proof of the theorem. To define Hecke algebra, we explain first a few things about Hilbert modular forms. Let I be the set of all field embeddings of F into $\overline{\mathbf{Q}}$. The weight $k = (k_\sigma)_{\sigma\in I}$ of a modular form will be an element of the free $\mathbf{Z}$-module $\mathbf{Z}[I]$ generated by elements of I. Actually, our holomorphic modular forms have double digit weight $(k,v) \in \mathbf{Z}[I]^2$ associated to the following automorphic factor:

$$J_{k,v}(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) = \Pi_{\sigma\in I}\{\det(\gamma_\sigma)^{v_\sigma - 1}(c^\sigma z_\sigma + d^\sigma)^{k_\sigma}\},$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F_\infty)$ ($F_\infty = F \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{R}^I$) with totally positive determinant and $z = (z_\sigma)_{\sigma\in I} \in \mathfrak{H}^I$ is a variable on the product of copies of upper half complex planes $\mathfrak{H}^I$ indexed by I. For each open compact subgroup V of the finite part of the adele group $GL_2(F_A)$, let $S_{k,v}(V)$ be the space of holomorphic cusp forms f of weight (k,v) defined in [H1, §2]. Namely f is a function on $GL_2(F_A)$ satisfying

$$f(\alpha x u) = f(x)J_{k,v}(u_\infty, z_0)^{-1} \quad \text{for} \quad \alpha \in GL_2(F) \quad \text{and} \quad u \in V \times C,$$

where C is the stabilizer of $z_0 = (\sqrt{-1}, \dots, \sqrt{-1}) \in \mathfrak{H}^I$ in $GL_2(F_\infty)$, which is isomorphic to the product of the center ($\cong (\mathbf{R}^\times)^I$) of $GL_2(F_\infty)$ and $SO_2(\mathbf{R})^I$.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

We can associate to f and each finite idele $t \in GL_2(F_{A_f})$, a function f_x on $\mathfrak{H}^I$ by

$$f_t(z) = f(t\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix})J_{k,v}(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}, z_0).$$

It is easy to check that f_t satisfies the automorphic condition:

$$f_t(\gamma(z)) = f_t(z)J_{k,v}(\gamma, z) \quad \text{for} \quad \gamma \in \Gamma_t = t^{-1}VtGL_2^+(F_\infty) \cap GL_2(F),$$

where $GL_2^+(F_\infty)$ is the connected component of $GL_2(F_\infty)$ with identity. Similarly we write $F_{\infty+}^\times$ for the connected component with identity of $F_\infty^\times$. Then we suppose for $f \in S_{k,v}(V)$ that, for all $t \in GL_2(F_{A_f})$,

(i) f_t is holomorphic on $\mathfrak{H}^I$ (holomorphy),
(ii) $f_t(z)$ has the following Fourier expansion:

$$\Sigma_{\xi \in F}\ c(\xi, f_t)\exp(2\pi i \mathrm{Tr}(\xi z))$$

with $c(\xi, f_t) = 0$ unless $\xi^\sigma > 0$ for all $\sigma \in I$ (cuspidality).

Let D be the relative discriminant of M/F and let $\mathfrak{r}$ and $\mathfrak{R}$ be the integer ring of F and M, respectively. As the open compact subgroup V, we take the group V_α given by

$$\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\hat{\mathfrak{r}}) \mid c \in Dp^\alpha\hat{\mathfrak{r}}, \quad a \equiv 1 \bmod p^\alpha\hat{\mathfrak{r}}, \quad d \equiv 1 \bmod Dp^\alpha\hat{\mathfrak{r}}\},$$

where $\mathfrak{r}$ is the integer ring of F and $\hat{\mathfrak{r}} = \varprojlim_N \mathfrak{r}/N\mathfrak{r}$ is the product of $\mathfrak{l}$-adic completion of $\mathfrak{r}$ over all primes $\mathfrak{l}$. Let $\chi : F_A^\times/F^\times \to \mathbf{Z}_p^\times$ be the cyclotomic character. If $c(\xi, f_t) \in \overline{\mathbf{Q}}$ for all $t \in GL_2(F_{A_f})$, we can associate to each f as above the following p-adic q-expansion (cf. [H4, §1]):

$$f(y) = \Sigma_{0 \ll \xi \in F}\ a(\xi yd, f)q^\xi \quad \text{with} \quad a(\xi yd, f) \in \overline{\mathbf{Q}}_p,$$

where d is any differental idele of F (i.e., its ideal is the different of $F/\mathbf{Q}$) and $y \mapsto a(y, f)$ is a function on finite ideles, vanishing outside integral ideles, given by

$$a(y, f) = c(\xi, f_t)y_p^{-v}\xi^v\chi(\det(t)) \quad \text{for} \quad t = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$
$$\text{with} \quad y \in \xi ad(V_\alpha \cap F_{A_f}^\times)F_{\infty+}^\times.$$

Out of this q-expansion, we can recover the Fourier expansion of f:

$$f\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) = |y|_A\{\Sigma_{0 \ll \xi \in F}\ a(\xi yd, f)(\xi dy)_p^v(\xi y_\infty)^{-v}\mathbf{e}_F(i\xi y_\infty)\mathbf{e}_F(\xi x)\}.$$

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721267.011
Cambridge Books Online © Cambridge University Press, 2009

Here note that $a(\xi yd, f)(\xi dy)_p^v$ is an algebraic number which is considered to be a complex number via the fixed embedding of $\overline{\mathbf{Q}}$ into $\mathbf{C}$. When $a(y, f)$ is algebraic for all y with $y_p = 1$, f is called algebraic (this is equivalent to asking that $c(\xi, f_t)$ are algebraic for all t). We consider the union $S(\overline{\mathbf{Q}})$ of all algebraic forms of all weight (k, v) inside the space of formal q-expansions. Then putting a p-adic uniform norm

$$|f|_p = \mathrm{Sup}_y |a(y, f)|_p$$

on $S(\overline{\mathbf{Q}})$, we define the space S of p-adic modular forms by the completion of $S(\overline{\mathbf{Q}})$ under the norm $|\ \ |_p$.

Now we define the Hecke operators. For each $x \in F_A^\times$ with $x_\infty = 1$, we can define the Hecke operator $T(x) = T_\alpha(x)$ acting on $S_{k,v}(V_\alpha)$ as follows: First take the double coset $V_\alpha \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} V_\alpha$ and decompose it into a disjoint union of finite right cosets $\cup_i x_i V_\alpha$. Then we define $T_\alpha(x)$ by

$$f \mid T_\alpha(x)(g) = \Sigma_i f(gx_i).$$

Since we have taken the average of right translation of f on a double coset, we can check easily that $T_\alpha(x)$ is a linear operator acting on $S_{k,v}(V_\alpha)$. Especially the action of $T(u)$ for $u \in \mathfrak{r}_p^\times$ factors through $(\mathfrak{r}/p^\alpha\mathfrak{r})^\times$. Similarly, the center $F_A^\times$ acts on $S_{k,v}(V_\alpha)$ so that $f \mid z(g) = f(gz)$. This action factors through $Z = F_A^\times / \overline{F^\times U(D)^{(p)} F_\infty^\times}$ for

$$U(D)^{(p)} = \{u \in \hat{\mathfrak{r}}^\times \mid u \equiv 1 \bmod D\hat{\mathfrak{r}} \text{ and } u_p = 1\}.$$

Thus $S_{k,v}(V_\alpha)$ has an action of the group $G = Z \times \mathfrak{r}_p^\times$ and Hecke operators $T(x)$. The group G is a profinite group and we can decompose

$$G = G_{\mathrm{tor}} \times W$$

so that $W \cong \mathbf{Z}_p^{[F:\mathbf{Q}]+1+\delta}$ and G_{tor} is a finite group. Since $M_A \supset F_A$, we have a natural homomorphism of Z into $\mathbf{G}$. On the other hand, by our choice of p-adic CM-type, we can identify $\mathfrak{r}_p = \mathfrak{r} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ with $\mathfrak{R}_S = \Pi_{\mathfrak{P} \in S} \mathfrak{R}_{\mathfrak{P}}$. This identification gives an injection of $\mathfrak{r}_p^\times$ into $M_A^\times$ and yields a homomorphism of $\mathfrak{r}_p^\times$ into $\mathbf{G}$. Thus we have natural morphisms:

$$\iota : G = Z \times \mathfrak{r}_p^\times \to \mathbf{G} \quad \text{and} \quad \iota_* : \mathfrak{O}[[G]] \to \mathfrak{O}[[\mathbf{G}]].$$

We can easily check that ι takes W into a subgroup of finite index of $\mathbf{W}$ and ι_* is an $\mathfrak{O}[[\mathbf{W}]]$-algebra homomorphism.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

We take the Galois closure Φ of F in $\overline{\mathbf{Q}}$ and let $\mathfrak{W}$ be the valuation ring of Φ corresponding to the embedding Φ into $\overline{\mathbf{Q}}_p$. We pick an element $\varpi_\mathfrak{p}$ for each prime factor $\mathfrak{p}$ of p in F such that $\varpi_\mathfrak{p}\mathfrak{r} = \mathfrak{p}\mathfrak{a}$ for an ideal $\mathfrak{a}$ prime to p. We consider $\varpi_\mathfrak{p}$ as a prime element in $F_\mathfrak{p}$. Then the p-adic Hecke algebra $\mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{W})$ with coefficients in $\mathfrak{W}$ is by definition the $\mathfrak{W}$-subalgebra of $\mathrm{End}_\mathfrak{W}(S_{k,v}(V_\alpha))$ generated by

(a) Hecke operators $T(x)$ for all $x \in \hat{\mathfrak{r}} \cap F_{A_f}^\times$,
(b) the Hecke operator $\varpi_\mathfrak{p}^{-v}T(\varpi_\mathfrak{p})(\varpi_\mathfrak{p} \in \mathfrak{r}_\mathfrak{p})$ for all $\mathfrak{p} \mid p$,
(c) the action of the group $G = Z \times \mathfrak{r}_p^\times$.

It is well known that $\mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{W})$ is free of finite rank over $\mathfrak{W}$ (cf [H1, Th.3.1]). Especially $T(\varpi_\mathfrak{p})$ is divisible by $\varpi_\mathfrak{p}^v = \Pi_{\sigma\in I}\varpi_\mathfrak{p}^{\sigma v_\sigma}$. For each extension K of $\mathbf{Q}_p$ containing Φ, let $\mathfrak{O}$ be the p-adic integer ring of K. Then the p-adic Hecke algebra of level Dp^α is defined by

$$\mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{O}) = \mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{W}) \otimes_\mathfrak{W} \mathfrak{O}.$$

By definition, the restriction of $T_\beta(x)$ acting on $S_{k,v}(V_\beta)$ to $S_{k,v}(V_\alpha)$ for $\beta > \alpha > 0$ coincides $T_\alpha(x)$. Thus the restriction induces a surjective $\mathfrak{O}$-algebra homomorphism:

$$\mathbf{h}_{k,v}(Dp^\beta;\mathfrak{O}) \to \mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{O})$$

which takes $T_\beta(x)$ to $T_\alpha(x)$. Thus we can take the projective limit

$$\mathbf{h}_{k,v}(Dp^\infty;\mathfrak{O}) = \varprojlim_\alpha \mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{O}),$$

which is naturally an algebra over the continuous group algebra $\mathfrak{O}[[G]]$. For each α, we can decompose

$$\mathbf{h}_{k,v}(Dp^\alpha;\mathfrak{O}) = \mathbf{h}_{k,v}^{n.\mathrm{ord}}(Dp^\alpha;\mathfrak{O}) \times \mathbf{h}_{k,v}^{s}(Dp^\alpha;\mathfrak{O})$$

so that $p^{-v}T(p)$ is a unit in $\mathbf{h}_{k,v}^{n.\mathrm{ord}}(Dp^\alpha;\mathfrak{O})$ and is topologically nilpotent in $\mathbf{h}_{k,v}^{s}(Dp^\alpha;\mathfrak{O})$. Then basic known facts are (see [H2]):

(H1) The pair $(\mathbf{h}_{k,v}(Dp^\infty;\mathfrak{O}), x_p^{-v}T(x))$ is independent of (k,v) if $k \geq 2t$, where $t = \Sigma_{\sigma\in I}\sigma$.

In fact, the union $S_{k,v}(V_\infty) = \cup_\alpha S_{k,v}(V_\alpha;\overline{\mathbf{Q}})$ of all algebraic modular forms of weight (k,v) is dense in S and thus the algebra $\mathbf{h}_{k,v}(Dp^\infty;\mathfrak{O})$ can be considered as a subalgebra of $\mathrm{End}(S)$ topologically generated by $x_p^{-v}T(x)$ and it is independent of (k,v). Now we can remove the suffix (k,v) from notation of the Hecke algebra and we write $\mathbf{h}(D;\mathfrak{O})$ (resp. $\mathbf{h} = \mathbf{h}^{n.\mathrm{ord}}(D;\mathfrak{O})$)

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

for $\mathbf{h}_{k,v}(Dp^\infty;\mathfrak{O})$ (resp. $\mathbf{h}_{k,v}^{n.\mathrm{ord}}(Dp^\infty;\mathfrak{O})$). In other words, there is a universal Hecke operator $\mathbf{T}(x) \in \mathbf{h}(D;\mathfrak{O})$ which is sent to $x_p^{-v}T(x)$ under the isomorphism: $\mathbf{h}(D;\mathfrak{O}) \cong \mathbf{h}_{k,v}(Dp^\infty;\mathfrak{O})$.

(H2) $\mathbf{h}$ is of finite type and torsion-free as $\mathfrak{O}[[W]]$-module.

(H3) There exists an $\mathfrak{O}[[W]]$-algebra homomorphism $\theta^* : \mathbf{h} \to \mathfrak{O}[[\mathrm{G}]]$ such that for primes outside Dp

$$\theta^*(T(\mathfrak{q})) = \begin{cases} [\mathfrak{Q}] + [\mathfrak{Q}^c] & \text{if } \mathfrak{q} = \mathfrak{Q}\mathfrak{Q}^c, \\ 0 & \text{if } \mathfrak{q} \text{ remains prime in } M \end{cases}$$

where $[\mathfrak{Q}]$ is the image of the prime ideal $\mathfrak{Q}$ under the Artin symbol.

This statement is just an interpretation of the existence of theta series $\theta(\varphi)$ for each A_0-type Hecke character φ of $\mathbf{G}$ characterized by

$$\theta(\varphi) \mid T(\mathfrak{q}) = \begin{cases} (\varphi(\mathfrak{Q}) + \varphi(\mathfrak{Q}^c))\theta(\varphi) & \text{if } \mathfrak{q} = \mathfrak{Q}\mathfrak{Q}^c, \\ 0 & \text{if } \mathfrak{q} \text{ remains prime in } M. \end{cases}$$

By (H3), we may consider the composite $\lambda_* \circ \theta^* : \mathbf{h} \to \Lambda$.

(H4) After tensoring the quotient field $\mathbf{L}$ of Λ over $\Lambda_0 = \mathfrak{O}[[\mathbf{W}]]$, we have a Λ_0-algebra decomposition

$$\mathbf{h} \otimes_{\Lambda_0} \mathbf{L} \cong \mathbf{L} \oplus \mathbf{B} \quad \text{for a complementary summand } \mathbf{B},$$

where the projection to the first factor is given by $\lambda_* \circ \theta^*$.

Then the congruence module of λ_* is defined by

(H5) $\mathfrak{C}(\lambda_*;\Lambda) = \Lambda/(\mathbf{h} \otimes_{\Lambda_0} \Lambda \cap \mathbf{L})$.

The congruence power series H is then defined by the characteristic power series of $\mathfrak{C}(\lambda_*;\Lambda)$. By definition, the principal ideal $H\Lambda$ is the reflexive closure of the ideal $\mathbf{h} \otimes_{\Lambda_0} \Lambda \cap \mathbf{L}$ in Λ.

3. We now give a sketch of the proof of Theorem 2.1. The idea of the proof is the comparison of two p-adic interpolations of Hecke L-functions of M. One is Katz's way and the other is the p-adic L-function attached to the Rankin product L-function of $\theta(\lambda_P)$ and $\theta(\mu_Q)$. Here μ is another character of $\mathbf{G}_{\mathrm{tor}}$ and we extend it to a character $\mu_* : \mathbf{G} \to \Lambda^\times$ similarly to λ_*. In fact, we can show by the method of p-adic Rankin convolution ([H4, Theorem I]) that there exists a power series Δ in $\mathfrak{O}[[\mathbf{W} \times \mathbf{W}]]$ such that

$$\frac{\Delta(P,Q)}{H(P)} = c(P,Q)\frac{D(1+\frac{m(Q)-m(P)}{2}, \theta(\lambda_P), \theta(\mu_Q \circ c))}{(\theta(\lambda_P), \theta(\lambda_P))}$$

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

whenever both P and Q are arithmetic and both $\lambda_P^{-1}\mu_Q$ and $\lambda_P^{-1}(\mu_Q^c)$ are critical. Here $D(s,\theta(\lambda_P),\theta(\mu_Q)^c)$ is the Rankin product of $\theta(\lambda_P)$ and $\theta(\mu_Q)^c$, i.e., the standard L-function for $GL(2)\times GL(2)$ attached to the tensor product of automorphic representations spanned by $\theta(\lambda_P)$ and $\theta(\mu_Q)^c$; $(\theta(\lambda_P),\theta(\lambda_P))$ is the self Petersson inner product of $\theta(\lambda_P)$ and $c(P,Q)$ is a simple constant including the modifying Euler p-factor, Gauss sums, Γ-factors and a power of π. The integer $m(P)$ is given as follows: Write the infinity type of λ_P as ξ and $m(P)=\xi_\sigma+\xi_{\sigma\rho}$ for $\sigma\in\Sigma$ (this value is independent of σ). Similarly $m(Q)$ is defined for μ_Q. Now looking at the Euler product of D and the functional equation of Hecke L-functions, we see

$$D\Big(1+\frac{m(Q)-m(P)}{2},\theta(\lambda_P),\theta(\mu_Q^c)\Big)\approx L(0,\lambda_P^{-1}\mu_Q)L(0,\lambda_P^{-1}\mu_Q^c).$$

It is also well known that, with a simple constant $c(P)$ similar to $c(P,Q)$,

$$(\theta(\lambda_P),\theta(\lambda_P))=c(P)(2^{1-[F:\mathbf{Q}]}h(M)/h(F))L(0,\lambda_P^c\lambda_P^{-1}).$$

Modifying the Katz measure L in $\mathfrak{O}[[\mathbf{G}]]$, we can find two power series L' and L'' in $\mathfrak{O}[[\mathbf{W}\times\mathbf{W}]]$ interpolating $L(0,\lambda_P^{-1}\mu_Q)$ and $L(0,\lambda_P^{-1}\mu_Q^c)$, respectively. Then out of the above formulas, we get the following identity:

$$\frac{\Delta}{H}=U\frac{L'L''}{2^{1-[F:\mathbf{Q}]}h(M)/h(F))L^-}\quad\text{in }\mathfrak{O}[[\mathbf{W}\times\mathbf{W}]],$$

where U is a unit in $\mathfrak{O}[[\mathbf{W}\times\mathbf{W}]]$. Thus if L' and L'' are prime to L^- in $\mathfrak{O}[[\mathbf{W}\times\mathbf{W}]]\otimes_{\mathbf{Z}}\mathbf{Q}$, we get the desired divisibility. Almost immediately from the construction of L' and L'', we know that for any character $P\in\mathfrak{X}(\mathbf{W})$ the half specialized power series $L'_P(X)=L'(P,X)$ and $L''_P(X)$ in $\mathfrak{O}[[\mathbf{W}]]$ have their μ-invariants *independent* of P, equal to the μ-invariant of the Katz measure along the irreducible component of $\lambda^{-1}\mu$ and $\lambda^{-1}\mu^c$. If (a characteristic 0) prime factor $\mathbf{P}(Y)$ (in $\mathfrak{O}_\Omega[[\mathbf{W}]]$) of $L^-(Y)$ divides L', then by letting P approach to a zero of $\mathbf{P}$, we observe that the μ-invariant of L'_P goes to infinity, which contradicts the constancy of the μ-invariant of L'_P. Thus L^- is prime to $L'L''$ in $\mathfrak{O}[[\mathbf{W}\times\mathbf{W}]]\otimes_{\mathbf{Z}}\mathbf{Q}$, which shows the desired assertion. Especially if the μ-invariant of the Katz measure vanishes, then we know the strong divisibility as in the theorem.

4. Now we explain briefly how one can show the other divisibility: $H\mid Iw^-$ by using Mazur's theory of deformation of Galois representations. We keep the notations and assumptions introduced above. In particular, we assume the ordinarity hypothesis and fix a p-adic CM-type S. To the pair (S,λ), where λ is a given character of $\mathbf{G}_{\mathrm{tor}}$, we attached a congruence module, with characteristic power series H. On the other hand, let M_∞ be the maximal abelian

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

extension of M unramified outside p of M; so, we have $\mathbf{G} = \mathrm{Gal}(M_\infty/M)$. We have defined a character $\lambda_* : \mathbf{G} \to \Lambda^\times$ for $\Lambda = \mathfrak{O}[[\mathbf{W}]]$ for a fixed finite order character $\lambda : \mathbf{G}_{\mathrm{tor}} \to \mathfrak{O}^\times$. In fact, on $\mathbf{G}_{\mathrm{tor}}$, λ_* coincides with λ and on $\mathbf{W}$, it is the tautological inclusion of $\mathbf{W}$ into Λ. Define the '$-$' part of λ_*, which we write as $\alpha = \alpha_\lambda$, by

$$\alpha = \lambda_*(\lambda_*^c)^{-1} \quad \text{for } \lambda_*^c(\sigma) = \lambda_*(c\sigma c^{-1}).$$

Let $M^- = M^-(\lambda_-)$ be the fixed part of M_∞ by $\mathrm{Ker}(\alpha)$, which contains $\mathbf{G}^+ = \{\sigma \in \mathbf{G} \mid c(\sigma) = \sigma\}$. We write $\mathbf{H} = \mathrm{Gal}(M^-(\lambda_-)/M) \cong \mathrm{Im}(\alpha)$. Let $\mathbf{M}_S(\lambda_-)$ be the maximal p-abelian extension of M^- unramified outside S. One can prove, under a weak Leopoldt type assumption for the extension $M^-(\lambda_-)/M$ (for details of this assumption, see our forthcoming paper), that $X_S = \mathrm{Gal}(\mathbf{M}_S(\lambda_-)/M^-)$ is torsion over $\mathbf{Z}_p[[\mathbf{H}]]$. The character $\lambda^- = \lambda/\lambda^c$: $\mathbf{G}_{\mathrm{tor}} \to \mathfrak{O}^\times$ factors through the torsion part $\mathbf{H}_{\mathrm{tor}}$ of $\mathbf{H}$ and the characteristic power series of the λ^--part $X_S(\lambda^-) = X_S \otimes_{\mathbf{Z}_p[\mathbf{H}_{\mathrm{tor}}]} \mathfrak{O}(\lambda^-)$ of X_S is nothing but Iw^-. Then the precise result, we can obtain at this date is as follows:

Theorem 4.1 (i) If $[F:\mathbf{Q}] > 1$, H divides $(h(M)/h(F))Iw^-$ in $\mathfrak{O}[[\mathbf{W}]]$.
(ii) If M is imaginary quadratic, then H divides $h(M)Iw^-$ in $\mathfrak{O}[[\mathbf{W}]]$ unless $\lambda^- = \lambda/\lambda^c$ restricted to the decomposition group D of $\mathfrak{P}$ in $\mathbf{G}$ is congruent to 1 modulo the maximal ideal $\pi\mathfrak{O}$ of $\mathfrak{O}$. In this exceptional case, we need to exclude the trivial zero, i.e., the divisibility holds in $\mathfrak{O}[[\mathbf{W}]][\frac{1}{P_\lambda}]$, where P_λ is a generator of the unique height one prime ideal corresponding to the character $\tau_\lambda : \mathbf{H} \to \mathfrak{O}^\times$ such that $\tau_\lambda(D) = 1$ and $\tau_\lambda \mid \mathbf{H}_{\mathrm{tor}} = \lambda^-$.

Comments (a) By a base change argument in Iwasawa theory, one can probably include the 'trivial zero' P_λ. Nevertheless, the argument possibly needs a sort of multiplicity one result for 'trivial zeros' of the Katz–Yager p-adic L-function which needs to be verified.

(b) The reason why things become easier when $[F:\mathbf{Q}] > 1$ is contained in the following easy lemma. To state the lemma, let us recall the character $\lambda_* : G \to \mathfrak{O}[[\mathbf{W}]]$ given by

$$\lambda_*(g, w) = \lambda(g)w \in \mathfrak{O}[[\mathbf{W}]] \quad \text{for } g \in \mathbf{G}_{\mathrm{tor}} \text{ and } w \in \mathbf{W} \text{ in §2.}$$

Lemma 4.2 (i) If $[F:\mathbf{Q}] > 1$, the ideal $\mathfrak{I}$ generated by the values $\lambda_*(\sigma) - \lambda_*(c(\sigma))$, σ running over the decomposition group $D_\mathfrak{p}$ at $\mathfrak{p}$ in $\mathbf{G}$ is of height greater than 1, i.e., is not contained in any prime of height one in $\Lambda = \mathfrak{O}[[\mathbf{W}]]$.
(ii) If $F = \mathbf{Q}$, this ideal is contained in $P_\lambda\Lambda$.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.013
Cambridge Books Online © Cambridge University Press, 2009

The outline of the proof of Theorem 4.1 runs as follows. Let us fix a prime P of height one such that the restrictions of λ and λ^c to $D_\mathfrak{p}$ are not congruent modulo P for all prime $\mathfrak{p}$ in F over p (by Lemma 4.2, this gives no restriction when $[F:\mathbb{Q}] \geq 2$). We consider the complete discrete valuation ring Λ_P with residue field $k(P)$ and look at the residual representation

$$\overline{\rho}_0 : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(k(P))$$

given as the reduction modulo P of the induced representation ρ_0 of $\lambda_* : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \Lambda^\times$. By the choice of P, $\lambda \not\equiv \lambda^c \bmod P$, hence $\overline{\rho}_0$ is irreducible. The main step in the proof of Theorem 4.1 is to relate $X_S(\lambda^-) \otimes_\Lambda \Lambda_P$ to a module of Kähler differentials attached to some deformation problem of $\overline{\rho}_0$ over Λ_P. Since $k(P)$ is not a finite field, the study of this deformation problem, though very similar to the one made by B. Mazur in [M], is slightly trickier. To define this problem, we need to introduce some notations. First, let N be the ray class field of M of conductor p (one has of course N inside M_∞) and $N^{(p)}$ be the maximal p-extension of N unramified outside p. It is clear that $\overline{\rho}_0$ restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/N)$ factors through $\Pi_N = \mathrm{Gal}(N^{(p)}/N)$, so that, for the deformation problem of $\overline{\rho}_0$, we can restrict ourselves to representations ρ of $\Pi = \mathrm{Gal}(N^{(p)}/F)$. The great advantage of such a limitation in the choice of ρ's is that Π is topologically of finite type (Π_N is a pro-p-group and its Frattini quotient is finite by Kummer theory over N). Now, let Art be the category of local artinian Λ_P-algebras with residue field $k(P)$, Sets the category of sets and $\mathfrak{F}$ the covariant functor

$$\mathfrak{F} : \mathsf{Art} \to \mathsf{Sets}$$

given for $A \in Ob(\mathsf{Art})$ with maximal ideal $\mathfrak{m}_A$ by

$$\mathfrak{F}(A) = \{\rho : \Pi \to GL_2(A) \mid \rho \text{ is finitely continuous and } \\ \rho \bmod \mathfrak{m}_A = \overline{\rho}_0\}/\approx .$$

Here (i) '$\approx$' denotes the strict equivalence of representations, that is, conjugation by a matrix in $GL_2(A)$ congruent to 1 modulo $\mathfrak{m}_A$.

(ii) The phrase 'finitely continuous' means that there exists a Λ-submodule L in A^2 of finite type stable by ρ generating A^2 over Λ_P. The reason for this definition instead of usual P-adic continuity is that Λ_P is not locally compact for the P-adic topology, but Π is even compact. Hence a P-adically continuous representation should have a very small image, and in some sense, we look for representations with open image (over Λ). Note that a finitely continuous representation induces a continuous representation: $\Pi \to GL(L)$, L being endowed with the usual $\mathfrak{m}$-adic topology for the maximal ideal $\mathfrak{m}$ of Λ.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

This notion of 'finite continuity' does not depend on the choice of the lattice L by the Artin–Rees lemma. We can extend this notion of finite continuity to any map u of Π to an A-module V requiring that u having values in a Λ-finite submodule L in V and the induced map $u : \Pi \to L$ is continuous under the $\mathfrak{m}$-adic topology on L. This generalized notion will be used later to define finitely continuous cohomology.

By using the fact that $\overline{\rho}_0$ is induced from a finitely continuous character: $\Pi \to k(P)^\times$, it is not so difficult to check by Schlessinger's criterion the following fact:

Theorem 4.3 The functor $\mathfrak{F}$ is pro-representable; that is, there exists a unique universal couple (R', ρ') where R' is a local noetherian complete Λ_P-algebra with residue field $k(P)$ and $\rho' \in \mathfrak{F}(R') = \varprojlim_\alpha \mathfrak{F}(R'/\mathfrak{m}_{R'}^\alpha)$.

Comments a) The 'continuity' property ρ' enjoys should be called 'profinite continuity', meaning that for any artinian quotient $\varphi : R' \to A$ of R', $\varphi \circ \rho'$ is finitely continuous. There is also an obvious notion of profinite continuity of maps from Π to any Λ_P-module.

b) It is natural to ask for the pro-representability of this problem starting from an *arbitrary* irreducible finitely continuous representation $\overline{\rho}_0$. The answer is not known in general because of the lack of a cohomology theory adapted to finite continuous representations and subgroups of $GL_2(k(P))$. Such theory is available when $k(P)$ is a p-adic field, due to Lazard [L], and allows us to give a positive answer in this case. See Appendix below.

In fact, the universal ring we need is smaller than R'. It will pro-represent a subfunctor $\mathfrak{F}_S$ of $\mathfrak{F}$ requiring local conditions at primes of F above p (these conditions involve the choice we made of a p-adic CM-type S). We call this problem the *S-nearly ordinary* deformation problem of $\overline{\rho}_0$. For $\mathfrak{P}$ in S, recalling $\mathfrak{p} = \mathfrak{P} \cap F$, we choose $D_\mathfrak{p}$ so that $D_\mathfrak{p}$ is the decomposition group of $\mathfrak{P}$ in $\Pi_M = \mathrm{Gal}(N^{(p)}/M)$. A strict equivalence class $[\rho]$ in $\mathfrak{F}(A)$ belongs to $\mathfrak{F}_S(A)$ if and only if for any representative ρ, the following conditions are satisfied:

(4.1a) For each prime $\mathfrak{p}$ above p in F, there exists a finitely continuous character $\delta_\mathfrak{p} : D_\mathfrak{p} \to A^\times$ such that ρ restricted to $D_\mathfrak{p}$ is equivalent (but not necessarily strictly) to $\begin{pmatrix} * & * \\ 0 & \delta_\mathfrak{p} \end{pmatrix}$;

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

(4.1b) $\delta_{\mathfrak{p}}$ is congruent modulo $\mathfrak{m}_A$ to the restriction of λ_*^c to $D_{\mathfrak{p}}$ and $\delta_{\mathfrak{p}}$ restricted to the inertia subgroup $I_{\mathfrak{p}}$ of $D_{\mathfrak{p}}$ coincides with the restriction to $I_{\mathfrak{p}}$ of λ_*^c;

(4.1c) $\det(\rho) = \det(\rho_0)$ (considered as having values in A via the structural morphism: $\Lambda \to \Lambda_P \to A$).

One can deduce from Theorem 4.3 that $\mathfrak{F}_S$ is pro-representable. We denote by (R_S, ρ_S) the corresponding universal couple. Let us define a Λ_P-module $\mathfrak{W}_P$ by

$$\mathfrak{W}_P = \cup_{m=1}^{\infty} P^{-m}\Lambda_P/\Lambda_P = \mathbf{L}/\Lambda_P,$$

where $\mathbf{L}$ is the quotient field of Λ. Then $\mathfrak{W}_P$ is the injective envelope of $k(P)$. We consider the algebra $R_S[\mathfrak{W}_P] = R_S \oplus \mathfrak{W}_P$ with $\mathfrak{W}_P^2 = 0$. One can consider, by abusing the notation, $\mathfrak{F}_S(R_S[\mathfrak{W}_P])$. Namely $\mathfrak{F}_S(R_S[\mathfrak{W}_P])$ is a set of profinitely continuous deformations of $\overline{\rho}$ satisfying the above conditions (i), (ii) and (iii). Since Π is topologically finitely generated, by the profinite continuity, ρ has image in a noetherian subring $R_m = R_S[P^{-m}\Lambda_P/\Lambda_P]$ for sufficiently large m. Thus we have a local Λ-algebra homomorphism φ_ρ : $R_S \to R_S[\mathfrak{W}_P]$ such that $\rho \approx \varphi_\rho \circ \rho_S$. Now we consider the subset

$$\mathfrak{F}_0(R_S[\mathfrak{W}_P]) = \{\rho \in \mathfrak{F}_S(R_S[\mathfrak{W}_P]) \mid \rho \bmod \mathfrak{W}_P = \rho_S\}.$$

We also define $\mathsf{Sect}_\Lambda(R_S[\mathfrak{W}_P]/R_S)$ to be the set of continuous sections (under the $\mathfrak{m}_{R_S}$-adic topology) $\varphi : R_S \to R_S[\mathfrak{W}_P]$ as R_S-algebras whose projection to $\mathfrak{W}_P$ is contained in $P^{-m}\Lambda_P/\Lambda_P$ for m sufficiently large. We put

$$sl_2(\mathfrak{W}_P) = \{x \in M_2(\mathfrak{W}_P) \mid \mathrm{Tr}(x) = 0\},$$

which is a module over Π under the action: $\sigma x = \rho_S(x) x \rho_S(x)^{-1}$. We consider the cohomology group $H^1(\Pi, sl_2(\mathfrak{W}_P))$, which is the quotient of the module of profinitely continuous 1-cocycles on Π having values in $sl_2(P^{-m}\Lambda_P/\Lambda_P)$ for sufficiently large m modulo usual coboundaries. In fact, for each $\rho \in \mathfrak{F}_S(R_S[\mathfrak{W}_P])$, $\varphi_\rho : R_S \to R_S[\mathfrak{W}_P]$ is a Λ-algebra homomorphism. If $\rho \in \mathfrak{F}_0(R_S[\mathfrak{W}_P])$, then by the fact that $\rho \bmod \mathfrak{W}_P = \rho_S$, $\pi \circ \varphi = \mathrm{id}_{R_S}$. Thus we have a morphism: $\mathfrak{F}_0(R_S[\mathfrak{W}_P]) \to \mathsf{Sect}_\Lambda(R_S[\mathfrak{W}_P]/R_S)$. This morphism is of course a surjective isomorphism because for $\varphi \in \mathsf{Sect}_\Lambda(R_S[\mathfrak{W}_P]/R_S)$, $\varphi \circ \rho_S$ is an element of $\mathfrak{F}_0(R_S[\mathfrak{W}_P])$. Therefore we know that

$$(4.2) \qquad \mathfrak{F}_0(R_S[\mathfrak{W}_P]) \cong \mathsf{Sect}_\Lambda(R_S[\mathfrak{W}_P]/R_S).$$

For each $\mathfrak{p} \in \Sigma$, we can find $\alpha_{\mathfrak{p}} \in GL_2(R_S)$ such that

$$\alpha_{\mathfrak{p}}\rho_S(\sigma)\alpha_{\mathfrak{p}}^{-1} = \begin{pmatrix} * & * \\ 0 & \delta_{\mathfrak{p}}^S(\sigma) \end{pmatrix} \quad \text{for all } \sigma \in D_{\mathfrak{p}}$$
$$\text{and } \delta_{\mathfrak{p}}^S \equiv \lambda^c \bmod \mathfrak{m}_{R_S}.$$

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

We fix such a $\alpha_\mathfrak{p}$ for each $\mathfrak{p}$. Then we define the ordinary cohomology subgroup $H^1_{\mathrm{ord}}(\Pi, sl_2(\mathfrak{W}_P))$ by the subgroup of cohomology classes of cocycle u satisfying, for every $\mathfrak{p}$ dividing p in F,

$$\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \supset \alpha_\mathfrak{p} u(D_\mathfrak{p})\alpha_\mathfrak{p}^{-1} \quad \text{and} \quad \left\{\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}\right\} \supset \alpha_\mathfrak{p} u(I_\mathfrak{p})\alpha_\mathfrak{p}^{-1}.$$

Theorem 4.4 We have a canonical isomorphism:

$$\mathrm{Hom}_{R_S}(\Omega_{R_S/\Lambda_P}, \mathfrak{W}_P) \cong H^1_{\mathrm{ord}}(\Pi, sl_2(\mathfrak{W}_P)),$$

where the Kähler differential module Ω_{R_S/Λ_P} is defined to be the module of continuous differentials, i.e., $\Omega_{R_S/\Lambda_P} = I/I^2$ for the kernel I of the multiplication map of the completed tensor product $R_S \hat{\otimes}_{\Lambda_P} R_S$ (under the adic topology of the maximal ideal of $R_S \otimes_{\Lambda_P} R_S$) to R_S.

Proof For each $\rho \in \mathfrak{F}_0(R_S[\mathfrak{W}_P])$, we define $u : \Pi \to M_2(\mathfrak{W}_P)$ by

$$\rho(\sigma) = (1 \oplus u(\sigma))\rho_S(\sigma) \quad \text{for } \sigma \in \Pi.$$

Since ρ_S and ρ are both profinitely continuous, u has values in $P^{-m}\Lambda_P/\Lambda_p$ for sufficiently large m and is profinitely continuous. Then by (6.1c), we know that $\det(\rho_S) = \det(\rho)$. This shows that u has values in $sl_2(\mathfrak{W}_P)$. Similarly by (6.1b), we know that $\left\{\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}\right\} \supset \alpha_\mathfrak{p} u(I_\mathfrak{p})\alpha_\mathfrak{p}^{-1}$. By the multiplicativity: $\rho(\sigma)\rho(\tau) = \rho(\sigma\tau)$, we see easily that u is a cocycle and u is a coboundary if and only if $\rho \approx \rho_S$. Thus the map $\mathfrak{F}_0(R_S[\mathfrak{W}_P]) \to H^1_{\mathrm{ord}}(\Pi, sl_2(\mathfrak{W}_P))$ is injective. Surjectivity follows from the fact that we can recover a profinitely continuous representation out of a profinitely continuous cocycle by the above formula. Namely we know that

$$\mathfrak{F}_0(R_S[\mathfrak{W}_P]) \cong H^1_{\mathrm{ord}}(\Pi, sl_2(\mathfrak{W}_P)).$$

If we have a section $\varphi \in \mathsf{Sect}_\Lambda(R_S[\mathfrak{W}_P]/R_S)$, we can write $\varphi(r) = r \oplus d_\varphi(r)$. Then $d_\varphi \in \mathrm{Der}_\Lambda(R_S, \mathfrak{W}_P) = \mathrm{Hom}_{R_S}(\Omega_{R_S/\Lambda}, \mathfrak{W}_P)$. It is easy that from any derivation $d : R_S \to \mathfrak{W}_P$, we can reconstruct a section by the above formula. Thus we know that

$$\mathrm{Hom}_{R_S}(\Omega_{R_S/\Lambda}, \mathfrak{W}_P) \cong \mathsf{Sect}_\Lambda(R_S[\mathfrak{W}_P]/R_S)$$

which conclude the proof by (4.2).

We have an injection

$$\mathrm{res} : H^1(\Pi, sl_2(\mathfrak{W}_P)) \to H^1(\Pi_M, sl_2(\mathfrak{W}_P))^{\mathrm{Gal}(M/F)}.$$

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

Note that as Π_M-module, $sl_2(\mathfrak{W}_P) \cong \mathfrak{W}_P(\alpha) \oplus \mathfrak{W}_P(\alpha^{-1}) \oplus \mathfrak{W}_P$, where $\alpha = \lambda_*(\lambda_*^c)^{-1}$ and $\mathfrak{W}_P(\alpha) \cong \mathfrak{W}_P$ as Λ-module but Π acts via the one-dimensional abelian character α. The action of c interchanges $\mathfrak{W}_P(\alpha)$ and $\mathfrak{W}_P(\alpha^{-1})$ and acts by -1 on $\mathfrak{W}_P$. Thus we see

$$H^1(\Pi_M, sl_2(\mathfrak{W}_P))^{\mathrm{Gal}(M/F)} = H^1(\Pi_M, \mathfrak{W}_P(\alpha)) \oplus \mathrm{Hom}_{\mathrm{conti}}(\mathbf{G}/(1+c)\mathbf{G}, \mathfrak{W}_P).$$

Recall that $M^-(\lambda_-)/M$ is the extension corresponding to $\mathrm{Ker}(\alpha)$. The inclusion of $H^1(\Pi_M, \mathfrak{W}_P(\alpha))$ into $H^1(\Pi_M, sl_2(\mathfrak{W}_P))^{\mathrm{Gal}(M/F)}$ is given in terms of cocycle by the cocycle U such that $U(\sigma) = \begin{pmatrix} 0 & u(\sigma) \\ u({}^c\sigma) & 0 \end{pmatrix}$ for ${}^c\sigma = c\sigma c^{-1}$. From this, it follows, by the ordinarity condition,

$$\mathrm{res}_{\Pi_{M^-}}(u)(cI_{\mathfrak{P}}c^{-1}) = \mathrm{res}_{\Pi_{M^-}}(u)(I_{\mathfrak{P}^c}) = 0 \text{ for all } \mathfrak{P} \in S,$$

where $M^- = M^-(\lambda_-)$. Namely $\mathrm{res}_{\Pi_{M^-}}(u)$ is unramified outside S. Thus we have a natural map:

$$\mathrm{res} : H^1_{\mathrm{ord}}(\Pi_M, \mathfrak{W}_P(\alpha)) \to \mathrm{Hom}_H(X_S, \mathfrak{W}_P(\alpha)) = \mathrm{Hom}_{\Lambda_-}(X_S(\lambda^-), \mathfrak{W}_P).$$

Comments We omitted α from the module of extreme right, because the Λ_--module structure on $\mathfrak{W}_P$ given by α coincides with the natural structure given by the inclusion $\Lambda_- = \mathfrak{O}[[\mathbf{W}^-]]$ into Λ through the Λ-module structure of $\mathfrak{W}_P$. Moreover we can write the extreme right as

$$\mathrm{Hom}_{\Lambda_-}(X_S(\lambda^-), \mathfrak{W}_P) = \mathrm{Hom}_{\Lambda}(X_S(\lambda^-) \otimes_{\Lambda_-} \Lambda, \mathfrak{W}_P).$$

Thus the variable coming from the '+' part $\mathbf{W}^+$ in Λ is just a 'fake' and the divisibility we will obtain is in fact the divisibility in Λ_- although we have variables coming from $\mathbf{W}^+$ inside the Hecke algebra. This is natural because $X_S(\lambda^-)$ is a Λ_--module. The use of '+'-variables is inevitable because we do not know *a priori* that the congruence power series belongs to the '$-$' part. In the appendix, we prove that when $F = \mathbf{Q}$, the congruence power series belongs to the ordinary part of the Hecke algebra, which can be regarded as the '$-$' part in our situation.

It is not difficult to show that the above map: res. is injective; namely,

Corollary 4.5 $\mathrm{Hom}_{\Lambda}(X_S(\lambda^-) \otimes_{\Lambda_-} \Lambda, \mathfrak{W}_P) \supset H^1_{\mathrm{ord}}(\Pi_M, \mathfrak{W}_P(\alpha))$.

Since the inclusion of $\mathrm{Hom}_{\mathrm{conti}}(\mathbf{G}/(1+c)\mathbf{G}, \mathfrak{W}_P)$ into $H^1(\Pi_M, sl_2(I_P))^{\mathrm{Gal}(M/F)}$ is given in terms of cocycle by

$$\mathrm{Hom}_{\mathrm{conti}}(\mathbf{G}/(1+c)\mathbf{G}, \mathfrak{W}_P) \ni u \mapsto U(\sigma) = \begin{pmatrix} u(\sigma) & 0 \\ 0 & -u(\sigma) \end{pmatrix},$$

we know that if U is ordinary, then u is unramified everywhere. Let Cl^- be the '$-$' quotient of the ideal class group of K. We thus know that

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721267.011
Cambridge Books Online © Cambridge University Press, 2009

Theorem 4.6 $H^1_{\mathrm{ord}}(\Pi, sl_2(\mathfrak{W}_P)) \cong \mathrm{Hom}_{\Lambda_P}(\Omega_{R_S/\Lambda_P} \otimes_{R_S} \Lambda_P, \mathfrak{W}_P)$ injects naturally into

$$\mathrm{Hom}_\Lambda(X_S(\lambda^-) \otimes_{\Lambda_-} \Lambda, \mathfrak{W}_P) \oplus \mathrm{Hom}(Cl^-, \mathfrak{W}_P)$$

as Λ-module.

To relate $X_S(\lambda^-)$ to the congruence power series, we recall the morphism $\lambda_* \circ \theta^* : \mathbf{h} \to \Lambda$ seen in §2, H3. Let R_0 be the local ring of $\mathbf{h}$ through which the above morphism factors. To make R_0 a Λ-algebra, we consider $R = R_0 \otimes_{\Lambda_0} \Lambda$, which is still a complete local ring. Consider the module of differentials $\mathfrak{C}_1 = \Omega_{R/\Lambda} \otimes_R \Lambda$ introduced in [H1, p. 319], where the tensor product is taken via

$$R \to \Lambda \otimes_{\Lambda_0} \Lambda \to \Lambda,$$

which is $\lambda_* \circ \theta^*$ composed with the multiplication on Λ. Let R_P be the completion of the localization of R at P. In [H3, Th.I], an S-nearly ordinary deformation $\rho^{\mathrm{mod}} : \Pi \to GL_2(R_P)$ of $(k(P), \overline{\rho}_0)$ has been constructed. Especially R_P is generated over Λ_P by $\mathrm{Tr}(\rho^{\mathrm{mod}})$, and hence, the natural map $\varphi : R_S \to R_P$ which induces the equality $[\varphi \circ \rho_S] = [\rho^{\mathrm{mod}}]$ is surjective. Then φ induces another surjection

$$\varphi_* : \Omega_{R_S/\Lambda_P} \otimes_{R_S} \Lambda_P \to \mathfrak{C}_1 \otimes_\Lambda \Lambda_P.$$

This combined with Theorem 4.6 yields

Theorem 4.7 We have a surjective homomorphism of Λ-modules:

$$(X_S(\lambda^-) \otimes_{\Lambda_-} \Lambda') \oplus (Cl^- \otimes_{\mathbf{Z}} \Lambda') \to \mathfrak{C}_1,$$

where Λ' is either Λ or $\Lambda[\frac{1}{P_\lambda}]$ in Lemme 4.2 according as $F \neq \mathbf{Q}$ or $F = \mathbf{Q}$ and λ_- mod $\pi\mathfrak{O}$ is trivial on $D_{\mathfrak{p}}$.

As explained in [T2], there is a divisibility theorem proven by M. Raynaud:

Theorem 4.8 H divides the characteristic power series of $\mathfrak{C}_1$ in Λ.

Then Theorems 4.7 and 4.8 prove Theorem 4.1.

Although we have concentrated to the anti-cyclotomic tower, there is a (hypothetical) way to include the case of the cyclotomic tower. To show the dependence on F, we add subscript F to each notation, for example L_F^- for L^- over F. Supposing the strong divisibility in $\Lambda : L_{F_n}^- \mid Iw_{F_n}^-$ for the nth layer F_n of the cyclotomic $\mathbf{Z}_p$-extension of F for all n, we hope that we could eventually get the full divisibility: $L \mid Iw$ over F? But for the moment, this is still far away.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

APPENDIX

Let $F/\mathbf{Q}$ be a finite extension and fix an arbitrary finite Galois extension N/F. Let $N^{(p)}/N$ be the maximal p-profinite extension of N unramified outside p and ∞. Put $\Pi = \mathrm{Gal}(N^{(p)}/F)$. In this appendix, we shall prove the existence of the universal deformation for any (continuous) *absolutely irreducible* Galois representation $\overline{\rho} : \Pi \to GL_n(K)$ for a finite extension $K/\mathbf{Q}_p$ and then we prove the divisibility in Λ' (as in Theorem 4.7) of $h(M)Iw^-$ by H when M is an imaginary quadratic field. Let Λ be a noetherian local ring with residue field K and suppose that Λ is complete under the $\mathfrak{m}$-adic topology for the maximal ideal $\mathfrak{m}$ of Λ. We consider the category Art_Λ of artinian local Λ-algebras with residue field K. For any object A in Art_Λ, the p-adic topology on A gives a locally compact topology on $GL_n(A)$. We consider the covariant functor

$$\mathfrak{F} : \mathsf{Art}_\Lambda \to \mathsf{Sets}$$

which associates to each object A in Art_Λ a set of strict equivalence classes of continuous representations $\rho : \Pi \to GL_n(A)$ such that $\rho \bmod \mathfrak{m}_A = \overline{\rho}$. Then we have

Theorem A.1 $\mathfrak{F}$ is pro-representable on Art_Λ.

Proof We verify the Schlessinger's criterion H_i $(i = 1, 2, \ldots, 4)$ for pro-representability ([Sch]). The conditions H_1, H_2 and H_4 can be checked in exactly the same manner as in [M, 1.2]. We verify the finiteness of tangential dimension; i.e.,

H3: $\dim_K \mathfrak{F}(K[\varepsilon])$ is finite, where $K[\varepsilon] = K \oplus K\varepsilon$ with $\varepsilon^2 = 0$.

If $\rho \in \mathfrak{F}(K[\varepsilon])$, then we define a map $u = u_\rho : \Pi \to M_n(K)$ by $\rho(\sigma) = (1 \oplus u(\sigma)\varepsilon)\overline{\rho}(\sigma)$. Since ρ is continuous, u is a continuous 1-cocycle with values in the Π-module $M_n(K)$, where Π acts on $M_n(K)$ by $\sigma x = \overline{\rho}(\sigma) x \overline{\rho}(\sigma)^{-1}$. On the other hand, if we have a continuous 1-cocycle u as above, we construct a representation ρ by $\rho(\sigma) = (1 \oplus u(\sigma)\varepsilon)\overline{\rho}(\sigma)$. As a map to $M_n(K)$, ρ is continuous. Then ρ is finitely continuous as a representation. Thus the map $\mathfrak{F}(K[\varepsilon]) \to H^1_c(\Pi, M_n(K))$ is surjective. Here 'H_c' indicates the continuous cohomology. We see easily that $u(\sigma) = (\sigma - 1)m$ if and only if $(1 \oplus m)^{-1}\overline{\rho}(1 \oplus m) = \rho$ (i.e., ρ is strictly equivalent to $\overline{\rho}$, which is the 'zero' element in $\mathfrak{F}(K[\varepsilon])$). Thus we have

$$\mathfrak{F}(K[\varepsilon]) \cong H^1_c(\Pi, M_n(K))$$

and

$$H^1_c(\Pi, M_n(K)) \cong H^1_c(\Pi, sl_n(K)) \oplus \mathrm{Hom}_c(\Pi, K). \tag{A.1}$$

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.015
Cambridge Books Online © Cambridge University Press, 2009

By class field theory, $\mathrm{Hom}_c(\Pi, K)$ is finite dimensional. We now claim

$$\text{(A.2)} \qquad \dim_K H^1_c(\Pi, sl_n(K)) < +\infty.$$

Let us prove this. Let F_∞ be the subfield of $N^{(p)}$ fixed by $\mathrm{Ker}(\overline{\rho})$. Since cohomology groups of a finite group with coefficients in finite dimensional vector space over K are finite dimensional, we may replace Π by any normal subgroup of finite index because of the inflation-restriction sequence. First we may assume that $H = \mathrm{Im}(\overline{\rho})$ is a pro-p-group without torsion and that F_∞/N is unramified outside p and ∞. Then applying a theorem of Lazard [L, III.3.4.4.4], we know that H has a subgroup of finite index which is pro-p-analytic. Hence we may even assume that H itself is pro-p-analytic. By inflation-restriction sequence, the sequence:

$$\text{(A.3)} \qquad 0 \to H^1_c(H, sl_n(K)) \to H^1_c(\Pi, sl_n(K)) \to \mathrm{Hom}_H(\mathrm{Ker}(\overline{\rho}), sl_n(K))$$

is exact. Let $\mathbf{M}_\infty/F_\infty$ be the maximal p-abelian extension unramified outside p and ∞ and X be the Galois group $\mathrm{Gal}(\mathbf{M}_\infty/F_\infty)$. Let $\mathbf{A} = \mathbf{Z}_p[[H]]$. Since H is pro-p-analytic and is contained in the maximal compact subgroup of $GL_n(K)$, we know that X is a $\mathbf{A}$-module of finite type by [Ha, §3]. The maximal topological abelian quotient $\mathrm{Ker}(\overline{\rho})^{ab}$ is a quotient of X and hence of finite type over $\mathbf{A}$. This proves that

$$\text{(A.4)} \qquad \dim_K \mathrm{Hom}_H(\mathrm{Ker}(\overline{\rho}), sl_n(K)) < +\infty.$$

Thus we need to show the finite dimensionality of $H^1_c(H, sl_n(K))$. Let $\mathfrak{H}$ be the Lie algebra of $G \cap H$. Then again by a result of Lazard [L, V.2.4.10], we see

$$H^1_c(H, sl_n(K)) \cong H^0(H, H^1(\mathfrak{H}, sl_n(K))),$$

which is finite dimensional.

Let $\mathbf{h}_0 = \mathbf{h}_0^{\mathrm{ord}}(D; \mathfrak{O})$ be the ordinary Hecke algebra defined in [H1, Th.3.3] for any positive integer D prime to p. In this case G in §2 is just $Z \times \mathbf{Z}_p^\times$ for $Z = ((\mathbf{Z}/D\mathbf{Z})^\times \times \mathbf{Z}_p^\times)/\{\pm 1\}$. Then we have

Theorem A.2 Suppose that $p \geq 5$ and $F = \mathbf{Q}$. Let $\chi : \mathbf{A}^\times \to \mathbf{Z}_p^\times$ be the cyclotomic character such that $\chi(\varpi_l) = l$ for the prime element ϖ_l in $\mathbf{Q}_l$ $(l \neq p)$. Then we have an $\mathfrak{O}[[G]]$-algebra isomorphism:

$$\mathbf{h} \cong \mathbf{h}_0 \hat{\otimes}_{\mathfrak{O}} \mathfrak{O}[[\mathbf{Z}_p^\times]],$$

which is given by $\mathbf{T}(x) \mapsto T(x) \otimes [\chi(x)]$ for all $x \in \hat{\mathbf{Z}} \cap A_f^\times$. Here $\mathbf{h}_0 \hat{\otimes}_{\mathfrak{O}} \mathfrak{O}[[\mathbf{Z}_p^\times]]$ is the profinite completion of $\mathbf{h}_0 \otimes_{\mathfrak{O}} \mathfrak{O}[[\mathbf{Z}_p^\times]]$, i.e., $\mathfrak{m}$-adic completion for the maximal ideal $\mathfrak{m}$ of Λ_0.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

Proof Let $S(\mathfrak{O}) = \{f \in S \mid a(y,f) \in O\}$ and $\mathbf{S} = eS(\mathfrak{O})$ for the idempotent e of $\mathbf{h}$ in $\mathbf{h}(D;\mathfrak{O})$. Let $\mathbf{S}_0$ be the ordinary subspace of $\mathbf{S}$ which is denoted by $S_0^{\mathrm{ord}}(D;\mathfrak{O})$ in [H1, p. 336]. Then it is known that the pairing given by

$$\langle h, f\rangle = a(1, f \mid h) \text{ on } \mathbf{h} \times \mathbf{S} \text{ and } \mathbf{h}_0 \times \mathbf{S}_0$$

is perfect in the sense that $\mathrm{Hom}_{\mathfrak{O}}(\mathbf{h}, \mathfrak{O}) \cong \mathbf{S}$ and vice versa [H4, Th.3.1]. For any character $\psi : \mathbf{Z}_p^\times \to \overline{\mathbf{Q}}_p$ and $f \in \mathbf{S}$, $f \otimes \psi(y)$ given by $a(y, f \otimes \psi) = \psi(\chi(y))a(y,f)$ is again an element in S with $f\otimes\psi \mid e = f\otimes\psi$ (cf. [H4, §7.VI]). This shows that we have a natural $\mathfrak{O}[[G]]$-linear map $m : \mathbf{S}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{C}(\mathbf{Z}_p^\times;\mathfrak{O}) \to \mathbf{S}$ given by

$$a(y, m(f \otimes \phi)) = \phi(\chi(y))a(y,f),$$

where $\mathfrak{C}(\mathbf{Z}_p^\times;\mathfrak{O})$ is the Banach $\mathfrak{O}$-module of all continuous functions on $\mathbf{Z}_p^\times$ into $\mathfrak{O}$ and $\mathbf{S}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{C}(\mathbf{Z}_p^\times;\mathfrak{O})$ is the p-adic completion of $\mathbf{S}_0 \otimes_{\mathfrak{O}} \mathfrak{C}(\mathbf{Z}_p^\times;\mathfrak{O})$. Note that $\mathrm{Hom}_{\mathfrak{O}}(\mathbf{S}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{C}(\mathbf{Z}_p^\times;\mathfrak{O}), \mathfrak{O}) \cong \mathbf{h}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{O}[[\mathbf{Z}_p^\times]]$. It is easy to verify that the dual map $m^* : \mathbf{h} \to \mathbf{h}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{O}[[\mathbf{Z}_p^\times]]$ is in fact an $\mathfrak{O}[[G]]$-algebra homomorphism. Since the projection map $\mathbf{h} \to \mathbf{h}_0$ is surjective by definition and since any $[z^{-1}] \in \mathfrak{O}[[\mathbf{Z}_p^\times]]$ for $z \in \mathbf{Z}_p^\times$ is the image of $\mathbf{T}(z)$, m^* is surjective. Note that $\mathbf{h}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{O}[[\mathbf{Z}_p^\times]]$ is free of finite rank over Λ_0 by [H7, Th.3.1]. Since $\mathbf{h}$ is torsion-free over Λ_0 and its generic rank is equal to that of $\mathbf{h}_0\hat{\otimes}_{\mathfrak{O}}\mathfrak{O}[[\mathbf{Z}_p^\times]]$, we conclude that m^* is an isomorphism.

Corollary A.3 The congruence power series H can be chosen inside Λ_-.

By this corollary, when $F = \mathbf{Q}$, it is sufficient to consider only ordinary Hecke algebras instead of nearly ordinary Hecke algebras and only ordinary deformations instead of nearly ordinary deformations. To make this fact more precise, let $M/\mathbf{Q}$ be an imaginary quadratic field of discriminant D satisfying the ordinarity hypothesis: $p = \mathfrak{P}\mathfrak{P}^c$. We also assume that $p \geq 5$. Let L (resp. L^*) be the maximal abelian extension of M unramified outside $\mathfrak{P}$ (resp. $\mathfrak{P}^c$). Let $G_{cw} = \mathrm{Gal}(L/M)$ and $G_{cw}^* = \mathrm{Gal}(L^*/M)$ and W_{cw} (resp. W_{cw}^*) be the maximal torsion-free quotient of G_{cw} (resp. G_{cw}^*). Then the restriction map gives an isomorphism $\mathbf{W} \cong W_{cw} \times W_{cw}^*$. Thus $\alpha : W_{cw} \ni w \mapsto wcw^{-1}c^{-1} \in \mathbf{W}_-$ gives an isomorphism. Similarly, without losing generality, we may assume that $\lambda : \mathbf{G}_{\mathrm{tor}} \to \mathfrak{O}^\times$ factors through G_{cw}. We decompose $G_{cw} = \Delta \times W_{cw}$. Let $\Lambda_- = \mathfrak{O}[[W_{cw}]]$ identifying $\mathbf{W}_-$ with W_{cw}. We consider the character $\lambda_* : G_{cw} \to \Lambda_-$ such that $\lambda_*(\delta, w) = \lambda(\delta)[w]$ for $\delta \in \Delta$ and $w \in W$. It is known that the μ-invariant of Iw^- and L^- are both trivial [G]. Thus we only worry about height one primes P (in Λ_-) of residual characteristic 0. We take $N/\mathbf{Q}$ to be the ray class field of M modulo p and consider the Galois group Π as in Theorem A.1. Let K be the quotient

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

field of Λ_-/P. Then $K/\mathbf{Q}_p$ is a finite extension and we consider the Galois representation:

$$\rho_0 = \mathrm{Ind}_{\Pi_K}^{\Pi}(\lambda_*) : \Pi \to GL_2(\Lambda_-), \quad \text{and}$$
$$\rho_P = \mathrm{Ind}_{\Pi_K}^{\Pi}(\lambda_* \bmod P) : \Pi \to GL_2(K).$$

Suppose that $P \neq P_\lambda$ as in Lemma 4.2. Then ρ_P is absolutely irreducible. Let Λ be the P-adic completion of the localization of Λ_- at P. Let Art be the category of artinian local Λ-algebras with residue field K. Any object A in Art is a locally compact ring with respect to p-adic topology and thus we do not worry about 'finite continuity' etc. Let (R', ρ') be the universal couple representing the functor $\mathfrak{F} : \mathsf{Art} \to \mathsf{Sets}$ defined for $\overline{\rho} = \rho_P$. We consider the subfunctor of $\mathfrak{F}$

$$\mathfrak{F}^{\mathrm{ord}} : \mathsf{Art} \to \mathsf{Sets}$$

which associates to $A \in Ob(\mathsf{Art})$ the set of strict equivalence class of representations $\rho : \Pi \to GL_2(A)$ such that

(i) $\rho \bmod \mathfrak{m}_A = \rho_P$,

(ii) There exists a continuous character $\delta : D_{\mathfrak{P}} \to A^\times$ such that ρ restricted to $D_{\mathfrak{P}}$ is equivalent (but not necessarily strictly) to $\begin{pmatrix} * & * \\ 0 & \delta \end{pmatrix}$;

(iii) δ is congruent modulo $\mathfrak{m}_A$ to the restriction of λ_*^c to $D_{\mathfrak{P}}$ and δ restricted to the inertia subgroup I_p of $D_{\mathfrak{p}}$ coincides with the restriction to I_p of λ_*^c (i.e., δ is **unramified** at $\mathfrak{P}$)

(iv) $\det(\rho) = \det(\rho_0)$.

We say that an ideal $\mathfrak{a}$ of R' is ordinary if $\rho' \bmod \mathfrak{a}$ satisfies (i), (ii), (iii) and (iv). Then it is an easy exercise to verify that if $\mathfrak{a}$ and $\mathfrak{b}$ are ordinary, then $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a} \cap \mathfrak{b}$ are ordinary. Namely for $\mathfrak{I} = \bigcap_{\mathfrak{a}:\mathrm{ordinary}} \mathfrak{a}$, $R^{\mathrm{ord}} = R'/\mathfrak{I}$ and $\rho^{\mathrm{ord}} = \rho' \bmod \mathfrak{I}$ represents $\mathfrak{F}^{\mathrm{ord}}$. Then the same argument as in §4 prove that $H \mid h(M)Iw^-$. From Theorem 2.1 and the vanishing of the μ-invariant [G], we conclude

Theorem A.4 Suppose $p \geq 5$ and that M is an imaginary quadratic field. Let $\Lambda' = \Lambda_-[\frac{1}{P_\lambda}]$ if $\lambda_- \bmod \pi\mathfrak{O}$ is trivial on $D_{\mathfrak{P}}$ and otherwise we put $\Lambda' = \Lambda_-$. Then we have

$$h(M)L^- \mid H \text{ in } \Lambda_- \quad \text{and} \quad H \mid h(M)Iw^- \text{ in } \Lambda'.$$

Although we confined ourselves to characters λ of p-power conductor, similar result holds for any character whose conductor is prime to its complex conjugate. We hope to prove the divisibility even at the 'trivial-zero' P_λ in our subsequent paper.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

REFERENCES

[G] R. Gillard, 'Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes', *J. reine angew. Math.* **358** (1985), 76–91.

[Ha] M. Harris, 'p-adic representations arising from descent on abelian varieties', *Compositio Math.* **39** (1979), 177–245.

[H1] H. Hida, 'On p-adic Hecke algebras for GL_2 over totally real fields', *Ann. of Math.* **128** (1988), 295-384.

[H2] H. Hida, 'On nearly ordinary Hecke algebras for $GL(2)$ over totally real fields', *Adv. Studies in Pure Math.* **17** (1989), 139–169.

[H3] H. Hida, 'Nearly ordinary Hecke algebras and Galois representations of several variables', *Proc. JAMI inaugural Conference, Supplement of Amer. J. Math.* (1989), 115–134.

[H4] H. Hida, 'On p-adic L-functions of $GL(2) \times GL(2)$ over totally real fields', preprint.

[H5] H. Hida, 'Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms', *Invent. Math.* **85** (1986), 545–613.

[H6] H. Hida, 'A p-adic measure attached to the zeta functions associated with two elliptic modular forms II', *Ann. Inst. Fourier* **38**, No.1 (1988), 1–83.

[H7] H. Hida, 'Iwasawa modules attached to congruences of cusp forms', *Ann. Scient. Ec. Norm. Sup.* 4e-serie, t.19, 1986, 231–273.

[K] N. M. Katz, 'p-adic L-functions for CM fields', *Invent. Math.* **49** (1978), 199–297.

[L] M. Lazard, 'Groupes analytiques p-adiques', *Publ. Math. I.H.E.S.* No.26, 1965.

[M] B. Mazur, 'Deforming Galois representations', in *Galois Groups over* $\mathbf{Q}$, *Proc. Workshop at MSRI*, 1987, pp.385–437.

[M-T] B. Mazur and J. Tilouine, 'Représentations galoisiennes, différentielles de Kähler et "conjecture principales" ', *Publ. I.H.E.S.*

[R] K. Rubin, 'The one-variable main conjecture for elliptic curves with complex multiplication', preprint.

[Sch] M. Schlessinger, 'Functors on Artin rings', *Trans. A.M.S.* **130** (1968), 208–22.

[T1] J. Tilouine, 'Sur la conjecture principale anticyclotomique', *Duke Math. J.*

[T2] J. Tilouine, 'Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire', *Compositio Math.* **65** (1988), 265–320.

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009

Downloaded from https://www.cambridge.org/core. Caltech Library, on 04 Nov 2018 at 14:08:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511526053.011
Cambridge Books Online © Cambridge University Press, 2009