COMPOSITIO MATHEMATICA

Big Galois representations and p-adic L-functions

Haruzo Hida

Compositio Math. **151** (2015), 603–664.

doi:10.1112/S0010437X14007684

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
150 YEARS

Compositio Math. 151 (2015) 603–664
doi:10.1112/S0010437X14007684

Big Galois representations and p-adic L-functions

Haruzo Hida

Abstract

Let $p \geqslant 5$ be a prime. If an irreducible component of the spectrum of the 'big' ordinary Hecke algebra does not have complex multiplication, under mild assumptions, we prove that the image of its Galois representation contains, up to finite error, a principal congruence subgroup $\Gamma(L)$ of $\mathrm{SL}_2(\mathbb{Z}_p[[T]])$ for a principal ideal $(L) \neq 0$ of $\mathbb{Z}_p[[T]]$ for the canonical 'weight' variable $t = 1+T$. If $L \notin \Lambda^\times$, the power series L is proven to be a factor of the Kubota–Leopoldt p-adic L-function or of the square of the anticyclotomic Katz p-adic L-function or a power of $(t^{p^m} - 1)$.

Contents

Introduction

Throughout the paper, we fix a prime $p \geqslant 3$, field embeddings $\mathbb{C} \overset{i_\infty}{\hookleftarrow} \overline{\mathbb{Q}} \overset{i_p}{\hookrightarrow} \overline{\mathbb{Q}}_p \subset \mathbb{C}_p$ and a positive integer N prime to p. Let χ be a Dirichlet character modulo Np^{r+1}. Consider the space of modular forms $\mathcal{M}_{k+1}(\Gamma_0(Np^{r+1}), \chi)$ with $(p \nmid N, r \geqslant 0)$ (containing Eisenstein series) and cusp forms $\mathcal{S}_{k+1}(\Gamma_0(Np^{r+1}), \chi)$. Here χ is the Neben-typus. Let $\mathbb{Z}[\chi] \subset \overline{\mathbb{Q}}$ and $\mathbb{Z}_p[\chi] \subset \overline{\mathbb{Q}}_p$ be the rings generated by the values χ over $\mathbb{Z}$ and $\mathbb{Z}_p$, respectively. The Hecke algebra $H = H_{k+1}(\Gamma_0(Np^{r+1}), \chi; \mathbb{Z}[\chi])$ over $\mathbb{Z}[\chi]$ is

$$H = \mathbb{Z}[\chi][T(n) \mid n = 1, 2, \ldots] \subset \mathrm{End}(\mathcal{M}_{k+1}(\Gamma_0(Np^{r+1}), \chi)).$$

Received 26 November 2013, accepted in final form 26 June 2014, published online 13 November 2014.
2010 Mathematics Subject Classification 11F11, 11F25, 11F33, 11F80 (primary).
Keywords: p-adic L-function, Hecke algebra, Galois representation, Galois deformation.

For any $\mathbb{Z}[\chi]$-algebra $A \subset \mathbb{C}$, $H_{k+1}(\Gamma_0(Np^{r+1}), \chi; A) := H \otimes_{\mathbb{Z}[\chi]} A$ is actually the A-subalgebra of $\mathrm{End}(\mathcal{M}_{k+1}(\Gamma_0(Np^{r+1}), \chi))$ generated over A by the $T(l)$. Then we put

$$H_{k+1,\chi} = H_{k+1,\chi/W} = H_{k+1}(\Gamma_0(Np^{r+1}), \chi; W) := H \otimes_{\mathbb{Z}[\chi]} W$$

for a p-adic complete discrete valuation ring $W \subset \mathbb{C}_p$ containing $\mathbb{Z}_p[\chi]$. Let $\Lambda = \mathbb{Z}_p[[T]]$ (respectively $\Lambda_W = W[[T]]$), and write $t = 1 + T \in \Lambda^\times$ (as $\mathrm{Spf}(\Lambda) = \widehat{\mathbb{G}}_m$ with variable t).

We often write our $T(l)$ as $U(l)$ when N is divisible by l. The ordinary part $\mathbf{H}_{k+1,\chi/W} \subset H_{k+1,\chi/W}$ is then the maximal ring direct summand on which $U(p)$ is invertible. We write e for the idempotent of $\mathbf{H}_{k+1,\chi/W}$; so, e is the p-adic limit in $H_{k+1,\chi/W}$ of $U(p)^{n!}$ as $n \to \infty$. We write the image of the idempotent as $\mathcal{M}^{\mathrm{ord}}_{k+1}$ for modular forms and $\mathcal{S}^{\mathrm{ord}}_{k+1}$ for cusp forms. Let $\chi_1 =$ the N-part of $\chi \times$ the tame p-part of χ. Then, by [Hid86a, Hid86b] (and [Hid11a, § 3.2]), we have a unique 'big' Hecke algebra $\mathbf{H} = \mathbf{H}_{\chi_1/W}$ such that:

(1) $\mathbf{H}$ is free of finite rank over Λ_W equipped with $T(n) \in \mathbf{H}$ for all n;
(2) if $k \geqslant 1$ and $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}(W)$ is a character, $\mathbf{H}/(t - \varepsilon(\gamma)\gamma^k)\mathbf{H} \cong \mathbf{H}_{k+1,\varepsilon\chi_k}$ for $\chi_k := \chi_1\omega^{1-k}$ ($\gamma = 1 + p \in \mathbb{Z}_p^\times$), sending $T(n)$ to $T(n)$, where ω is the Teichmüller character.

The corresponding objects for cusp forms are denoted by the corresponding lower case characters; so, $h = \mathbb{Z}[\chi][T(n) \mid n = 1, 2, \ldots] \subset \mathrm{End}(\mathcal{S}_{k+1}(\Gamma_0(Np^{r+1}), \chi))$, $h_{k+1,\chi/W} = h_{k+1}(\Gamma_0(Np^{r+1}), \chi; W) := h \otimes_{\mathbb{Z}[\chi]} W$, the ordinary part $\mathbf{h}_{k+1,\chi} \subset h_{k+1,\chi}$ and the 'big' cuspidal Hecke algebra $\mathbf{h} = \mathbf{h}_{\chi_1}(N)_{/W}$. Replacing modular forms by cusp forms (and upper case symbols by lower case symbols), we can construct the cuspidal Hecke algebra $\mathbf{h}$. Then, similarly to the case of modular forms, we have the following characterization of the cuspidal Hecke algebra $\mathbf{h}_{/W}$:

(1) $\mathbf{h}$ is free of finite rank over Λ_W equipped with $T(n) \in \mathbf{h}$;
(2) $\mathbf{h}/(t - \varepsilon(\gamma)\gamma^k)\mathbf{h} \cong \mathbf{h}_{k+1,\varepsilon\chi_k}$ sending $T(n)$ to $T(n)$, if $k \geqslant 1$.

We have a surjective Λ_W-algebra homomorphism $\mathbf{H} \twoheadrightarrow \mathbf{h}$ sending $T(n)$ to $T(n)$.

Write Q for the quotient field of Λ, and fix an algebraic closure $\overline{Q}$ of Q. A two-dimensional Galois representation is called odd if its determinant of complex conjugation is equal to -1. We have a two-dimensional odd semi-simple odd representation $\rho_{\mathbf{H}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in the total quotient ring $Q(\mathbf{H})$ of $\mathbf{H}$ (see [Hid86b] and [Hid11a, § 4.3]). The total quotient ring $Q(\mathbf{H})$ is the ring of fractions by the multiplicative set of all non-zero divisors; so, $Q(\mathbf{H}) = \mathbf{H} \otimes_\Lambda Q$. This representation preserves an $\mathbf{H}$-lattice $\mathcal{L} \subset Q(\mathbf{H})^2$ (i.e. an $\mathbf{H}$-submodule of $Q(\mathbf{H})^2$ of finite type which spans $Q(\mathbf{H})^2$ over $Q(\mathbf{H})$), and as a map of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into the profinite group $\mathrm{Aut}_{\mathbf{H}}(\mathcal{L})$, it is continuous. The representation $\rho_{\mathbf{H}}$ restricted to the p-decomposition group $D_p \cong \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (associated to i_p) is isomorphic to an upper triangular representation with unramified rank 1 quotient. Write $\rho^{\mathrm{ss}}_{\mathbf{H}}$ for the semi-simplification over D_p. As is well known now (e.g. [Hid11a, § 4.3.2]), $\rho_{\mathbf{H}}$ satisfies, for $t = 1 + T$,

$$\mathrm{Tr}(\rho_{\mathbf{H}}(\mathrm{Frob}_l)) = T(l) (l \nmid Np), \quad \rho^{\mathrm{ss}}_{\mathbf{H}}([\gamma^s, \mathbb{Q}_p]) \sim \begin{pmatrix} t^s & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho^{\mathrm{ss}}_{\mathbf{H}}([p, \mathbb{Q}_p]) \sim \begin{pmatrix} * & 0 \\ 0 & U(p) \end{pmatrix}, \tag{Gal}$$

where $\gamma^s = (1+p)^s \in \mathbb{Z}_p^\times$ for $s \in \mathbb{Z}_p$ and $[x, \mathbb{Q}_p]$ is the local Artin symbol.

For each prime $P \in \mathrm{Spec}(\mathbf{H})$, let $\kappa(P)$ be the residue field of P. Then $\mathrm{Tr}(\rho_{\mathbf{H}})$ mod P has values in $\mathbf{H}/P$, and by the technique of pseudo representations (cf. [Hid00, § 2.2]), we can construct a unique semi-simple Galois representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P))$ such that

$$\mathrm{Tr}(\rho_P(\mathrm{Frob}_l)) = (T(l) \bmod P) \quad \text{for all prime } l \nmid Np.$$

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

For any ideal $\mathfrak{a} \subset \mathbf{H}$ with reduced $\mathbf{H}/\mathfrak{a}$, we write $\rho_{\mathfrak{a}} = \prod_P \rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(Q(\mathbf{H}/\mathfrak{a}))$ for the total quotient ring $Q(\mathbf{H}/\mathfrak{a})$ of $\mathbf{H}/\mathfrak{a}$, where P runs over minimal primes of $\mathrm{Spec}(\mathbf{H}/\mathfrak{a})$. If $\mathfrak{a} = \mathrm{Ker}(\mathbf{H} \to \mathbb{I})$ (respectively $\mathfrak{a} = \mathrm{Ker}(\mathbf{H} \to \mathbb{T}^{\mathrm{red}})$) for an irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$ (respectively a connected component $\mathrm{Spec}(\mathbb{T}) \subset \mathrm{Spec}(\mathbf{h})$), we write $\rho_{\mathbb{I}}$ (respectively $\rho_{\mathbb{T}}$) for $\rho_{\mathfrak{a}}$, where $\mathbb{T}^{\mathrm{red}}$ is $\mathbb{T}$ modulo its nilradical. If $\mathbb{T}$ or its irreducible component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{T})$ is fixed in the context, we write $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ for $\rho_{\mathfrak{m}_{\mathbb{T}}} = \rho_{\mathfrak{m}_{\mathbb{I}}}$ for the maximal ideals $\mathfrak{m}_{\mathbb{T}}$ of $\mathbb{T}$ and $\mathfrak{m}_{\mathbb{I}}$ of $\mathbb{I}$.

Let $\mathrm{Spec}(\mathbb{I})$ be an irreducible (reduced) component of $\mathrm{Spec}(\mathbf{H})$ and write its normalization as $\mathrm{Spec}(\widetilde{\mathbb{I}})$. We often call $\mathbb{I}$ a component of $\mathbf{H}$ and regard it as sitting inside $\overline{Q}$ (when W is finite over $\mathbb{Z}_p$). We denote by $Q(\mathbb{I})$ the quotient field of $\mathbb{I}$. We call a prime ideal $P \subset R$ of a ring R a *prime divisor* if $\mathrm{Spec}(R/P)$ has codimension 1 in $\mathrm{Spec}(R)$. We call an ideal $\mathfrak{D}$ of $\mathbb{I}$ a *divisor* if $\mathfrak{D} = \bigcap_P P^{m_P}$ for finitely many prime divisors P. Write $a(n)$ for the image of $T(n)$ (n prime to Np) in $\mathbb{I}$ and $a(l)$ for the image of $U(l)$ if $l|Np$. If a prime divisor P of $\mathrm{Spec}(\mathbb{I})$ contains $(t - \varepsilon(\gamma)\gamma^k)$ with $k \geqslant 1$, by (2) we have a Hecke eigenform $f_P \in \mathcal{M}_{k+1}(\Gamma_0(Np^{r(P)+1}), \varepsilon\chi_k)$ such that its eigenvalue for $T(n)$ is given by $a_P(n) := (a(n) \bmod P) \in \overline{\mathbb{Q}}_p$ for all n. A prime divisor P with $P \cap \Lambda_W = (t - \varepsilon(\gamma)\gamma^k)$ with $k \geqslant 1$ and a character $\varepsilon : \mathbb{Z}_p^\times \to \mu_{p^\infty}(W)$ is called an *arithmetic* point (or prime), and we write $\varepsilon_P = \varepsilon$ and $k(P) = k \geqslant 1$ for an arithmetic P. Thus $\mathbb{I}$ gives rise to an analytic family $\mathcal{F}_{\mathbb{I}} = \{f_P \mid \text{arithemtic points } P \text{ in } \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)\}$ of slope 0 classical Hecke eigenforms. A component $\mathbb{I}$ (or the associated family) is called *cuspidal* if $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbf{h})$. A cuspidal component $\mathbb{I}$ is called a *CM component* if there exists a non-trivial character $\xi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{I}^\times$ such that $\rho_{\mathbb{I}} \cong \rho_{\mathbb{I}} \otimes \xi$. If a cuspidal $\mathbb{I}$ is not a CM component, we call it a non-CM component.

Put $\Gamma(\mathfrak{a}) = \{x \in \mathrm{SL}_2(\Lambda) \mid x \equiv 1 \bmod \mathfrak{a} \cdot M_2(\Lambda)\}$ for an ideal $\mathfrak{a} \subset \Lambda$, and write $\Gamma(L) = \Gamma(\mathfrak{a})$ if $\mathfrak{a} = (L)$ ($L \in \Lambda$). The representation $\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(Q(\mathbb{I}))$ leaves stable a $\widetilde{\mathbb{I}}$-lattice $\mathcal{L}$ in $Q(\mathbb{I})^2$ with $Q \cdot \mathcal{L} = Q(\mathbb{I})^2$. We assume throughout the paper, after extending scalars W,

(F) the representation $\rho_{\mathbb{I}}$ has values in $\mathrm{GL}_2(\widetilde{\mathbb{I}})$ (i.e. we assume the ability to find an $\widetilde{\mathbb{I}}$-free $\mathcal{L}$).

If $\overline{\rho}$ is absolutely irreducible, by the technique of pseudo representation, (F) can be checked to be true. If $\mathbb{I}$ is a unique factorization domain with $\mathrm{Spec}(\widetilde{\mathbb{I}})(W) \neq \emptyset$, in particular, if $\mathbb{I}$ is regular (so far, there is no known non-regular example of $\widetilde{\mathbb{I}}$), replacing $\mathcal{L}$ by its reflexive closure (i.e. the intersection of all $\widetilde{\mathbb{I}}$-free modules in $Q(\mathbb{I})^2$ containing $\mathcal{L}$), $\mathcal{L}$ is free of rank 2 over $\mathbb{I}$. By resolution of singularity of surfaces (see [Lip78]), we can find an injective local Λ-algebra homomorphism $\mathbb{I} \hookrightarrow \mathbb{I}^{sm} \subset Q(\mathbb{I})$ for a regular two-dimensional $\mathbb{I}^{sm}$, though $\mathbb{I}^{sm}$ may not be finite over $\mathbb{I}$. Thus replacing $\mathbb{I}$ by $\mathbb{I}^{sm}$ (and extending scalars to achieve $\mathrm{Spec}(\mathbb{I}^{sm})(W) \neq \emptyset$), we have a model $\rho_{\mathbb{I}^{sm}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{I}^{sm})$ isomorphic to $\rho_{\mathbb{I}}$ over $Q(\mathbb{I})$. See § 9 for details of these facts. Anyway, we assume (F) in this paper.

Actually we choose $\mathcal{L}$ coming from the projective limit (relative to p-power level) of Tate modules of modular jacobians, and for this choice of $\mathcal{L}$, $\mathbb{I}$-freeness of $\mathcal{L}$ is known if $\mathbb{T}$ is Gorenstein (which in turn follows from irreducibility of $\overline{\rho}$ and the p-distinguished-ness condition (R) below). Thus in most cases, we can choose the scalar extension to $\widetilde{\mathbb{I}}$ of the canonical $\mathcal{L}$ free over $\mathbb{I}$. Write $[\rho_{\mathbb{I}}]$ for the isomorphism class of $\rho_{\mathbb{I}}$ over $Q(\mathbb{I})$. Pick and fix a *non*-CM component $\mathbb{I}$ of prime-to-p level N, and assume the following condition (R) throughout the paper,

(R) $\overline{\rho}|_{D_p} \cong \left(\begin{smallmatrix} \overline{\epsilon} & * \\ 0 & \overline{\delta} \end{smallmatrix}\right)$ with $\overline{\delta}$ unramified and $\overline{\epsilon} \neq \overline{\delta}$.

THEOREM I. *Suppose $p \geqslant 3$. Then there exists a representation $\rho \in [\rho_{\mathbb{I}}]$ with values in $\mathrm{GL}_2(\widetilde{\mathbb{I}})$ such that $G := \mathrm{Im}(\rho) \cap \mathrm{SL}_2(\Lambda)$ contains $\Gamma(\mathfrak{a})$ for an ideal $0 \neq \mathfrak{a} \subset \Lambda$. If $\mathfrak{c}$ is the Λ-ideal maximal among $\mathfrak{a}$ with $G \supset \Gamma(\mathfrak{a})$, the ideal $\mathfrak{c}_P \subset \Lambda_P$ localized at a prime divisor P of Λ only depends*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

on the isomorphism class $[\rho_{\mathbb{I}}]$ *as long as* $\rho_{\mathfrak{P}}$ *is absolutely irreducible for all prime divisors* $\mathfrak{P}|P$ *in* $\widetilde{\mathbb{I}}$*; in particular, if* $\overline{\rho} = \rho_{\mathfrak{m}}$ *for the maximal ideal* $\mathfrak{m}$ *of* $\mathbb{I}$ *is absolutely irreducible, the reflexive closure* (L) *of* $\mathfrak{c}$ *is independent of the choice of* ρ *with* $G \supset \Gamma(\mathfrak{a}) \neq 1$.

The reflexive closure $\widetilde{\mathfrak{c}}$ of an ideal $\mathfrak{c} \subset \Lambda$ means the intersection $\bigcap_{(\lambda)\supset\mathfrak{c}}(\lambda) \subset \Lambda$ of all principal ideals (λ) containing $\mathfrak{c}$ which is a principal ideal. It can also be defined as the intersection $\widetilde{\mathfrak{c}} = \bigcap_P \mathfrak{c}_P$ inside Q for P running over all prime divisors of Λ (see [Bou98, ch. 7] for these facts). We write $0 \neq L = L(\mathbb{I}) \in \Lambda$ for a generator of the ideal $\widetilde{\mathfrak{c}}$. We call $\mathfrak{c}$ as above the *conductor* of ρ (or of G).

We prove the theorem under one of the following conditions:

- (s) $\mathrm{Im}(\rho_{\mathbb{I}})$ and $\rho_{\mathbb{I}}(D_p)$ are both normalized by an element $g \in \mathrm{GL}_2(\mathbb{I})$ with $\overline{g} := (g \bmod \mathfrak{m}_{\mathbb{I}})$ having eigenvalues $\overline{\alpha}, \overline{\beta}$ in $\mathbb{F}_p$ with $\overline{\alpha}^2 \neq \overline{\beta}^2$;
- (u) $\rho_{\mathbb{I}}(D_p)$ contains a non-trivial unipotent element $g \in \mathrm{GL}_2(\mathbb{I})$;
- (v) $\rho_{\mathbb{I}}(D_p)$ contains a unipotent element $g \in \mathrm{GL}_2(\mathbb{I})$ with $g \not\equiv 1 \bmod \mathfrak{m}_{\mathbb{I}}$.

Obviously, (v) implies (u); so, we actually assume either (s) or (u). By [Zha12], the condition (u) is always satisfied; so, the theorem is stated only assuming (R) and $p > 3$.

The reason for assuming the conditions (R) and one of (s) and (u) is technical. These conditions are used to show in a key lemma, Lemma 2.9, that the Lie algebra $\mathcal{M}^0$ of $\mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\Lambda)$ (in the sense of Pink [Pin93]; see the following section) is large so that $\mathfrak{sl}_2(\Lambda)/\mathcal{M}^0$ is a Λ-torsion module.

The condition (u) is always satisfied by $\rho_{\mathbb{I}}$; it was first proven in [GV04] as Theorem 3 under (R) and absolute irreducibility of the residual representation $\overline{\rho}$ over $\mathbb{Q}[\mu_p]$. The two assumptions in [GV04] ((R) and absolute irreducibility of $\overline{\rho}$) are now eliminated for the validity of (u) by a method different from [GV04] (see [Hid13b, Zha12]), and (u) holds unconditionally. The condition (s) is easy to check (for example, it is valid if $\overline{\epsilon}|_{I_p}$ has order $\geqslant 3$; indeed, by local class field theory, we view $\overline{\epsilon}|_{I_p}$ as a character of $\mathbb{Z}_p^\times$, which has values in $\mathbb{F}_p^\times$, and hence, if $\zeta = \overline{\epsilon}(\sigma)$ has order $\geqslant 3$ for $\sigma \in I_p$, the adjoint action $\mathrm{Ad}(j)$ of $j = \overline{\rho}(\sigma)$ on $\mathfrak{sl}_2(\mathbb{I}/\mathfrak{m}_{\mathbb{I}})$ has three distinct eigenvalues $\zeta, 1, \zeta^{-1}$ in $\mathbb{F}_p$). In the condition (s), we may replace g by $\lim_{n\to\infty} g^{q^n}$ for a sufficiently large p-power q; so, we may assume that g has eigenvalues in $\mathbb{Z}_p$. This theorem will be proven in § 3. The proof is difficult if $\mathbb{I} \neq \Lambda$, and the easier case of $\mathbb{I} = \Lambda$ is treated in [Hid11a, Theorems 4.3.21 and 4.3.23]. When $\overline{\rho}$ is absolutely irreducible, we call $L = L(\mathbb{I})$ as in the theorem the *global level* of $\rho_{\mathbb{I}}$ or of $\mathbb{I}$. More generally, when ρ_P is absolutely irreducible, the localized ideal $\mathfrak{c}_P$ is well determined by $\rho_{\mathbb{I}}$ (see Lemma 3.3). When ρ_P is reducible, there is a way of normalizing $\mathfrak{c}_P$ as we will explain in § 3. We believe that the following standard choice $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ of the lattice $\mathcal{L}$ satisfies this normalization; so, we state the result for $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ in this introduction, though such a choice is not necessary. Then we define $(L(\mathbb{I})) = \bigcap_P \mathfrak{c}_P$ using this normalized $\mathfrak{c}_P$.

To describe this standard example of $\mathcal{L}$ stable under the Galois action, we note that $\rho_{\mathbf{h}}$ was constructed in [Hid86b] through the Galois action on the χ_1-part J of

$$\varprojlim_n e \cdot (T_p J_1(Np^n) \otimes_{\mathbb{Z}_p} W)$$

for the p-adic Tate module $T_p J_1(Np^n)$ of the jacobian $J_1(Np^n)_{/\mathbb{Q}}$ of the modular curve $X_1(Np^n)_{/\mathbb{Q}}$. Suppose that $\mathbb{I}$ is cuspidal. Let $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ (respectively $\mathcal{L}_{\mathrm{can}}(\mathbb{I})$) be the image of $J \otimes_{\mathbf{h}} \widetilde{\mathbb{I}}$ (respectively $J \otimes_{\mathbf{h}} \mathbb{I}$) in $J \otimes_{\mathbf{h}} Q(\mathbb{I}) \cong Q(\mathbb{I})^2$ for $\mathbf{h} = \mathbf{h}_{\chi_1/\mathbb{Z}_p}$. Consider the following version of (F):

($\mathrm{F}_{\mathrm{can}}$) $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ is free of rank 2 over $\widetilde{\mathbb{I}}$.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

This condition holds under (R) and absolute irreducibility of $\overline{\rho}$ (see § 7 for this fact). Under the condition (R) (and ($\mathrm{F_{can}}$)), the Galois module $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ fits into the canonical exact sequence of D_p-modules $0 \to \widetilde{\mathbb{I}} \to \mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}}) \to \widetilde{\mathbb{I}} \to 0$, coming from the connected-étale exact sequence of the Tate modules $e \cdot T_p J_1(Np^n)$, and the assertion (Gal) is realized through this exact sequence. Thus assuming (R), we take the Galois representation $\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widetilde{\mathbb{I}})$ realized on $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$.

If R is a p-profinite local ring (or its localization), as we will describe in § 10, any Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R)$ ramified at finitely many primes has a well-defined prime-to-p conductor $C(\rho)$. We call $\mathbb{I}$ minimal if $C(\rho_{\mathbb{I}})$ is minimal among $C(\rho_{\mathbb{I}} \otimes \xi)$ for ξ running all finite order characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified at p. Since the global level of $\rho_{\mathbb{I}}$ and $\rho_{\mathbb{I}} \otimes \xi$ are equal, to describe $L(\mathbb{I})$, we may assume that $\mathbb{I}$ is minimal and primitive in the sense of [Hid86a, § 3 p. 252] (so, $f_P \in \mathcal{F}_{\mathbb{I}}$ is a p-stabilized N-new form). In many cases, we can relate the generator $L(\mathbb{I})$ with p-adic L-functions. Write $\varphi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times|$. The following is a summary of determination of $L(\mathbb{I})$.

THEOREM II. *Suppose $p \geqslant 5$, ($\mathrm{F_{can}}$) and (R) and one of the conditions (s) and (v). Take a non-CM minimal primitive cuspidal component $\mathbb{I}$ of prime-to-p cube-free level N.*

(1) *If $\mathrm{Im}(\overline{\rho})$ contains $\mathrm{SL}_2(\mathbb{F}_p)$ and $p \geqslant 7$, then $L(\mathbb{I}) = 1$.*

(2) *If the projected image of $\overline{\rho}$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ is either a tetrahedral, an octahedral or an icosahedral group, then $T | L(\mathbb{I}) | T^n$ for an integer $n > 0$.*

(3) *Suppose that $\overline{\rho}$ is absolutely irreducible and $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$ for a quadratic field M and a character $\overline{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \overline{\mathbb{F}}_p^\times$. Write $\mathfrak{C}(\overline{\psi})$ for the prime-to-p part of the conductor of $\overline{\psi}$:*

(a) *if there is no other imaginary quadratic field M' such that $\overline{\rho} \cong \mathrm{Ind}_{M'}^{\mathbb{Q}} \overline{\varphi}$ for a character $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M') \to \overline{\mathbb{F}}_p^\times$ and either M is real or p does not split in M, $L(\mathbb{I})$ is a factor of $(t^{p^m} - 1)^2$ for an integer $m \geqslant 0$;*

(b) *suppose $p \nmid \varphi(N)$ and $N = C(\overline{\rho})$. If M is an imaginary quadratic field in which p splits, $\overline{\psi}$ ramifies at a prime over p and there is no other quadratic field M' such that $\overline{\rho} \cong \mathrm{Ind}_{M'}^{\mathbb{Q}} \overline{\varphi}$ for a character $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M') \to \overline{\mathbb{F}}_p^\times$, then $L(\mathbb{I})$ is a factor of the square of the product of the (primitive) anticyclotomic Katz p-adic L-functions (cf. [Kat78]) of prime-to-p conductor $\mathfrak{C}(\overline{\psi}^-)$ whose branch character modulo p is the anticyclotomic projection $\overline{\psi}^-$ of $\overline{\psi}$. Here $\overline{\psi}^-$ is given by $\sigma \mapsto \overline{\psi}(\sigma)\overline{\psi}(c\sigma c^{-1})^{-1}$ for complex conjugation c.*

(4) *Suppose $p \nmid \varphi(N)$ and ($\mathrm{F_{can}}$). If $\overline{\rho} \cong \overline{\theta} \oplus \overline{\psi}$ (with $\overline{\theta}$ ramified at p and $\overline{\psi}$ unramified at p) and there is no quadratic field M' such that $\overline{\rho} \cong \mathrm{Ind}_{M'}^{\mathbb{Q}} \overline{\varphi}$ for a character $\overline{\varphi} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{F}}_p^\times$, then $L(\mathbb{I})$ is a factor of a product of the Kubota–Leopoldt p-adic L-functions specified in Definition 4.1(2).*

The product of p-adic L-functions in the theorem will be made precise in § 8 depending on $\overline{\rho}$. The assertion (1) is a version of a result of Mazur and Wiles in [MW86] and Fischman [Fis02] where $\mathbb{I} = \Lambda$ is assumed (see Remark 8.3). The assertion (3b) is the most difficult to prove, and a sketch and the strategy of the proof are given after Theorem 8.5 before giving its long detailed proof. Theorem 8.5 gives a result slightly stronger than (3b) (in particular, we do not need to assume that N is cube-free). The assertion (4) can be proven similarly to (3b), and Ohta's determination [Oht03] of the congruence module between the Eisenstein component and a cuspidal component is crucial. Some more complicated cases missing from Theorem II are discussed in § 9.

This type of result, asserting that the image of the modular Galois representation of each non-CM Hecke eigenform contains, up to conjugation, an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, was proven

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

in a paper by Ribet [Rib75] (and [Rib85]) in 1975 and by Momose [Mom81] in 1981. As we will see in Proposition 5.1, a CM component and a non-CM component do not intersect at any of the arithmetic points, and therefore $\mathrm{Im}(\rho_{\mathfrak{P}})$ contains, up to conjugation, an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ for arithmetic points $\mathfrak{P} \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ as long as $\mathbb{I}$ is a non-CM component. An investigation of the image for Λ-adic Galois representations was first done in 1986 by Mazur–Wiles in [MW86] (just after the representation was constructed in [Hid86b]). We call a prime divisor $\mathfrak{P} \in \mathrm{Spec}(\mathbb{I})$ *full* (in a weak sense) if $\mathrm{Im}(\rho_{\mathfrak{P}})$ contains, up to conjugation in $\mathrm{GL}_2(\kappa(\mathfrak{P}))$ for the residue field $\kappa(\mathfrak{P}) = Q(\mathbb{I}/\mathfrak{P})$ of $\mathfrak{P}$, an open subgroup of either $\mathrm{SL}_2(\mathbb{Z}_p)$ or $\mathrm{SL}_2(\mathbb{F}_p[[T]])$. Fullness of most primes above $(p) \subset \Lambda$ is treated in [Hid13a] (see also [SW99], in particular, results about 'nice' primes there). The existence of such a full prime divisor is a key ingredient of the proof of the above theorems.

1. Lie algebras of p-profinite subgroups of SL(2)

If A is a ring of characteristic p, the power series $\log(1+X)$ and $\exp(X)$ do not make much sense to create the logarithm and the exponential map; so, the relation between closed subgroups in $\mathrm{GL}_n(A)$ and Lie subalgebras of $\mathfrak{gl}_n(A)$ appears not very direct. The *principal congruence subgroup*

$$\Gamma_A(\mathfrak{a}) := \mathrm{SL}_2(A) \cap (1 + \mathfrak{a} \cdot \mathfrak{gl}_2(A)) = \{x \in \mathrm{SL}_2(A) \mid x \equiv 1 \bmod \mathfrak{a}\}$$

for an A-ideal $\mathfrak{a}$ obviously plays an important role in this paper. To study a general p-profinite subgroup $\mathcal{G}$ of $\mathrm{SL}_2(A)$ for a general p-profinite ring A, we want to have an explicit relation between p-profinite subgroups $\mathcal{G}$ of the form $\mathrm{SL}_2(A) \cap (1 + X)$ and a Lie $\mathbb{Z}_p$-subalgebra $X \subset \mathfrak{gl}_2(A)$. Assuming $p > 2$, Pink [Pin93] found a functorial explicit relation between closed subgroups in $\mathrm{SL}_2(A)$ and Lie subalgebras of $\mathfrak{gl}_2(A)$ (valid even for A of characteristic p). We call subgroups of the form $\mathrm{SL}_2(A) \cap (1 + X)$ (for a p-profinite Lie $\mathbb{Z}_p$-subalgebra X of $\mathfrak{gl}_2(A)$) *basic subgroups*, following Pink.

We prepare some notation to quote here the results in [Pin93]. Let A be a semi-local p-profinite ring (not necessarily of characteristic p). Since Pink's result allows semi-local p-profinite algebra, we do not assume A to be local in the exposition of his result. We assume $p > 2$. Define maps $\Theta : \mathrm{SL}_2(A) \to \mathfrak{sl}_2(A)$ and $\zeta : \mathrm{SL}_2(A) \to Z(A)$ for the center $Z(A)$ of the algebra $M_2(A)$ by

$$\Theta(x) = x - \frac{1}{2}\mathrm{Tr}(x)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \zeta(x) = \frac{1}{2}(\mathrm{Tr}(x) - 2)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For each p-profinite subgroup $\mathcal{G}$ of $\mathrm{SL}_2(A)$, define L by the closed additive subgroup of $\mathfrak{sl}_2(A)$ topologically generated by $\Theta(x)$ for all $x \in \mathcal{G}$. Then we put $C = \mathrm{Tr}(L \cdot L)$. Here $L \cdot L$ is the closed additive subgroup of $M_2(A)$ generated by $\{xy \mid x, y \in L\}$ for the matrix product xy, similarly L^n is the closed additive subgroup generated by iterated products (n times) of elements in L. We then define $L_1 = L$ and inductively $L_{n+1} = [L, L_n]$; so, $L_2 = [L, L]$, where $[L, L_n]$ is the closed additive subgroup generated by Lie bracket $[x, y] = xy - yx$ for $x \in L$ and $y \in L_n$. Then by [Pin93, Proposition 3.1], we have

$$[L, L] \subset L, C \cdot L \subset L, L = L_1 \supset \cdots \supset L_n \supset L_{n+1} \supset \cdots \quad \text{and} \quad \bigcap_{n \geqslant 1} L_n = \bigcap_{n \geqslant 1} L^n = 0. \tag{1.1}$$

In particular, L is a Lie $\mathbb{Z}_p$-subalgebra of $\mathfrak{sl}_2(A)$. Put $\mathcal{M}_n(\mathcal{G}) = C\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \oplus L_n \subset M_2(A) = \mathfrak{gl}_2(A)$, which is a closed Lie $\mathbb{Z}_p$-subalgebra by (1.1). We write simply $\mathcal{M}(\mathcal{G})$ (respectively $\mathcal{M}^0(\mathcal{G})$) for $\mathcal{M}_2(\mathcal{G})$ (respectively $\mathcal{M}_2(\mathcal{G}) \cap \mathfrak{sl}_2(A) = [L, L]$). Define

$$\mathcal{H}_n = \{x \in \mathrm{SL}_2(A) \mid \Theta(x) \in L_n, \mathrm{Tr}(x) - 2 \in C\} \quad \text{for } n \geqslant 1.$$

If $x \in \mathcal{H}_n$, then $x = \Theta(x) + \zeta(x) + \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$; thus, $\mathcal{H}_n \subset \mathrm{SL}_2(A) \cap (1 + \mathcal{M}_n(\mathcal{G}))$. If we pick $x \in \mathrm{SL}_2(A) \cap (1 + \mathcal{M}_n(\mathcal{G}))$, then $x = 1 + c \cdot 1 + y$ with $y \in L_n$ and $c \in C$. Thus $\mathrm{Tr}(x) - 2 = 2c \in C$ and $\Theta(x) = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) + c \cdot \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) + y - \frac{1}{2}(2 + 2c) \cdot \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) = y$. This shows

$$\mathcal{H}_n = \mathrm{SL}_2(A) \cap (1 + \mathcal{M}_n(\mathcal{G})) \quad \text{in particular, } \mathcal{H}_2 = \mathrm{SL}_2(A) \cap (1 + \mathcal{M}(\mathcal{G})).$$

Here is a result of Pink [Pin93, Theorem 3.3 combined with Theorem 2.7].

THEOREM 1.1 (Pink). *Let the notation be as above. Suppose $p > 2$, and let A be a semi-local p-profinite commutative ring with identity. Take a p-profinite subgroup $\mathcal{G} \subset \mathrm{SL}_2(A)$. Then we have:*

(1) *$\mathcal{G}$ is a normal closed subgroup of $\mathcal{H}_1$ (defined as above for $\mathcal{G}$);*
(2) *$\mathcal{H}_n$ is a p-profinite subgroup of $\mathrm{SL}_2(A)$ inductively given by $\mathcal{H}_{n+1} = (\mathcal{H}_1, \mathcal{H}_n)$ which is the closed subgroup topologically generated by commutators (x, y) with $x \in \mathcal{H}_1$ and $y \in \mathcal{H}_n$;*
(3) *$\{\mathcal{H}_n\}_{n \geqslant 2}$ coincides with the descending central series of $\{\mathcal{G}_n\}_{n \geqslant 2}$ of $\mathcal{G}$, where $\mathcal{G}_{n+1} = (\mathcal{G}, \mathcal{G}_n)$ starting with $\mathcal{G}_1 = \mathcal{G}$.*

In particular, we have

(P) *the topological commutator subgroup $\mathcal{G}'$ of $\mathcal{G}$ is the subgroup given by $\mathrm{SL}_2(A) \cap (1 + \mathcal{M}(\mathcal{G}))$ for the closed additive subgroup $\mathcal{M}(\mathcal{G}) \subset M_2(A)$ as above.*

Put $\mathcal{M}_j^0(\mathcal{G}) = \mathcal{M}_j(\mathcal{G}) \cap \mathfrak{sl}_2(A)$. By the above expression, $\mathcal{G} \mapsto \mathcal{M}_j(\mathcal{G})$ (respectively $\mathcal{G} \mapsto \mathcal{M}_j^0(\mathcal{G})$) is a covariant functor from p-profinite subgroups of $\mathrm{SL}_2(A)$ into closed Lie $\mathbb{Z}_p$-subalgebras of $\mathfrak{gl}_2(A)$ (respectively $\mathfrak{sl}_2(A)$). In particular, $\mathcal{M}_j(\mathcal{G})$ and $\mathcal{M}_j^0(\mathcal{G})$ are stable under the adjoint action $x \mapsto gxg^{-1}$ of $\mathcal{G}$. For an A-ideal $\mathfrak{a}$, writing $\overline{\mathcal{G}}_{\mathfrak{a}} = (\mathcal{G} \bmod \mathfrak{a}) = (\mathcal{G} \cdot \Gamma_A(\mathfrak{a}))/\Gamma_A(\mathfrak{a})$, $\mathcal{M}_j(\overline{\mathcal{G}}_{\mathfrak{a}}) \subset \mathfrak{gl}_2(A/\mathfrak{a})$ (respectively $\mathcal{M}_j^0(\overline{\mathcal{G}}_{\mathfrak{a}}) \subset \mathfrak{sl}_2(A/\mathfrak{a})$) is the surjective image of $\mathcal{M}_j(\mathcal{G})$ (respectively $\mathcal{M}_j^0(\mathcal{G})$) under the reduction map $x \mapsto (x \bmod \mathfrak{a})$. Since $\mathcal{H}_1$ is a basic subgroup with $\mathcal{H}_1/\mathcal{G}$ abelian, we call $\mathcal{H}_1$ the *basic closure* of $\mathcal{G}$. If $\mathcal{G}$ is normalized by an element of $\mathrm{GL}_2(A)$, by construction, the basic closure $\mathcal{H}_1$ is also normalized by the same element. Thus the normalizer of $\mathcal{G}$ in $\mathrm{GL}_2(A)$ is contained in the normalizer of $\mathcal{H}_1$ in $\mathrm{GL}_2(A)$. By the above theorem, any p-profinite subgroup of $\mathrm{SL}_2(A)$ is basic up to abelian error.

LEMMA 1.2. *Let A be an integral domain finite flat either over $\mathbb{F}_p[[T]]$, Λ or $\mathbb{Z}_p$ with quotient field $Q(A)$. If a subgroup $G \subset \mathrm{SL}_2(A)$ contains the subgroup $\Gamma_A(\mathfrak{c})$ for a non-zero A-ideal $\mathfrak{c}$, then $\alpha G \alpha^{-1}$ for $\alpha \in \mathrm{GL}_2(Q(A))$ contains $\Gamma_A(\mathfrak{c}')$ for another non-zero A-ideal $\mathfrak{c}'$ depending on α.*

Proof. We give a proof assuming $p > 2$. Write $\Gamma(\mathfrak{c})$ for $\Gamma_A(\mathfrak{c})$. We may suppose that $G = \Gamma(\mathfrak{c})$ for $\mathfrak{c} \subset \mathfrak{m}_A$; so, G is p-profinite. Then $\mathcal{M}(G) \supset \mathfrak{c}^2 \cdot \mathfrak{L}$ for $\mathfrak{L} = M_2(A)$. Replacing α by $\xi\alpha$ for a suitable $\xi \in A \cap Q(A)^\times$ for the quotient field $Q(A)$ of A, we may assume that $\alpha \in M_2(A) \cap \mathrm{GL}_2(Q(A))$. Then $(\alpha \mathfrak{L} \alpha^{-1} \cap \mathfrak{L}) \supset \alpha \mathfrak{L} \alpha^\iota$ for $\alpha^\iota = \det(\alpha)\alpha^{-1} \in M_2(A)$. Since $\mathfrak{L}$ and $\alpha \mathfrak{L} \alpha^\iota$ are both free A-module of rank 4, $\mathfrak{L}/\alpha \mathfrak{L} \alpha^\iota$ is a torsion A-module finite type annihilated by a non-zero A-ideal $\mathfrak{c}''$. Then $\mathcal{M}(\alpha \Gamma(\mathfrak{c}) \alpha^{-1} \cap \mathrm{SL}_2(A)) \supset \mathfrak{c}^2 \cdot \alpha \mathfrak{L} \alpha^{-1} \supset \mathfrak{c}^2 \mathfrak{c}'' \mathfrak{L}$. Thus the ideal $\mathfrak{c}_\alpha = \mathfrak{c}^2 \mathfrak{c}''$ does the job. □

Let $\mathcal{B}_{/\mathbb{Z}_p} \subset \mathrm{GL}(2)_{/\mathbb{Z}_p}$ (respectively $\mathcal{Z}_{/\mathbb{Z}_p}$) be the upper triangular Borel subgroup (respectively the center of $\mathrm{GL}(2)_{/\mathbb{Z}_p}$) as an algebraic group. Write $\mathcal{U}_{/\mathbb{Z}_p}$ for the unipotent radical of $\mathcal{B}_{/\mathbb{Z}_p}$, and put $\mathcal{ZU}(A) = \mathcal{Z}(A)\mathcal{U}(A) \subset \mathrm{GL}_2(A)$. Let $\mathfrak{B}_{/\mathbb{Z}_p}$ (respectively $\mathfrak{U}_{/\mathbb{Z}_p}$) be the Lie algebra of $\mathcal{B}_{/\mathbb{Z}_p}$ (respectively $\mathcal{U}_{/\mathbb{Z}_p}$). We write $\mathcal{B} = \mathbb{G}_m^2 \ltimes \mathcal{U}$ by the splitting $\mathbb{G}_m^2 \ni (a, a') \mapsto \left(\begin{smallmatrix}a & 0\\ 0 & a'\end{smallmatrix}\right) \in \mathcal{B}$. Define $t^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n \in \Lambda$.

LEMMA 1.3. *Suppose $p > 2$, and let $\mathbb{I}$ be a domain finite flat over Λ. Let $\mathbb{G} \subset \mathrm{SL}_2(\mathbb{I})$ be a p-profinite subgroup. Suppose the following two conditions.*

(B) *The group $\mathbb{G}$ contains a subgroup of $\mathcal{B}(\mathbb{I}) \cap \mathrm{SL}_2(\mathbb{I})$ which is, under the projection: $\mathcal{B} \to \mathcal{B}/\mathcal{Z}\mathcal{U} = \mathbb{G}_m$, isomorphic to the image of*

$$\mathcal{T} = \left\{ t(s) := \begin{pmatrix} t^{s/2} & 0 \\ 0 & t^{-s/2} \end{pmatrix} \,\middle|\, s \in \mathbb{Z}_p \right\} \cong \Gamma \ (t = 1 + T).$$

(U) *The subgroup $U = \left\{ \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) \mid u \in \Lambda \right\} \cap \mathbb{G}$ is non-trivial.*

We denote by $\mathfrak{u}$ the ideal $\mathfrak{u} = \left\{ u \in \Lambda \mid \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) \in U \right\}$. Let $\mathbb{G}'$ be the topological commutator subgroup of $\mathbb{G}$ and $U' = U \cap \mathbb{G}'$. The group $\mathcal{T}$ acts on U and U' by the conjugate action. Then we have the following.

(1) *The action of $\mathbb{Z}_p[[\mathcal{T}]]$ on U and U' coincides with the action of Λ via the isomorphism $\mathbb{Z}_p[[\mathcal{T}]] \cong \Lambda$ sending $t(1)$ to t (under the notation in (B)). Under this identification, U/U' is torsion of finite type (as a Λ-module) killed by the ideal (T) of Λ.*

(2) *If moreover there exists $g = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{B}(\mathbb{I}) \cap \mathbb{G}$ whose image in $\mathcal{B}(\mathbb{I})/\mathcal{Z}\mathcal{U}(\mathbb{I})$ is non-trivial, U/U' is killed by $ad^{-1} - 1$. If $ad^{-1} - 1$ is prime to T, U/U' is finite.*

Replacing the pair (U, U') by $(\mathbb{U} = \mathbb{G} \cap \mathcal{U}(\mathbb{I}), \mathbb{U}' = \mathbb{G}' \cap \mathcal{U}(\mathbb{I}))$, the same assertions (1–2) hold under the condition $\mathbb{U} \neq 1$.

Proof. Since the proof is the same for (U, U') and $(\mathbb{U}, \mathbb{U}')$, we give a proof for the pair (U, U'). Often we identify $\mathfrak{u}$ with the Lie subalgebra $\left\{ \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mid b \in \mathfrak{u} \right\}$ in $\mathfrak{sl}_2(\Lambda)$. Under this identification, by definition, we have $U = 1 + \mathfrak{u} \subset \mathbb{G}$. Since U and $\mathbb{G}'$ are normalized by the adjoint (conjugation) action of $\mathbb{G} \cap \mathcal{B}(\Lambda)\mathcal{U}(\mathbb{I})$, $\mathcal{T} \hookrightarrow \mathcal{B}(\mathbb{I})/\mathcal{Z}\mathcal{U}(\mathbb{I})$ acts on U and U'. Then the $\mathbb{Z}_p$-module U/U' carries a continuous action of Γ via $\Gamma = \{t^s \mid s \in \mathbb{Z}_p\} \cong \mathcal{T}$. Note that $\mathbb{Z}_p[[\Gamma]] = \Lambda$. Since the Λ-module structure on U induced by the adjoint action of $\mathcal{T}$ and the one induced by the isomorphism $\log : U \ni (1+u) \mapsto u \in \mathfrak{u}$ match, $U \cong \mathfrak{u} \subset \mathfrak{sl}_2(\Lambda)$ is a Λ-module of finite type (as Λ is noetherian). Thus U/U' is a Λ-module of finite type embedded in $\mathbb{G}/\mathbb{G}'$. Pick $\tau \in \mathcal{B}(\mathbb{I}) \cap \mathbb{G}$ whose image in $\mathcal{T}$ is equal to $\left(\begin{smallmatrix} t^{1/2} & 0 \\ 0 & t^{-1/2} \end{smallmatrix}\right)$. Then $\tau - 1$ acts on U/U' by multiplication by T and kills $\mathbb{G}/\mathbb{G}'$. Thus T is in the annihilator $\mathrm{Ann}(U/U')$ of U/U' as asserted in (1).

If we have further $g = \left(\begin{smallmatrix} a & * \\ 0 & d \end{smallmatrix}\right) \in \mathbb{G} \cap \mathcal{B}(\mathbb{I})$ as in (2), by the same argument, U/U' is killed by $ad^{-1} - 1 \neq 0$. Thus U/U' is a module over a finite extension $\Lambda[\theta] \subset \mathbb{I}$ of Λ for $\theta = ad^{-1} - 1$. Taking a minimal polynomial $\Phi(X)$ of θ over Q, we have $\Lambda[\theta] \cong \Lambda[X]/(\Phi(X))$; so, $\Lambda[\theta]$ is finite flat over Λ. If θ is prime to T, U/U' is killed by an open ideal (θ, T) of $\Lambda[\theta] \subset \mathbb{I}$. Since U/U' is a Λ-module of finite type, it is a finite Λ-module. □

Here is another easy remark.

LEMMA 1.4. *Let the notation and the assumption be as in Lemma 1.3. In addition, we assume that we have $j = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta' \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that $j\mathbb{G}j^{-1} = \mathbb{G}$ and $\zeta - \zeta' \in \mathbb{Z}_p^\times$. Then the group $\mathbb{G}$ contains the subgroup $\mathcal{T}$; in particular, the group $\mathcal{Z}(\Lambda)\mathcal{T} \subset \mathrm{SL}_2(\Lambda)$ normalizes $\mathbb{G}$.*

Proof. Forgetting about the center $\mathcal{Z}(\Lambda)$, we only need to show that $\mathcal{T}$ normalizes $\mathbb{G}$. By assumption, there exists $\tau \in \mathbb{G}$ of the form $\tau = \left(\begin{smallmatrix} a & u \\ 0 & a^{-1} \end{smallmatrix}\right)$ for $a = t^{1/2}$. By computation, for the commutator (τ, j), we have $(\tau, j) = \left(\begin{smallmatrix} 1 & ua(1-\zeta\zeta'^{-1}) \\ 0 & 1 \end{smallmatrix}\right) \in \mathbb{G}$. Thus $\mathbb{U} = \mathcal{U}(\mathbb{I}) \cap \mathbb{G}$ contains $\left(\begin{smallmatrix} 1 & ua(1-\zeta\zeta'^{-1}) \\ 0 & 1 \end{smallmatrix}\right)$. Since $\mathbb{U}$ is a $\mathbb{Z}_p$-module, we can divide elements in $\mathbb{U}$ by the $\mathbb{Z}_p$-unit $(1 - \zeta\zeta'^{-1})$; so, $\mathbb{U}$ contains $\left(\begin{smallmatrix} 1 & ua \\ 0 & 1 \end{smallmatrix}\right)$ and $\tau^{-1}\left(\begin{smallmatrix} 1 & ua \\ 0 & 1 \end{smallmatrix}\right)\tau = \left(\begin{smallmatrix} 1 & a^{-1}u \\ 0 & 1 \end{smallmatrix}\right) =: \beta \in \mathbb{U}$. Then $\mathbb{G}$ contains $\tau\beta^{-1} = t(1) = \left(\begin{smallmatrix} t^{1/2} & 0 \\ 0 & t^{-1/2} \end{smallmatrix}\right)$, and $\mathbb{G}$ contains $\mathcal{T} = \{t(1)^s \mid s \in \mathbb{Z}_p\}$ which in particular normalizes $\mathbb{G}$. □

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

For a prime divisor P of $\mathrm{Spec}(\Lambda)$, we write A_0 for the subring $\mathbb{Z}_p \subset \kappa(P)$ if $\kappa(P)$ is of characteristic 0, and if $P = (p)$, we put $A_0 = \mathbb{F}_p[[T]] = \Lambda/P \subset \kappa(P)$.

Lemma 1.5. *Let the notation and the assumption be as in Lemma 1.3. Put $G = \mathbb{G} \cap \mathrm{SL}_2(\Lambda)$ and let G_U be the subgroup of G topologically generated by gUg^{-1} for all $g \in G$. If there exists a prime divisor $P \in \mathrm{Spec}(\Lambda)$ such that the image of G_U in $\mathrm{SL}_2(\Lambda/P)$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, then we can find a Λ-module $\mathfrak{L} \subset \mathcal{M}(G) \cap \mathfrak{sl}_2(\Lambda)$ such that $\mathfrak{sl}_2(\Lambda)/\mathfrak{L}$ is Λ-torsion with $\mathfrak{sl}_2(\Lambda_P)/\mathfrak{L}_P = 0$ after localization and $\mathfrak{L} \subset \mathcal{M}(G_U) \cap \mathfrak{sl}_2(\Lambda) \subset \mathcal{M}(G) \cap \mathfrak{sl}_2(\Lambda) \subset \mathfrak{sl}_2(\Lambda)$. Moreover G_U contains $\Gamma_\Lambda(\mathfrak{c})$ for a non-zero Λ-ideal $\mathfrak{c} = \{\lambda \in \Lambda \mid \lambda \cdot M_2(\Lambda) \subset \mathcal{M}(G_U)\}$ prime to P.*

Proof. As before, we identify $\mathfrak{u}$ with the Lie subalgebra $\left\{\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) | b \in \mathfrak{u}\right\}$ in $\mathfrak{sl}_2(\Lambda)$; then $U = 1 + \mathfrak{u}$. Let $\overline{H}$ (respectively $\overline{\mathfrak{H}}$) be the image of a subgroup H (respectively a submodule $\mathfrak{H}$) of $\mathrm{SL}_2(\Lambda)$ (respectively of $\mathfrak{sl}_2(\Lambda)$) in $\mathrm{SL}_2(\Lambda/P)$ (respectively in $\mathfrak{sl}_2(\Lambda/P)$). If G'_U is the topological commutator subgroup of G_U, its image $\overline{G}'_U$ in $\mathrm{SL}_2(\Lambda/P)$ is the topological commutator subgroup of $\overline{G}_U$. Since $\overline{G}_U$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, $\overline{G}'_U$ contains an open subgroup of $\mathrm{SL}_2(A_0)$. Since $G' \supset G'_U$, we find $U' = G' \cap U \supset U'' := G'_U \cap U$. In any case, we find $\overline{U} = 1 + \overline{\mathfrak{u}} \neq 1$, where $\overline{\mathfrak{u}}$ is the image of $\mathfrak{u}$ in $\mathfrak{sl}_2(\Lambda/P)$ (so, $\overline{\mathfrak{u}} \neq 0$). By Lemma 1.3, $U' = U \cap G'$ is non-trivial, and if $P \nmid T$, $\mathfrak{u}' = \{u \in \mathfrak{sl}_2(\Lambda) \mid 1 + u \in U'\}$ is a non-trivial Lie Λ-subalgebra of $\mathfrak{sl}_2(\Lambda)$ with non-trivial image $\overline{\mathfrak{u}}'$ in $\mathfrak{sl}_2(\Lambda/P)$. Even if $P \mid T$, since $\overline{G}'_U$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, $\overline{U}'' \subset \overline{U}'$ is non-trivial; so, $\overline{\mathfrak{u}}' \neq 0$. Let $H \subset G'$ be the subgroup generated by $gU'g^{-1}$ for all $g \in G$. Let $\mathcal{M} = \mathcal{M}(G_U)$ and $\overline{\mathcal{M}} = \mathcal{M}(\overline{G}_U)$. Then we have a natural surjection $\pi : \mathcal{M} \twoheadrightarrow \overline{\mathcal{M}}$ given by $x \mapsto x \bmod P$ for $x \in M_2(\Lambda)$. Let $\mathfrak{L} = \sum_{g \in G_U} g\mathfrak{u}'g^{-1} \subset \mathcal{M} \cap \mathfrak{sl}_2(\Lambda)$ and $\overline{\mathfrak{L}} = \sum_{g \in \overline{G}_U} g\overline{\mathfrak{u}}'g^{-1} \subset \overline{\mathcal{M}} \cap \mathfrak{sl}_2(\Lambda/P)$. As seen in the proof of Lemma 1.3, $\mathfrak{u}'$ is a torsion-free Λ-submodule of $\mathfrak{sl}_2(\Lambda)$; so, $\mathfrak{L}$ is a torsion-free Λ-submodule of $\mathfrak{sl}_2(\Lambda)$. Note that $\mathfrak{L}$ is stable under the adjoint action of G_U. Since $\overline{G}_U$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, the adjoint action of $\overline{G}_U$ on $\overline{\mathfrak{L}}$ is irreducible; so, $\overline{\mathfrak{L}} \otimes_\Lambda \kappa(P)$ has dimension 3 over $\kappa(P)$; so, $\overline{\mathfrak{L}} \otimes_\Lambda \kappa(P) = \mathfrak{sl}_2(\kappa(P))$. By Nakayama's lemma, we have $\mathfrak{L}_P = \mathfrak{sl}_2(\Lambda_P)$. In particular, $\mathfrak{sl}_2(\Lambda)/\mathfrak{L}$ is a Λ-torsion module of finite type. The Lie algebra $L = \mathcal{M}^0$ contains $\mathfrak{L}$, and hence $L \cdot L \supset \mathfrak{L} \cdot \mathfrak{L}$. For the annihilator $\mathfrak{a}$ of $\mathfrak{sl}_2(\Lambda)/\mathfrak{L}$, by a simple computation $\mathcal{M}$ contains $\widetilde{L} = \mathfrak{a}^2 \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \oplus \mathfrak{L} \subset M_2(\Lambda)$. Since $\mathfrak{L}_P = \mathfrak{sl}(\Lambda_P)$, $\mathfrak{a}$ is prime to P. Thus for the maximal Λ-submodule $\widetilde{\mathcal{M}}$ of $\mathcal{M}$, we conclude $\widetilde{\mathcal{M}} \supset \widetilde{L}$, and $M_2(\Lambda)/\widetilde{\mathcal{M}}$ is a torsion Λ-module. Thus the annihilator ideal $\mathfrak{c}$ of $M_2(\Lambda)/\widetilde{\mathcal{M}}$ is prime to P and $G_U \supset \Gamma_\Lambda(\mathfrak{c})$. □

Question 1.6. Under the conditions (B) and (U) in Lemma 1.3, are $\mathcal{M}(G)$ and $\mathcal{M}(\mathbb{G})$ Λ-modules? It is likely to be the case up to finite error, and if they are, our argument in the rest of the paper could be simplified a lot. They are obviously stable under the adjoint action of $\mathcal{T}$.

2. Fullness of Lie algebra

We start with the following well-known fact whose proof is left to the reader.

Lemma 2.1. *Let K be a field of characteristic 0. If $\mathfrak{L}$ is a non-trivial proper Lie subalgebra over K in $\mathfrak{sl}_2(K)$, then $\mathfrak{L}$ is a conjugate in $\mathfrak{sl}_2(K)$ of one of the following Lie K-subalgebras:*

(1) $\{x \in M \mid \mathrm{Tr}_{M/\mathbb{Q}}(x) = 0\}$ *as an abelian Lie subalgebra for a semi-simple quadratic extension M of K (Cartan subalgebra);*
(2) $\mathfrak{U}_{/K} = \left\{\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right) \mid x \in K\right\}$ *(nilpotent subalgebra);*
(3) $\mathfrak{B}_{/K} = \left\{\left(\begin{smallmatrix} a & x \\ 0 & -a \end{smallmatrix}\right) \mid a, x \in K\right\}$ *(Borel subalgebra).*

Corollary 2.2. *Let $K \neq \mathbb{F}_3$ be a field of characteristic different from 2 and L/K be a field extension. Let $0 \neq \mathfrak{L} \subset \mathfrak{sl}_2(L)$ be a vector K-subspace stable under the adjoint action of $\mathrm{SL}_2(K)$. Then there exists $g \in \mathrm{GL}_2(L)$ such that $g\mathfrak{L}g^{-1} \supset \mathfrak{sl}_2(K)$. If $\mathfrak{L}$ contains some non-zero elements in $\mathfrak{sl}_2(K)$, $\mathfrak{L}$ contains $\mathfrak{sl}_2(K)$ without conjugation.*

Proof. Put $\mathfrak{n}(X) = \{\left(\begin{smallmatrix}0 & x\\ 0 & 0\end{smallmatrix}\right) \in \mathfrak{sl}_2(X) \mid x \in X\}$ for any intermediate extension $L/X/K$. As $K \neq \mathbb{F}_2$ and $\mathbb{F}_3$, we have some diagonal matrix $g = \left(\begin{smallmatrix}a & 0\\ 0 & a^{-1}\end{smallmatrix}\right)$ in $\mathrm{SL}_2(K)$ with $a^2 \neq a^{-2}$. The space $\mathfrak{n}(X)$ is the eigenspace in $\mathfrak{sl}_2(X)$ of $\mathrm{Ad}(g)$ with eigenvalue a^2. Since adjoint action: $Y \mapsto gYg^{-1}$ ($Y \in \mathfrak{sl}_2(L)$) of $g \in \mathrm{SL}_2(K)$ is absolutely irreducible (as K has characteristic $\neq 2$), we see that $\mathfrak{L}$ spans $\mathfrak{sl}_2(L)$ over L, and hence the eigenspace $\mathfrak{L}(a^2)$ in $\mathfrak{L}$ of $\mathrm{Ad}(g)$ with eigenvalue a^2 is non-trivial. In particular, $\mathfrak{L} \cap \mathfrak{n}(L) = \mathfrak{L}(a^2) \neq 0$. Let T be the diagonal torus in GL_2; so, $T(X) = \{\left(\begin{smallmatrix}a & 0\\ 0 & b\end{smallmatrix}\right) \in \mathrm{GL}_2(X) \mid a, b \in K^\times\}$. Note that $T(X)$ acts transitively on $\mathfrak{n}(X)\backslash\{0\}$. Thus conjugating $\mathfrak{L}$ by an element of $T(L)$, we may assume that $\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right) \in \mathfrak{L}$. Since the adjoint action of $\mathrm{SL}_2(K)$ on $\mathfrak{sl}_2(K)$ is absolutely irreducible, $\mathfrak{L} \cap \mathfrak{sl}_2(K) \neq \{0\}$ implies $\mathfrak{L} \supset \mathfrak{sl}_2(K)$, as desired. □

Here is a well-known corollary (whose proof can be found in [Hid11a, Corollary 4.3.14]).

Corollary 2.3. *If G is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ of infinite order, then G has one of the following four forms:*

1. *G is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$;*
2. *G is an open subgroup of the normalizer of $M^\times \cap \mathrm{SL}_2(\mathbb{Q}_p)$ for a semi-simple quadratic extension $M_{/\mathbb{Q}_p} \subset M_2(\mathbb{Q}_p)$;*
3. *G is $\mathrm{SL}_2(\mathbb{Z}_p)$-conjugate to an open subgroup of the upper triangular Borel subgroup $\mathcal{B}(\mathbb{Z}_p) \subset \mathrm{SL}_2(\mathbb{Z}_p)$;*
4. *G is $\mathrm{SL}_2(\mathbb{Z}_p)$-conjugate to an open subgroup of the upper triangular unipotent subgroup $\mathcal{U}(\mathbb{Z}_p) \subset \mathrm{SL}_2(\mathbb{Z}_p)$.*

Lemma 2.4. *Suppose that $p > 2$ and let A be an integral domain finite flat over $\mathbb{F}_p[[T]]$. If a closed subgroup G of $\mathrm{SL}_2(A)$ contains $\overline{\mathcal{T}} := \{\left(\begin{smallmatrix}t^s & 0\\ 0 & t^{-s}\end{smallmatrix}\right) \mid s \in \mathbb{Z}_p\}$ and non-trivial upper unipotent and lower unipotent subgroups, then G contains an open subgroup of $\mathrm{SL}_2(\mathbb{F}_p[[T]])$, and if G is p-profinite, $\mathcal{M}(G)$ contains an open submodule of $M_2(\mathbb{F}_p[[T]])$.*

Proof. Replacing G by $G \cap \Gamma_A(\mathfrak{m}_A)$, we may assume that G is p-profinite. Writing $K = \mathbb{F}_p((T))$ and $L = A \otimes_{\mathbb{F}_p[[T]]} K$, L is a finite field extension of K. Consider the X-span $\mathfrak{L}_X$ of $\mathcal{M}_1^0(G)$ for $X = K, L$. Then $\dim_L \mathfrak{L}_L = 3$; so, $\mathfrak{L}_L = \mathfrak{sl}_2(L)$. Thus up to conjugation, $\mathfrak{L}_K$ contains $\mathfrak{sl}_2(K)$ by the existence of non-trivial unipotent elements. Thus we may assume that $A = \mathbb{F}_p[[T]]$. By conjugation action of $\overline{\mathcal{T}}$, the unipotent groups $U = \mathcal{U}(\mathbb{F}_p[[T]]) \cap G$ and $U_t = {}^t\mathcal{U}(\mathbb{F}_p[[T]]) \cap G$ are non-zero $\mathbb{F}_p[[T]]$-modules, thus $[\mathcal{U}(\mathbb{F}_p[[T]]) : U] < \infty$ and $[{}^t\mathcal{U}(\mathbb{F}_p[[T]]) : U_t] < \infty$. Let $\mathfrak{u}$ (respectively $\mathfrak{u}_t$) be the Lie algebra of U (respectively U_t); so, for example, $\mathfrak{u} = \{u - 1 \in \mathfrak{sl}_2(\mathbb{F}_p[[T]]) \mid u \in U\}$. Thus we find that $[\mathfrak{u}, \mathfrak{u}_t] \neq 0$ is also an $\mathbb{F}_p[[T]]$-module in $\mathcal{M}^0(G)$, and hence $\mathcal{M}^0(G)$ has rank 3 over $\mathbb{F}_p[[T]]$. Also $C = \mathrm{Tr}(\mathcal{M}^0(G) \cdot \mathcal{M}^0(G))$ as in Theorem 1.1 contains $\mathfrak{u}\mathfrak{u}_t$ regarding $\mathfrak{u}$ and $\mathfrak{u}_t$ as an ideal of $\mathbb{F}_p[[T]]$ by an obvious isomorphism $\mathfrak{U}(\mathbb{F}_p[[T]]) \cong {}^t\mathfrak{U}(\mathbb{F}_p[[T]]) \cong \mathbb{F}_p[[T]]$. Then G contains $\Gamma_{\mathbb{F}_p[[T]]}(\mathfrak{u}\mathfrak{u}_t)$, and hence G is open in $\mathrm{SL}_2(\mathbb{F}_p[[T]])$. Note that $\mathcal{M}(G)$ is well defined containing $C \cdot 1_2 \oplus \mathcal{M}^0(G)$ with $\mathrm{rank}_{\mathbb{F}_p[[T]]} \mathcal{M}^0(G) = 3$ and $C \neq 0$. This implies that $\mathcal{M}(G)$ is open in $M_2(\mathbb{F}_p[[T]])$. □

Lemma 2.5. *Let V be a local $\mathbb{Z}_p$-algebra and A be a flat V-algebra. Then for a subgroup B of $\mathcal{B}(V)$ containing $\left(\begin{smallmatrix}\delta & \beta\\ 0 & \delta'\end{smallmatrix}\right)$ with $\delta - \delta' \in V^\times$ and a unipotent element $\left(\begin{smallmatrix}1 & \varepsilon\\ 0 & 1\end{smallmatrix}\right)$ with $\varepsilon \in V^\times$,*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

the semi-group $\mathbb{B} = \{g \in \mathcal{B}(A) \mid gBg^{-1} \subset \mathcal{B}(V)\}$ is contained in $\mathcal{B}(V)$ modulo the center of $\mathrm{GL}_2(A)$. If A is reduced, the same assertion holds replacing $\{g \in \mathcal{B}(A) \mid gBg^{-1} \subset \mathcal{B}(V)\}$ by $\{g \in \mathrm{GL}_2(A) \mid gBg^{-1} \subset \mathcal{B}(V)\}$.

Proof. Take $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(A)$ satisfying $gBg^{-1} \subset \mathcal{B}(V)$; so, we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \varepsilon \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ which immediately implies $c^2 = 0$. Thus if A is reduced $c = 0$, and $g \in \mathcal{B}(A)$. Thus we may assume either $g = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{B}(A)$ or that A is reduced to continue. The identity

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & (a/d)\varepsilon \\ 0 & 1 \end{pmatrix} \in \mathcal{B}(V)$$

implies $d/a, a/d \in V^\times$. Note $g = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b/a \\ 0 & 1 \end{smallmatrix}\right)$. The identity for $u = b/a$

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \delta & \beta \\ 0 & \delta' \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \delta & u(\delta' - \delta) + \beta \\ 0 & 1 \end{pmatrix} \in \mathcal{B}(V)$$

implies $u \in V$. Thus $g = a\left(\begin{smallmatrix} 1 & b/a \\ 0 & d/a \end{smallmatrix}\right) \in \mathcal{Z}(A)\mathcal{B}(V)$. This finishes the proof. □

Lemma 2.6. *Let L/K be a finite field extension and $\mathfrak{s}$ be a Lie K-subalgebra of $\mathfrak{sl}_2(L)$ containing $\mathfrak{U}(K)$. Suppose that we have a diagonal matrix $j \in \mathrm{GL}_2(K)$ such that $\mathfrak{s}$ is stable under the adjoint action $\mathrm{Ad}(j)$ on $\mathfrak{sl}_2(L)$ and $\mathrm{Ad}(j)$ has three distinct eigenvalues on $\mathfrak{sl}_2(K)$. If the L-span $\mathfrak{s}_L := L\cdot\mathfrak{s}$ is equal to $\mathfrak{sl}_2(L)$, then $\mathfrak{s}$ contains $\mathfrak{sl}_2(K)$.*

Proof. The nilradical $\mathfrak{R}$ of $\mathfrak{s}$ is in the nilradical of $\mathfrak{s}_L = \mathfrak{sl}_2(L)$; so, $\mathfrak{R} = 0$, and $\mathfrak{s}$ is semi-simple. Thus we can decompose $\mathfrak{s}$ into a product of simple Lie algebras: $\mathfrak{s} = \mathfrak{s}_1 \oplus \cdots \oplus \mathfrak{s}_n$ for K-simple components $\mathfrak{s}_j$. Since $\mathfrak{s}_m$ is simple (non-trivial), $\dim_K \mathfrak{s}_m = 3$. Thus each $\mathfrak{s}_m$ generates $\mathfrak{sl}_2(L)$ over L. Suppose thats we have more than one simple component of $\mathfrak{s}$. Since $[\mathfrak{s}_m, \mathfrak{s}_n] = 0$ for $m \neq n$, for any $s_? \in \mathfrak{s}_?$ and any $\alpha, \beta \in L$, $[\alpha s_m, \beta s_n] = \alpha\beta[s_m, s_n] = 0$. This implies that for the L-span $L \cdot \mathfrak{s}_?$, we have $[L \cdot \mathfrak{s}_m, L \cdot \mathfrak{s}_n] = 0$; so, $[\mathfrak{sl}_2(L), \mathfrak{sl}_2(L)] = 0$, a contradiction. Thus we conclude $\mathfrak{s}$ is simple. The centralizer of j (i.e. the subalgebra fixed by $\mathrm{Ad}(j)$) in $\mathfrak{s}$ is a Cartan subalgebra $\mathfrak{h}_K$ split over K (as j is diagonal in $\mathrm{GL}_2(K)$ with $\mathrm{Ad}(j)$ having three distinct eigenvalues), and $\mathfrak{h}_0 = \mathfrak{h}_K \cap \mathfrak{sl}_2(K)$ is a split Cartan subalgebra of $\mathfrak{sl}_2(K)$ normalizing $\mathfrak{U}(K)$ in $\mathfrak{s}$. Thus $\mathfrak{s}_K$ is a split K-simple algebra containing an isomorphic image of $\mathfrak{sl}_2(K)$. Therefore, for a subfield $K' \subset L$ containing K, $\mathfrak{s}$ is an inner conjugate of $\mathfrak{sl}_2(K')$; i.e. $\mathfrak{s} = g \cdot \mathfrak{sl}_2(K')g^{-1}$ for $g \in \mathrm{GL}_2(L)$. Since $g \cdot \mathfrak{sl}_2(K')g^{-1} = \mathfrak{s} \supset \mathfrak{h}_0\mathfrak{U}(K) \subset \mathfrak{sl}_2(K)$, we have $g^{-1}\mathfrak{h}_0\mathfrak{U}(K)g \subset \mathfrak{sl}_2(K')$. We can then find $h_1 \in \mathrm{SL}_2(K')$ such that $h_1^{-1}g^{-1}\mathfrak{h}_0\mathfrak{U}(K)gh_1 \subset \mathfrak{h}_0\mathfrak{U}(K')$. Pick $\left(\begin{smallmatrix} 0 & u \\ 0 & 0 \end{smallmatrix}\right) \in h_1^{-1}g^{-1}\mathfrak{h}_0\mathfrak{U}(K)gh_1$ with $0 \neq u \in K'$. Define $h_2 = \left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then, for $h = h_1h_2$, $h^{-1}g^{-1}\mathfrak{h}_0\mathfrak{U}(K)gh \subset \mathfrak{h}_0\mathfrak{U}(K)$. Then by Lemma 2.5, $gh \in K'^\times\mathcal{B}(K)$. Note that $gh \cdot \mathfrak{sl}_2(K')(gh)^{-1} = g \cdot \mathfrak{sl}_2(K')g^{-1}$; so, we may assume that $g \in \mathcal{B}(K)$; so, in particular, $\mathfrak{s} \supset \mathfrak{sl}_2(K)$. This finishes the proof. □

Lemma 2.7. *Let V be a p-profinite discrete valuation ring with quotient field K. If a closed subgroup $H \subset \mathrm{SL}_2(V)^m$ has open image in each factor of $\mathrm{SL}_2(V)$, a conjugate in $\mathrm{GL}_2(K)^m$ of H contains an open subgroup of $\mathrm{SL}_2(V)$ diagonally embedded in $\mathrm{SL}_2(V)^m$.*

Proof. The p-profinite property of V implies that V has finite residue field. We may assume that H is p-profinite. Since the topological commutator subgroup of H still has open image in each factor of $\mathrm{SL}_2(V)$ (cf. [Hid11a, Lemma 4.3.8]), replacing H by its commutator, we may assume that H is basic. The result in Theorem 1.1 can be applied to the semi-local ring $A = V^m$. Consider the closed Lie $\mathbb{Z}_p$-subalgebra $\mathcal{M}_1(H)$ of $\mathfrak{gl}_2(A)$ associated to H and its subalgebra

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

$\mathcal{M}_1^0(H) = \mathcal{M}_1(H) \cap \mathfrak{sl}_2(A)$. Write $\mathfrak{M}$ for the V-span of $\mathcal{M}_1^0(H)$. This Lie algebra $\mathfrak{M}$ is stable under the adjoint action of H. Write $\mathfrak{M}_j$ (respectively H_j) for the projection to the j-th factor $\mathfrak{sl}_2(V)$ (respectively $\mathrm{SL}_2(V)$) of $\mathfrak{M}$ (respectively H). Then $\mathfrak{M}_j$ is the V-span of $\mathcal{M}_1^0(H_j)$. Since $\mathcal{M}_1^0(H_j) \cap \mathfrak{n}(K)$ for the upper nilpotent Lie algebra $\mathfrak{n}(X)$ as in the proof of Corollary 2.2 is an open ideal of V, $\mathcal{M}_1^0(H_j)$ is an open Lie $\mathbb{Z}_p$-subalgebra of $\mathfrak{M}_j$ by the absolute irreducibility of the adjoint action of H_j on $\mathfrak{M}_j$; i.e. $[\mathfrak{M}_j : \mathcal{M}_1^0(H_j)] < \infty$. Then, by our assumption and Corollary 2.2, $\mathfrak{M}_j$ for each j has rank 3 over V. We proceed by induction on m. If the intersection of $\mathfrak{M}$ with one factor $\mathfrak{sl}_2(V)$, say the first one, is non-trivial, the intersection is stable under the adjoint action of $\mathfrak{M}$ and H. Then the intersection projected to the first component has to have an open image in the first component $\mathfrak{sl}_2(V)$ as $\mathfrak{sl}_2(K)$ is a simple Lie algebra. Thus the intersection is either trivial or contains an open subalgebra of $\mathfrak{sl}_2(V)$. If it contains an open subalgebra, we can project H and $\mathfrak{M}$ to the complementary direct summand, and by induction, we get the job done. Thus we may assume that any intersection of $\mathfrak{M}$ with a direct factor $\mathfrak{sl}_2(V)$ is trivial. Thus the projection to the complementary direct summand $\mathfrak{sl}_2(V)^{m-1}$ is an injection. By the induction assumption, conjugating H by an element in $\mathcal{B}(K)^{m-1}$, we may assume that the image of $\mathfrak{M}$ in $\mathfrak{sl}_2(V)^{m-1}$ is contained in the diagonal image $\Delta(\mathfrak{sl}_2(V))$ of $\mathfrak{sl}_2(V)$. Thus we are reduced to the case where $m = 2$ regarding $\mathfrak{M} \subset \mathfrak{sl}_2(V) \times \Delta(\mathfrak{sl}_2(V)) \cong \mathfrak{sl}_2(V)^2$. Then $K \cdot \mathfrak{M} \subset \mathfrak{sl}_2(K)^2$ is a graph of an isomorphism $L : \mathfrak{sl}_2(K) \to \mathfrak{sl}_2(K)$ of Lie K-algebras. As is well known, such an isomorphism is inner given by a conjugation by an element of $\mathrm{GL}_2(K)$. This finishes the proof. □

Corollary 2.8. *Let V be a p-profinite discrete valuation ring with quotient field K, and let $A_0 = \mathbb{Z}_p$ if K has characteristic 0 and $A_0 = \mathbb{F}_p[[T]] \subset V$ if K has characteristic $p > 0$ for an element $T \in V$ analytically independent over $\mathbb{F}_p$. If a closed subgroup $H \subset \mathrm{SL}_2(V)^m$ has image in each factor of $\mathrm{SL}_2(V)$ containing an open subgroup of $\mathrm{SL}_2(A_0)$ up to conjugation in $\mathrm{GL}_2(K)$, then a conjugate in $\mathrm{GL}_2(K)^m$ of H contains an open subgroup of $\mathrm{SL}_2(A_0)$ diagonally embedded in $\mathrm{SL}_2(V)^m$.*

Proof. If a p-profinite subgroup G of $\mathrm{SL}_2(V)$ contains up to conjugation an open subgroup of $\mathrm{SL}_2(A_0)$, we have $K \cdot \mathcal{M}^0(G) = \mathfrak{sl}_2(K)$ as the adjoint action of G on both sides of the identity is absolutely irreducible; so, $V \cdot \mathcal{M}^0(G)$ is an open Lie subalgebra of $\mathfrak{sl}_2(V)$. We apply the argument which proves Lemma 2.7 to the Lie algebra $V \cdot \mathcal{M}^0(H)$ which has projection to each factor $\mathfrak{sl}_2(V)$ with open image. Then after conjugation, $V \cdot \mathcal{M}^0(H)$ contains the diagonal image of an open Lie V-subalgebra of $\mathfrak{sl}_2(V)$. Thus $\mathcal{M}^0(H)$ must contain an open Lie V-subalgebra of $\mathfrak{sl}_2(A_0)$, which implies that H contains an open subgroup of $\mathrm{SL}_2(A_0)$ diagonally embedded into $\mathrm{SL}_2(V)^m$. □

Recall the quotient field Q of Λ. As before, we fix a domain $\mathbb{I}$ finite flat over Λ. For $g \in \mathrm{GL}_2(\mathbb{I})$ and $x \in \mathfrak{sl}_2(\mathbb{I})$, we write $\mathrm{Ad}(g)(x) = gxg^{-1}$ (the adjoint action of g). Hereafter we assume $p > 2$. The following lemma will be applied to $\mathbb{G} = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_\Lambda(\mathfrak{m}_\Lambda)$ to show that $\mathrm{Im}(\rho_{\mathbb{I}})$ for a non-CM component $\mathbb{I}$ contains a congruence subgroup $\Gamma_\Lambda(\mathfrak{c})$. A main idea is to reduce the problem to openness of $\mathrm{SL}_2(A_0) \cap \mathrm{Im}(\rho_{P\mathbb{I}})$ in $\mathrm{SL}_2(A_0)$ for a prime divisor $P \in \mathrm{Spec}(\Lambda)$. The proof is onerous if $\mathbb{I} \neq \Lambda$ as $\mathbb{I}/P\mathbb{I}$ may not be even a reduced ring. We use Lemma 2.7 and Lemma 2.8 at step (c) in the proof (if $\mathbb{I} \neq \Lambda$) to reduce this problem to the containment of an open subgroup of $\mathrm{SL}_2(A_0)$ in $\mathrm{Im}(\rho_{\mathfrak{P}})$ for prime divisors $\mathfrak{P} \mid P$ of $\mathbb{I}$ (which is shown by Ribet in our application when P is arithmetic).

Lemma 2.9. *Let $G = \mathbb{G} \cap \mathrm{SL}_2(\Lambda)$ for a p-profinite subgroup $\mathbb{G}$ of $\mathrm{SL}_2(\mathbb{I})$ satisfying condition (B) of Lemma 1.3. Let P be a prime divisor of Λ. Suppose that $\mathbb{I}$ is an integrally closed domain flat over Λ and one of the following conditions on existence of elements j, υ in $\mathrm{GL}_2(\mathbb{I})$:*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

(1) *there exists* $j \in \mathcal{B}(\mathbb{I})$ *with* $j\mathbb{G}j^{-1} = \mathbb{G}$ *such that the three eigenvalues of* $\mathrm{Ad}(j)$ *are in* $\mathbb{Z}_p$ *distinct modulo* $\mathfrak{m}_{\mathbb{I}}$*;*

(2) *there exists* $j \in \mathcal{B}(\mathbb{I})$ *with* $j\mathbb{G}j^{-1} = \mathbb{G}$ *and* $\upsilon \in \mathbb{G} \cap \mathcal{U}(\mathbb{I})$ *such that the two eigenvalues of* j *are in* $\mathbb{Z}_p$ *distinct modulo* $\mathfrak{m}_{\mathbb{I}}$ *and that* υ *is non-trivial modulo* $\mathfrak{m}_{\mathbb{I}}$*;*

(3) *there exists* $j \in \mathcal{B}(\mathbb{I})$ *with* $j\mathbb{G}j^{-1} = \mathbb{G}$ *and* $\upsilon \in \mathbb{G} \cap \mathcal{U}(\mathbb{I})$ *such that the two eigenvalues of* j *are in* $\mathbb{Z}_p$ *distinct modulo* $\mathfrak{m}_{\mathbb{I}}$ *and that* υ *is non-trivial modulo* $\mathfrak{P}$ *for all prime ideals* $\mathfrak{P}|P$*.*

If the image $\overline{\mathbb{G}}_{\mathfrak{P}}$ *of* $\mathbb{G}$ *in* $\mathrm{SL}_2(\mathbb{I}/\mathfrak{P})$ *for every prime divisor* $\mathfrak{P}|P$ *in* $\mathbb{I}$ *contains, up to conjugation, an open subgroup of* $\mathrm{SL}_2(A_0)$*, then there exists a non-zero ideal* $\mathfrak{c}$ *in* Λ *prime to* P *and* $\alpha \in \mathcal{B}(\mathbb{I}_P)$ *such that* $\alpha \cdot G\alpha^{-1} \supset \Gamma_\Lambda(\mathfrak{c})$*. In particular, the image* $\overline{\alpha}\overline{G}_P\overline{\alpha}^{-1}$ *of* $\alpha G\alpha^{-1}$ *in* $\mathrm{SL}_2(\mathbb{I}_P/P\mathbb{I}_P)$ *contains an open subgroup of* $\mathrm{SL}_2(A_0)$*, and replacing* G *by* $\alpha \cdot G\alpha^{-1}$*, the subgroups* $U = G \cap \mathcal{U}(\Lambda)$ *and* $U_t = G \cap {}^t\mathcal{U}(\Lambda)$ *for the opposite unipotent subgroup* ${}^t\mathcal{U}$ *are both non-trivial with non-zero image in* $\mathrm{GL}_2(\Lambda/P)$*. If assumption (2) holds, we can choose* $\alpha \in \mathcal{B}(\mathbb{I})$*.*

Proof. Replacing j by $\lim_{n\to\infty} j^{p^n}$, we may assume that j has finite order with two eigenvalues in $\mathbb{Z}_p$ distinct modulo $\mathfrak{m}_\Lambda$; and hence is semi-simple. Write $j = \left(\begin{smallmatrix}\zeta & * \\ 0 & \zeta'\end{smallmatrix}\right) \in \mathcal{B}(\mathbb{I})$. Conjugating G by $\alpha_0 = \left(\begin{smallmatrix}1 & */(\zeta-\zeta') \\ 0 & 1\end{smallmatrix}\right) \in \mathcal{U}(\mathbb{I})$, we assume that $j = \left(\begin{smallmatrix}\zeta & 0 \\ 0 & \zeta'\end{smallmatrix}\right)$ normalizes $\alpha_0\mathbb{G}\alpha_0^{-1} \subset \mathrm{GL}_2(\Lambda)$. We replace $\mathbb{G}$ by $\alpha_0\mathbb{G}\alpha_0^{-1}$. By Lemma 1.4, we have the group $\mathcal{T}$ contained in $\mathbb{G}$. Since α_0 commutes with upper unipotent element, this does not affect υ in condition (2) or (3). Write $\upsilon = \left(\begin{smallmatrix}1 & u \\ 0 & 1\end{smallmatrix}\right)$. We have

$$u \in \mathbb{I}^\times \text{ under (2)}, \quad \text{and} \quad u \in \mathbb{I}_P^\times \text{ under (3)}. \tag{2.1}$$

Conjugating by $\alpha_1 = \left(\begin{smallmatrix}u^{-1} & 0 \\ 0 & 1\end{smallmatrix}\right)$, under either (2) or (3), we have $\upsilon = \left(\begin{smallmatrix}1 & 1 \\ 0 & 1\end{smallmatrix}\right) \in G$. Since $(t(s), \upsilon) = t(s)\upsilon t(s)^{-1}\upsilon^{-1} = \left(\begin{smallmatrix}1 & t^s-1 \\ 0 & 1\end{smallmatrix}\right)$ for $t(s)$ in (B) of Lemma 1.3, in either case, we have $\mathcal{U}(\Lambda) \subset G$.

First, we assume $\mathbb{I} = \Lambda$ and (1) and prove the lemma. Thus $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$. We have the adjoint operator $\mathrm{Ad}(j)$ acting on $M_2(\mathbb{I})$, $\mathcal{M} = \mathcal{M}(\mathbb{G})$ and $\overline{\mathcal{M}} = \mathcal{M}(\overline{\mathbb{G}}_{\mathfrak{P}})$. Write three eigenvalues of $\mathrm{Ad}(j)$ as $a = \zeta\zeta'^{-1}$, 1 and a^{-1}. Then for $X = M_2(\mathbb{I})$, $\mathcal{M}$ and $\overline{\mathcal{M}}$, we have a decomposition $X = X[a] \oplus X[1] \oplus X[a^{-1}]$ into the direct sum of eigenspaces $X[\lambda]$ with eigenvalue λ. The reduction map $\mathcal{M}[\lambda] \to \overline{\mathcal{M}}[\lambda]$ modulo $\mathfrak{Q}$ is a surjective map for any prime $\mathfrak{Q} \in \mathrm{Spec}(\mathbb{I})$. If $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, we find that $\overline{\mathcal{M}}[\lambda]$ is non-trivial for all eigenvalues λ, and hence $\mathcal{M}[\lambda] \neq 0$ surjects down to $\overline{\mathcal{M}}[\lambda]$. Since $\mathcal{M}[a] = \mathcal{M} \cap \mathfrak{U}(\mathbb{I})$, we find $U = 1 + \mathcal{M}[a] \subset \mathbb{G}'$ maps onto $\overline{U} = 1 + \overline{\mathcal{M}}[a] \subset \overline{\mathbb{G}}'_{\mathfrak{P}}$. Similarly $U_t = 1 + \mathcal{M}[a^{-1}] \subset \mathbb{G}'$ maps onto $\overline{U}_t = 1 + \overline{\mathcal{M}}[a^{-1}] \subset \overline{\mathbb{G}}'_{\mathfrak{P}}$. Since $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, the two eigenspaces $\overline{\mathcal{M}}[a]$ and $\overline{\mathcal{M}}[a^{-1}]$ are both non-trivial; so, $\overline{U} \neq 1$ and $\overline{U}_t \neq 1$. Since $\mathfrak{u} = \left\{b \in \mathbb{I} \mid \left(\begin{smallmatrix}1 & b \\ 0 & 1\end{smallmatrix}\right) \in U\right\}$ and $\mathfrak{u}_t = \left\{c \in \mathbb{I} \mid \left(\begin{smallmatrix}1 & 0 \\ c & 1\end{smallmatrix}\right) \in U_t\right\}$ are non-zero $\mathbb{I}$-ideals, $\overline{U} \neq 1$ and $\overline{U}_t \neq 1$ implies $\mathfrak{u}$ and $\mathfrak{u}_t$ are prime to $\mathfrak{P}$. We often identify $\mathfrak{u}$ (respectively $\mathfrak{u}_t$) with the corresponding Lie algebra $\left\{\left(\begin{smallmatrix}0 & b \\ 0 & 0\end{smallmatrix}\right) \mid b \in \mathfrak{u}\right\} = \mathfrak{U}(\mathbb{I}) \cap \mathcal{M}_1(\mathbb{G})$ (respectively ${}^t\mathfrak{U}(\mathbb{I}) \cap \mathcal{M}_1(\mathbb{G})$). Therefore $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains open subgroups $\overline{U}$ of $\mathcal{U}(\mathbb{I}/\mathfrak{P})$ and $\overline{U}_t$ of ${}^t\mathcal{U}(\mathbb{I}/\mathfrak{P})$. This implies that $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup H of $\mathrm{SL}_2(\mathbb{I}/\mathfrak{P})$ as $\overline{U}$ and $\overline{U}_t$ generate an open subgroup of $\mathrm{SL}_2(\mathbb{I}/\mathfrak{P})$. Indeed, for $b \in \mathfrak{u}$ and $c \in \mathfrak{u}_t$, taking $X = \left(\begin{smallmatrix}0 & b \\ 0 & 0\end{smallmatrix}\right)$ and $Y = \left(\begin{smallmatrix}0 & 0 \\ c & 0\end{smallmatrix}\right)$, we have in $\mathcal{M}(H)$ the element

$$[X, Y] = XY - YX = \begin{pmatrix} bc & 0 \\ 0 & -bc \end{pmatrix}.$$

Similarly, by Theorem 1.1, $\mathcal{M}(H)$ contains $\mathrm{Tr}\left(\left(\begin{smallmatrix}0 & a \\ 0 & 0\end{smallmatrix}\right)\left(\begin{smallmatrix}0 & 0 \\ b & 0\end{smallmatrix}\right)\right) = ab$ as a central element; so, it contains $\mathfrak{u}\mathfrak{u}_t M_2(\mathbb{I})$; i.e. $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup $\Gamma_{\mathbb{I}}(\mathfrak{u}\mathfrak{u}_t)/\Gamma_{\mathbb{I}}(\mathfrak{u}\mathfrak{u}_t P)$ in $\mathrm{SL}_2(\mathbb{I}/\mathfrak{P})$. Then for the closed subgroup $G_U \subset \mathbb{G}$ topologically generated by conjugates gUg^{-1} for all $g \in \mathbb{G}$, $\overline{G}_U$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ by Corollary 2.3 and Lemma 2.4. By Lemma 1.5, we get the desired assertion.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

Since the two conditions (2) and (3) are similar, the proof is basically the same, though we need to localize the argument at P under (3). As is clear from the above proof under (1), we only need to prove $P \nmid \mathfrak{u}\mathfrak{u}_t$. We give a proof under $\mathbb{I} = \Lambda$ and (2). Since the reduction map $\mathcal{M}[1] \to \overline{\mathcal{M}}[1]$ modulo $\mathfrak{P}$ is onto, $\mathbb{G}$ has an element $g \in \mathcal{B}(\mathbb{I})$ with eigenvalues z, z' with $z \not\equiv z' \bmod \mathfrak{P}$. By Lemma 1.3(2), U/U' is killed by $(z'z^{-1} - 1, T)$, and we find $c \in \mathbb{I} \cap \mathbb{I}_{\mathfrak{P}}^{\times}$ in the annihilator of U/U'. Let

$$\mathcal{M}_0 := \mathcal{M} \cap (\mathfrak{U}(\mathbb{I}) \oplus {}^t\mathfrak{U}(\mathbb{I})) \quad \text{and} \quad \overline{\mathcal{M}}_0 := \overline{\mathcal{M}} \cap (\mathfrak{U}(\mathbb{I}/\mathfrak{P}) \oplus {}^t\mathfrak{U}(\mathbb{I}/\mathfrak{P})).$$

Then, under the reduction map modulo $\mathfrak{P}$, $\mathcal{M}_0$ surjects down to $\overline{\mathcal{M}}_0$ which has non-trivial intersection ${}^t\mathfrak{U}(\mathbb{I}/\mathfrak{P})$. Thus we have an element $(a, b) \in \mathcal{M}_0$ with $a \in \mathfrak{U}(\mathbb{I})$ and $b \in {}^t\mathfrak{U}(\mathbb{I})$ with $b \bmod \mathfrak{P} \neq 0$. Since $\mathbb{G} \supset \mathfrak{U}(\Lambda)$, we have $(ca, 0) \in \mathcal{M}_0$; so, $(0, cb) = (ca, cb) - (ca, 0) \in \mathcal{M}_0$. Thus we find that U_t and $\overline{U}_t$ cannot be trivial. Then by the same argument as above, we conclude the assertion. Under (3), we go exactly the same way, replacing $\mathbb{I}$ and Λ in the above argument by $\mathbb{I}_P$ and Λ_P.

Now we assume (1) and that $\mathbb{I} \supsetneq \Lambda$. We proceed in steps. First we prove

(a) conjugating $\mathbb{G}$ by an element in $\mathcal{B}(\mathbb{I}_P)$, we achieve that $\overline{\mathbb{G}}'_{\mathfrak{P}} \cap \mathrm{SL}_2(A_0)$ (for the topological commutator subgroup $\overline{\mathbb{G}}'_{\mathfrak{P}}$ of $\overline{\mathbb{G}}_{\mathfrak{P}}$) is open in $\mathrm{SL}_2(A_0)$ for all prime divisors $\mathfrak{P}|P$ in $\mathbb{I}$.

Since $\overline{\mathbb{G}}_{\mathfrak{P}}$ (up to conjugation) contains an open subgroup of $\mathrm{SL}_2(A_0)$ for each $\mathfrak{P}|P$, its derived group $\overline{\mathbb{G}}'_{\mathfrak{P}}$ contains an open subgroup of a conjugate of $\mathrm{SL}_2(A_0)$. Thus the $\kappa(\mathfrak{P})$-span of $\overline{\mathcal{M}}^0 = \mathcal{M}^0(\overline{\mathbb{G}}_{\mathfrak{P}})$ has dimension 3 (by the irreducibility of the adjoint action of an open subgroup of) $\mathrm{SL}_2(A_0)$. Thus a-eigenspace $\overline{\mathcal{M}}[a] = \mathfrak{U}(\kappa(\mathfrak{P})) \cap \overline{\mathcal{M}}$ under the action of $\mathrm{Ad}(j)$ is non-trivial. Taking $0 \neq u_{\mathfrak{P}} \in \mathbb{I}/\mathfrak{P}$ such that $\left(\begin{smallmatrix} 0 & u_{\mathfrak{P}} \\ 0 & 0 \end{smallmatrix}\right) \in \overline{\mathcal{M}}[a]$ and putting $\alpha_{\mathfrak{P}} = \left(\begin{smallmatrix} u_{\mathfrak{P}}^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we have $\mathfrak{U}(A_0) \subset \mathcal{M}(\alpha_{\mathfrak{P}}\overline{\mathbb{G}}_{\mathfrak{P}}\alpha_{\mathfrak{P}}^{-1})$. By the approximation theorem (e.g. [Bou98, VII.2.4]) applied to the Dedekind ring $\mathbb{I}_P$, we find $\alpha \in \mathcal{B}(\mathbb{I}_P)$ such that $\alpha \bmod \mathfrak{P} = \alpha_{\mathfrak{P}}$ for all $\mathfrak{P}|P$; so, replacing $\mathbb{G}$ by $\alpha\mathbb{G}\alpha^{-1}$, we start with $\mathbb{G}$ with $\overline{\mathbb{G}}_{\mathfrak{P}}$ containing $\mathcal{U}(A_0)$ for all $\mathfrak{P}|P$. Let $Q_0 := Q(A_0)$. Consider the Q_0-span $\bar{\mathfrak{s}}_{\mathfrak{P}}$ of $\mathcal{M}^0(\overline{\mathbb{G}}_{\mathfrak{P}})$. Then $\kappa(\mathfrak{P}) \cdot \bar{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$ as the adjoint action of $\mathrm{SL}_2(A_0)$ (more precisely of its conjugate) is absolutely irreducible. Then by Lemma 2.6 applied to $L = \kappa(\mathfrak{P})$ and $K = Q_0$, $\bar{\mathfrak{s}}_{\mathfrak{P}}$ contains $\mathfrak{sl}_2(Q_0)$, which implies the claim.

Next we show, for the topological commutator subgroup $\mathbb{G}'$ of $\mathbb{G}$ that

(b) conjugating $\mathbb{G}$ by an element in $\mathcal{B}(\mathbb{I}_P)$, we achieve $U = \mathcal{U}(\Lambda) \cap \mathbb{G} \neq 0$ and $U' = \mathcal{U}(\Lambda) \cap \mathbb{G}' \neq 0$.

To see this, we use the same symbol introduced at the beginning of this proof. In particular, $j = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta' \end{smallmatrix}\right) \in \mathcal{B}(\mathbb{I})$ and $\overline{\mathbb{G}}_P$ (respectively $\overline{\mathbb{G}}'_P$) is the image of $\mathbb{G}$ (respectively $\mathbb{G}'$) in $\mathrm{SL}_2(\mathbb{I}/P\mathbb{I})$. Since $\overline{\mathbb{G}}_{\mathfrak{P}}$ (and hence $\overline{\mathbb{G}}'_{\mathfrak{P}}$) for each $\mathfrak{P}|P$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, we find the image $\mathcal{M}(\overline{\mathbb{G}}_{\mathfrak{P}})[\lambda]$ of $\overline{\mathcal{M}}[\lambda]$ in $\mathfrak{gl}_2(\mathbb{I}/\mathfrak{P})$ is non-trivial for all eigenvalues λ of $\mathrm{Ad}(j)$ and all $\mathfrak{P}|P$, we conclude, as before:

(1) $\mathcal{M}[\lambda] \neq 0$ and $\mathcal{M}(\overline{\mathbb{G}}_{\mathfrak{P}})[\lambda] \neq 0$ for all $\mathfrak{P}|P$;
(2) the $\mathbb{I}$-ideal $\mathfrak{a}$ generated by $\mathfrak{n} = \left\{a \in \mathbb{I} \mid \left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right) \in \mathcal{M}[a]\right\}$ is prime to P ($\Rightarrow \mathbb{U} \neq 0$);
(3) the $\mathbb{I}$-ideal $\mathfrak{a}_t$ generated by $\mathfrak{n}_t = \left\{a \in \mathbb{I} \mid \left(\begin{smallmatrix} 0 & 0 \\ b & 0 \end{smallmatrix}\right) \in \mathcal{M}[a^{-1}]\right\}$ is prime to P ($\Rightarrow \mathbb{U}_t \neq 0$).

By (1), we can pick $u \in \mathfrak{n}$ prime to P such that $(u \bmod \mathfrak{P}) \in A_0$ for all $\mathfrak{P}|P$. Conjugating $\mathbb{G}$ by $\alpha = \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{B}(\mathbb{I}_P)$ with image $\overline{\alpha} \in \mathcal{B}(Q(A_0))$, we may assume that $\mathfrak{u} = \mathfrak{n} \cap \Lambda = \Lambda$ and $\overline{\alpha}\overline{\mathbb{G}}'_{\mathfrak{P}}\overline{\alpha}^{-1}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ for all $\mathfrak{P}|P$. Since α is diagonal, j still normalizes $\mathbb{G}$

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

and $\mathbb{G}'$. Just to have $\mathfrak{u} \neq 0$, we only need to choose any $0 \neq u \in Q(\mathbb{I})\mathfrak{n}$; so, we can assume that u is prime to any given finite set of primes. We now claim that

(c) $\overline{\mathbb{G}}'_P$ (and hence $\overline{\mathbb{G}}_P$) contains an open subgroup of $\mathrm{SL}_2(A_0)$ regarding $A_0 \subset \mathbb{I}/P\mathbb{I}$.

To see this, recall $\mathcal{M}^0(\mathcal{G}) = \mathcal{M}(\mathcal{G}) \cap \mathfrak{sl}_2(A)$ for a p-profinite subgroup $\mathcal{G}$ of $\mathrm{SL}_2(A)$. Write $\mathcal{M}^0 = \mathcal{M}^0(\mathbb{G})$ and $\overline{\mathcal{M}}^0 = \mathcal{M}^0(\overline{\mathbb{G}}_P)$. Replacing $\mathbb{I}$ by the integral closure of $\mathbb{I}$ in the Galois closure of $Q(\mathbb{I})$ over Q, we may assume that $Q(\mathbb{I})$ is a Galois extension of Q. Then $P = \prod_{\mathfrak{P}\in\Sigma} \mathfrak{P}^e$ for the finite set Σ of primes $\mathfrak{P}$ in $\mathbb{I}$ over P. Identify $\kappa(\mathfrak{P})$ with a finite extension k of $\kappa := \kappa(P)$ for all $\mathfrak{P}|P$. Since $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ for every $\mathfrak{P} \in \Sigma$, by Corollary 2.8, the image $\overline{\mathbb{G}}_{\sqrt{P}}$ of $\mathbb{G}$ in $\mathrm{SL}_2(\mathbb{I}_P/\sqrt{P}\mathbb{I}_P) = \prod_{\mathfrak{P}|P} \mathrm{SL}_2(k)$ contains an open subgroup H of $\mathrm{SL}_2(A_0)$ diagonally embedded in $\prod_{\mathfrak{P}|P} \mathrm{SL}_2(k)$, where $\sqrt{P} = \prod_{\mathfrak{P}\in\Sigma} \mathfrak{P}$ (the radical of P in $\mathbb{I}$). Then H acts on $\kappa \cdot \mathcal{M}^0$ by the adjoint action. Since $\mathfrak{U}(\Lambda) \subset \Lambda_P \cdot \mathcal{M}^0$, under the action of the group algebra $\kappa[H]$, $\mathfrak{U}(\kappa) \subset \overline{\mathcal{M}}^0$ generates an irreducible subspace equal to $\mathfrak{sl}_2(\kappa)$ (since $\mathfrak{U}(\kappa) \subset \mathfrak{sl}_2(\kappa)$ is the highest weight root space and the adjoint square is absolutely irreducible as $p > 2$). Therefore $\kappa \cdot \mathcal{M}^0(\overline{\mathbb{G}}_P)$ contains $\mathfrak{sl}_2(\kappa)$, which implies that $\overline{\mathbb{G}}'_P$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ by Lemma 2.4 and Corollary 2.3.

Next we look into the A-span $\mathfrak{s}_A := A \cdot \mathcal{M}^0$ of $\mathcal{M}^0$ for a subalgebra A of $Q(\mathbb{I})$, which is a Lie A-subalgebra of $\mathfrak{sl}_2(Q(\mathbb{I}))$. Let $\mathfrak{u} = \mathcal{M}^0[a] \cap \mathfrak{sl}_2(\Lambda)$ and $\mathfrak{u}_t = \mathcal{M}^0[a^{-1}] \cap \mathfrak{sl}_2(\Lambda)$. We claim

(d) $\mathfrak{s}_Q = Q \cdot \mathcal{M}^0$ contains $\mathfrak{sl}_2(Q)$, $\dim_Q Q \cdot \mathfrak{u} = \dim_Q Q \cdot \mathfrak{u}_t = 1$ and $P \nmid \mathfrak{u}$.

To see this, pick a prime factor $\mathfrak{P}|P$ of P in $\mathbb{I}$. Taking $A = \mathbb{I}_{\mathfrak{P}}$, the image $\bar{\mathfrak{s}}_A$ of $\mathfrak{s}_A$ in $\mathfrak{sl}_2(\kappa(\mathfrak{P}))$ contains a non-trivial upper nilpotent algebra $\bar{\mathfrak{u}}_{\mathfrak{P}}$ which is the image of the Lie algebra of U. Since the image $\overline{\mathbb{G}}_{\mathfrak{P}}$ of $\mathbb{G}$ in $\mathrm{SL}_2(\kappa(\mathfrak{P}))$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, $\bar{\mathfrak{s}}_A = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$, which implies $\mathfrak{s}_A/\mathfrak{P}\mathfrak{s}_A = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$. From Nakayama's lemma, we deduce $\mathfrak{s}_{\mathbb{I}_{\mathfrak{P}}} = \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}})$. Thus $\mathfrak{s}_Q$ spans over $Q(\mathbb{I})$ the entire $\mathfrak{sl}_2(Q(\mathbb{I}))$. Again applying Lemma 2.6 for $\mathfrak{s}_Q$, $K = Q$ and $L = Q(\mathbb{I})$, we get $\mathfrak{s}_Q \supset \mathfrak{sl}_2(Q)$. This proves that $\dim_Q Q \cdot \mathfrak{u} = \dim_Q Q \cdot \mathfrak{u}_t = 1$. In particular, $U = 1 + \mathfrak{u} \subset G$ and $U_t = 1 + \mathfrak{u}_t \subset G$ are non-trivial unipotent subgroups. Regarding $\mathfrak{u}$ and $\mathfrak{u}_t$ as ideals of Λ, we find $G \supset \Gamma_\Lambda(\mathfrak{u}\mathfrak{u}_t)$. By (c), the image $\bar{\mathfrak{u}}$ in $\mathfrak{sl}_2(\Lambda/P)$ is non-trivial; so, $P \nmid \mathfrak{u}$.

Therefore, to finish the proof under (1) and $\mathbb{I} \neq \Lambda$, we need to prove that

(e) $P \nmid \mathfrak{u}_t$.

Let $\overline{H} = \overline{\mathbb{G}}'_P \cap \mathrm{SL}_2(A_0)$, which is an open subgroup of $\mathrm{SL}_2(A_0)$. Put $H = \pi^{-1}(\overline{H})$ for the projection $\pi : \mathbb{G}' \twoheadrightarrow \overline{\mathbb{G}}'_P$. Note that H is still normalized by j. For the order $\mathbb{I}' = \Lambda + P\mathbb{I} \subset \mathbb{I}$, $H \subset \mathrm{GL}_2(\mathbb{I}')$. Note that $P\mathbb{I}'$ is still a prime in $\mathbb{I}'$ with residue field $\kappa(P)$. In the above argument, we replace $\mathbb{G}$ by H, $\mathbb{I}$ by $\mathbb{I}'$ and $\mathfrak{s}_Q$ by $\mathfrak{s} = \Lambda_P \cdot \mathcal{M}^0$. Then $\mathfrak{s}$ is a Lie Λ_P-subalgebra of Q-simple Lie algebra $\mathfrak{s}_Q$. We consider the adjoint action of $\overline{\mathbb{G}}_P$, which is now an open subgroup of $\mathrm{SL}_2(A_0)$. By our replacement of $\mathbb{I}$ by $\mathbb{I}'$, P is a prime in $\mathbb{I}'$ with $\kappa = \kappa(P) = \kappa(P\mathbb{I})$. Consider the image $\bar{\mathfrak{s}}_P$ of $\mathfrak{s}$ in $\mathfrak{sl}_2(\mathbb{I}/P\mathbb{I})$. Since $\bar{\mathfrak{s}}_P$ is generated by $\kappa \cdot \bar{\mathfrak{u}}$ under the action of the group algebra $\kappa[\overline{\mathbb{G}}_P]$, noting $\overline{\mathbb{G}}_P$ is now an open subgroup of $\mathrm{SL}_2(A_0)$, we have $\bar{\mathfrak{s}}_P = \mathfrak{sl}_2(\kappa)$. Thus $\overline{\mathbb{G}}_P$ acts on $\bar{\mathfrak{s}}_P = \mathfrak{sl}_2(\kappa)$ by the adjoint representation $\mathrm{Ad}(\kappa)$. Therefore its a^{-1}-eigenspace $\bar{\mathfrak{s}}_P[a^{-1}]$ of $\mathrm{Ad}(j)$ is non-trivial in $\kappa[\mathbb{G}] \cdot \bar{\mathfrak{u}} = \mathfrak{sl}_2(\kappa)$. This shows $\Lambda_P[\mathbb{G}] \cdot \bar{\mathfrak{u}} = \mathfrak{sl}_2(\kappa)$. By Nakayama's lemma, we conclude $\mathbb{I}_P[\mathbb{G}] \cdot \mathfrak{u} = \mathfrak{sl}_2(\mathbb{I}_P)$. Since $\Lambda_P[\mathbb{G}] \cdot \mathfrak{u}$ spans $\mathfrak{sl}_2(\mathbb{I}_P)$ stable under the action of $\mathbb{G}$, it contains $\mathfrak{sl}_2(\Lambda_P)$. Thus $\mathfrak{s} \supset \Lambda_P[\mathbb{G}] \cdot \mathfrak{u} \supset \mathfrak{sl}_2(\Lambda_P)$, and

$$ {}^t\mathfrak{U}(\Lambda_P) \supset \Lambda_P \cdot \mathfrak{u}_t = \mathfrak{s} \cap {}^t\mathfrak{U}(\Lambda_P) \supset \mathfrak{sl}_2(\Lambda_P) \cap {}^t\mathfrak{U}(\Lambda_P) = {}^t\mathfrak{U}(\Lambda_P). $$

Thus $\Lambda_P \cdot \mathfrak{u}_t = {}^t\mathfrak{U}(\Lambda_P)$, and we conclude $\bar{\mathfrak{u}}_t \neq 0$; so, $P \nmid \mathfrak{u}_t$.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

We now assume (2) or (3) in the lemma and $\mathbb{I} \neq \Lambda$. As we have seen, $\mathfrak{u} = \left\{b \in \Lambda \mid \left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) \in \mathbb{G}\right\}$ has non-trivial image $\overline{\mathfrak{u}}$ in $\mathfrak{sl}_2(\mathbb{I}/\mathfrak{P})$ for all primes $\mathfrak{P}|P$. We have shown above, from the non-triviality of $\overline{\mathfrak{u}}$, $\mathfrak{s}_{\mathbb{I}_P} = \mathfrak{sl}_2(\mathbb{I}_P)$. After reaching this point, by the same argument as above, we conclude $\overline{\mathfrak{u}}_t \neq 0$; so, we get the desired assertion. □

Remark 2.10. We insert here another shorter proof of the above lemma under (1) assuming an extra assumption $P \nmid (p)$. We first replace $\mathbb{I}$ by the integral closure of $\mathbb{I}$ in the Galois closure of $Q(\mathbb{I})$ over Q. Write $\mathfrak{g} = \mathrm{Gal}(Q(\mathbb{I})/Q)$ for the finite Galois group. Let H be as in step (c) in the above proof. We then replace $\mathbb{G}$ by $\mathbb{G} = \{h \in \mathbb{G}|\pi(h) \in \overline{H}\}$ for the reduction map $\pi : \mathrm{GL}_2(\mathbb{I}_P) \to \mathrm{GL}_2(\mathbb{I}_P/P\mathbb{I}_P)$. We now replace $\mathbb{I}$ by $\Lambda + P\mathbb{I}$. By this, we lose normality of $\mathbb{I}$ but $\mathbb{I}_P$ becomes local with only one maximal ideal $P\mathbb{I}_P$ satisfying $\kappa(P) = \kappa(P\mathbb{I})$ and $\mathcal{M}(\overline{\mathbb{G}}_P) \subset \mathfrak{gl}_2(\mathbb{Z}_p)$ invariant under $\mathfrak{g}$. Recall

$$\mathcal{M}_0 = \mathcal{M} \cap (\mathfrak{U}(\mathbb{I}) \oplus {}^t\mathfrak{U}(\mathbb{I})).$$

As before, we find $\mathbb{I}_P \cdot \mathcal{M}^0 = \mathfrak{sl}_2(\mathbb{I}_P)$, and $\mathbb{I}_P \cdot \mathcal{M}_0 = \mathfrak{U}(\mathbb{I}_P) \oplus {}^t\mathfrak{U}(\mathbb{I}_P)$. Thus $\mathfrak{g}$ acts on $\mathbb{I}_P \cdot \mathcal{M}^0$ and $\mathbb{I}_P \cdot \mathcal{M}_0$. The $\mathfrak{g}$-cohomology sequence attached to the exact sequence

$$0 \to P\mathbb{I}_P \cdot \mathcal{M}_0 \to \mathbb{I}_P \cdot \mathcal{M}_0 \to \kappa(P) \cdot \overline{\mathcal{M}}_0 \to 0$$

gives a short exact sequence for $M = \mathcal{M}_0$

$$0 \to H^0(\mathfrak{g}, P\mathbb{I}_P \cdot M) \to H^0(\mathfrak{g}, \mathbb{I}_P \cdot M) \to \kappa(P) \cdot \overline{M} \to 0 \qquad (*)$$

since $H^1(\mathfrak{g}, P\mathbb{I}_P \cdot \mathcal{M}_0) = 0$ (as $P\mathbb{I}_P \cdot \mathcal{M}_0$ is a $\mathbb{Q}_p$-vector space). Similarly, $\mathfrak{g}$ acts on $\mathbb{I}_P \cdot \mathcal{M}^0$ and we have a short exact sequence (∗) for $M = \mathcal{M}^0$. Since $\mathcal{M}_0$ is a Λ-module, the quotient $X := H^0(\mathfrak{g}, \mathbb{I}_P \cdot \mathcal{M}_0)/\mathcal{M}_0$ is a Λ-module of finite type. The quotient $Y := H^0(\mathfrak{g}, \mathbb{I}_P \cdot \mathcal{M}^0)/\mathcal{M}^0$ contains X as a direct summand (i.e. $Y = X \oplus Z$ with $\mathrm{Ad}(j)$ acting trivially on Z), and on Y the open subgroup $\overline{G}_P$ of $\mathrm{SL}_2(\mathbb{Z}_p)$ acts by the adjoint action. Consider the Λ_P-span $\Lambda_P \cdot Y = (\Lambda_P \cdot X) \oplus (\Lambda_P \cdot Z)$. Since $H^0(\mathfrak{g}, \Lambda_P \cdot \mathcal{M}[a]) = \mathfrak{U}(\Lambda_P) = H^0(\mathfrak{g}, \mathfrak{U}(\mathbb{I}_P))$, the $\overline{G}_P$-module $\overline{Y} := Y \otimes_{\Lambda_P} \kappa(P)$ does not have any highest weight vector with respect to $\mathcal{B}(\kappa(P)) \cap \overline{\mathbb{G}}_P$; so, $\overline{Y} = 0$. By Nakayama's lemma, we have $Y = 0$; so, we get $\Lambda_P \cdot X = 0$. Thus $H^0(\mathfrak{g}, \mathbb{I}_P \cdot \mathcal{M}[a^{-1}])$ surjects down to ${}^t\mathfrak{U}(\kappa(P))$ under the reduction map modulo P; i.e. $\mathfrak{u}_t = \mathcal{M}[a^{-1}]$ has non-trivial image in ${}^t\mathfrak{U}(\kappa(P))$. In particular, $P \nmid \mathfrak{u}\mathfrak{u}_t$.

Remark 2.11. In step (b) in the above proof, conjugation by $\alpha = \left(\begin{smallmatrix}u^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)$ brings $\mathbb{G}$ into a subgroup $\alpha\mathbb{G}\alpha^{-1}$ containing $\Gamma_\Lambda(\mathfrak{c})$ for its conductor $\mathfrak{c} \neq 0$. To prove this fact, we only needed to make $\mathfrak{u} \neq 0$. As remarked in the proof, allowing u to be another non-zero element u' in $Q(\mathbb{I}) \cdot \mathfrak{n}$, we achieve $\mathfrak{u} \neq 0$; so, we get another conductor $\mathfrak{c}'$ using this u' and $\alpha' = \left(\begin{smallmatrix}u'^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)$; i.e. $\alpha'\mathbb{G}\alpha'^{-1} \supset \Gamma_\Lambda(\mathfrak{c}')$ maximally. For any other prime divisor $P' \neq P$, as long as $\rho_{\mathfrak{P}'}$ is irreducible for all $\mathfrak{P}'|P'$ (and $\alpha'\mathbb{G}\alpha'^{-1} \subset \mathrm{GL}_2(\mathbb{I}_{P'})$), we will prove $\mathfrak{c}_{P'} = \mathfrak{c}'_{P'}$ in Lemma 3.3.

Theorem 2.12. *Suppose $p > 2$ and that $\mathbb{I}$ is integrally closed. Let $\mathbb{G}$ be a p-profinite subgroup of $\mathrm{SL}_2(\mathbb{I})$ satisfying condition (B) of Lemma 1.3 and one of the three conditions (1–3) of Lemma 2.9. Take a prime divisor P of Λ. Suppose that the projected image $\overline{\mathbb{G}}_{\mathfrak{P}} \hookrightarrow \mathrm{SL}_2(\mathbb{I}/\mathfrak{P})$ of $\mathbb{G}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ for all prime factors $\mathfrak{P}|P$ in $\mathbb{I}$. Then there exists $\alpha \in \mathcal{B}(\mathbb{I}_P)$ such that, writing $\mathbb{G}_\alpha = \alpha\mathbb{G}\alpha^{-1}$ and $G_\alpha = \mathbb{G}_\alpha \cap \mathrm{SL}_2(\Lambda)$:*

(1) *the image $\mathcal{M}^0(G_\alpha)$ in $\mathfrak{sl}_2(\Lambda)$ spans over Q the entire Lie algebra $\mathfrak{sl}_2(Q)$;*
(2) *there exists a unique non-zero ideal $\mathfrak{c}_\alpha$ of Λ prime to P (dependent on α) maximal among ideals $\mathfrak{a} \subset \Lambda$ such that $\mathbb{G}_\alpha \supset \Gamma_\Lambda(\mathfrak{a})$ ($\Leftrightarrow G_\alpha \supset \Gamma_\Lambda(\mathfrak{a})$);*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

(3) *the ideal* $\bigcap_{(\lambda)\supset\mathfrak{c}_\alpha}(\lambda)$ *(the intersection of all principal ideals containing* $\mathfrak{c}_\alpha$*) is a principal ideal* (L_α)*, and* $\Gamma_\Lambda(L_\alpha)/\Gamma_\Lambda(\mathfrak{c}_\alpha)$ *is finite.*

The above ideal $\mathfrak{c}_\alpha$ will be called the *conductor* of G_α or $\mathbb{G}_\alpha$. The assertion (1) follows from Lemma 2.9. The other two assertions are covered by [Hid11a, Theorem 4.3.21].

Remark 2.13. When $\mathbb{G}$ is the largest p-profinite subgroup of $\mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\mathbb{I})$, there should be a canonical Λ-subalgebra $\mathbb{I}_0 \subset \mathbb{I}$ finite over Λ such that $\mathbb{G}_\alpha$ for a suitable $\alpha \in \mathcal{B}(\mathbb{I}_P)$ contains $\Gamma_{\mathbb{I}_0}(\mathfrak{c}_\alpha)$ for an ideal $\mathfrak{c}_\alpha \neq 0$ of $\mathbb{I}_0$. The author hopes to be able to come back to this problem later.

3. Global level of $\rho_{\mathbb{I}}$

Take an irreducible non-CM component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbf{h})$ with its normalization $\mathrm{Spec}(\widetilde{\mathbb{I}})$. Assume the conditions (R) and (F) in the introduction for $\rho_{\mathbb{I}}$. Under (F), we consider $\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widetilde{\mathbb{I}}) \subset \mathrm{GL}_2(A)$ having values in $\mathrm{GL}_2(A)$ for an $\widetilde{\mathbb{I}}$-subalgebra A of $\overline{Q}$, and to indicate its coefficients explicitly, we write ρ_A for it. We state a condition which is a version of (Gal).

(Gal_A) *Up to isomorphism over* A*,* ρ_A *is upper triangular over* D_p*,* $\rho_A([\gamma^s, \mathbb{Q}_p]) \cong \begin{pmatrix} t^s & * \\ 0 & 1 \end{pmatrix}$ $(t = 1 + T)$ *and* $\rho_A([p, \mathbb{Q}_p]) \cong \begin{pmatrix} * & * \\ 0 & a(p) \end{pmatrix}$ *for the image* $a(p)$ *of* $U(p)$ *in* $\mathbb{I}$*, simultaneously.*

The conditions (R), (F) and (Gal) (that is, $(\mathrm{Gal}_{Q(\mathbb{I})})$) combined imply $(\mathrm{Gal}_{\widetilde{\mathbb{I}}})$. Indeed, by (F), choosing $\sigma \in D_p$ with $\overline{\rho}(\sigma)$ having distinct eigenvalues modulo $\mathfrak{m}_{\widetilde{\mathbb{I}}}$, we can split $\widetilde{\mathbb{I}}^2$ into the direct sum of each eigenspace of $\rho(\sigma)$. Each eigenspace is $\widetilde{\mathbb{I}}$-free (by $\widetilde{\mathbb{I}}$-flatness $\Rightarrow$ $\widetilde{\mathbb{I}}$-freeness), and hence $(\mathrm{Gal}_{\widetilde{\mathbb{I}}})$ is satisfied. The condition $(\mathrm{Gal}_{\widetilde{\mathbb{I}}})$ is what we need, though often we take $\rho_{\mathbb{I}}$ realized on $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ as a standard choice. If $\overline{\rho}$ is absolutely irreducible, the isomorphism class of $\rho_{\widetilde{\mathbb{I}}}$ is unique over $\widetilde{\mathbb{I}}$ (even over $\mathbb{I}$), and we do not need to take the specific one realized over $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$. Even if $\overline{\rho}$ is not absolutely irreducible, there is no compelling reason for us to take $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$. We make this choice often to fix our idea, though we will state the result without assuming that $\rho_{\mathbb{I}}$ is realized on $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$.

Here is a heuristic reason for our making this choice (when $\overline{\rho}$ is reducible). Pick an Eisenstein prime divisor $\mathfrak{P} \in \mathrm{Spec}(\widetilde{\mathbb{I}})$ (i.e. $\rho_{\mathfrak{P}}$ is reducible). If e is the maximal exponent such that $\rho_{\widetilde{\mathbb{I}}} \bmod \mathfrak{P}^e$ is a direct sum of two characters, by a trick of Ribet [Rib76] of changing lattice applied to $\rho_{\widetilde{\mathbb{I}}_{\mathfrak{P}}}$ (i.e. changing the isomorphism class of $\rho_{\widetilde{\mathbb{I}}_{\mathfrak{P}}}$ over $\widetilde{\mathbb{I}}_{\mathfrak{P}}$ in the 'isogeny' class), we may increase the level of $\rho_{\widetilde{\mathbb{I}}}$ from $\mathfrak{P}^e$ to $\mathfrak{P}^{2e}$ at P, still keeping the condition $(\mathrm{Gal}_{\widetilde{\mathbb{I}}})$. This new $\rho_{\widetilde{\mathbb{I}}}$ modulo $\mathfrak{P}$ (not the semi-simplified $\rho_{\mathfrak{P}}$) is non-semi-simple (and hence $\mathfrak{P}^{2e}$ is the deepest possible level at $\mathfrak{P}$). If this is the case, via Wiles' argument through μ-deprived quotients, $\mathfrak{P}^{2e}$ would be a factor of the characteristic power series of the corresponding Iwasawa module, and hence the level $\mathfrak{P}^{2e}$ would be a factor of the corresponding Kubota–Leopoldt p-adic L function by the solution of the main conjecture by Mazur–Wiles. Anyway, the original level $\mathfrak{P}^e$ divides the Kubota–Leopoldt p-adic L function, and the assertion of divisibility holds for the starting lattice. Thus our choice of $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ is not essential. Ohta's point in his proof of the main conjecture in [Oht00, § 3.3] under some assumptions (which developed a seed idea of Harder–Pink) is that the proof can be done without using Ribet's trick; i.e. $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ does create a fully non-splitting extension modulo $\mathfrak{P}$. If this holds for all our cases of cube-free N, the choice of $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})$ produces highest possible divisibility for the component $\mathbb{I}$ and justifies our choice.

In the isomorphism class $[\rho_{\mathbb{I}}]$ over $\mathbb{I}$, we have $\rho_{\mathbb{I}}$ satisfying $(\mathrm{Gal}_{\mathbb{I}})$ if $\overline{\rho}$ is absolutely irreducible. In the reducible case, $\rho_{\widetilde{\mathbb{I}}_{\mathfrak{P}}}$ realized on $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}})_{\mathfrak{P}}$ satisfies $(\mathrm{Gal}_{\widetilde{\mathbb{I}}_{\mathfrak{P}}})$ for any prime divisor $\mathfrak{P}$ of $\widetilde{\mathbb{I}}$.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

We put $\mathbb{G} = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_{\widetilde{\mathbb{I}}}(\mathfrak{m}_{\widetilde{\mathbb{I}}})$, which satisfies the condition (B) of Lemma 1.3 by (Gal_A) for A as above.

Now we state one more fundamental property of $\rho_{\mathbb{I}}$,

$$\det(\rho_{\mathbb{I}})(\sigma) = t^{\log_p(\mathcal{N}(\sigma))/\log_p(\gamma)}\chi_1(\sigma) \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \tag{Det}$$

where χ is the Neben character as in the introduction and $\mathcal{N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character (see the second edition of [Hid11a, Theorem 4.3.1] for this fact).

Lemma 3.1. *Assume ($Gal_{\widetilde{\mathbb{I}}}$). Then for each prime divisor $\mathfrak{P}$ of $\widetilde{\mathbb{I}}$, the image of $\mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\widetilde{\mathbb{I}})$ in $\mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$ is an open subgroup of $\mathrm{Im}(\rho_{\mathfrak{P}}) \cap \mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$. In particular, the reduction map: $\mathbb{G} = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_{\widetilde{\mathbb{I}}}(\mathfrak{m}_{\widetilde{\mathbb{I}}}) \to \mathrm{Im}(\rho_{\mathfrak{P}}) \cap \Gamma_{\widetilde{\mathbb{I}}/\mathfrak{P}}(\mathfrak{m}_{\widetilde{\mathbb{I}}/\mathfrak{P}})$ given by $x \mapsto (x \bmod \mathfrak{P})$ has finite cokernel.*

Proof. Let $\mathbb{H} := \{g \in \mathrm{Im}(\rho_{\mathbb{I}}) \mid \det(g) \in \Gamma \text{ and } (g \bmod \mathfrak{m}_{\widetilde{\mathbb{I}}}) \in \mathcal{U}(\mathbb{F})\}$ for $\mathbb{F} = \widetilde{\mathbb{I}}/\mathfrak{m}_{\widetilde{\mathbb{I}}}$ and $\mathbb{S} = \mathbb{H} \cap \mathrm{SL}_2(\widetilde{\mathbb{I}})$ for $\Gamma = \{t^s\} \subset \Lambda^\times$. By ($\mathrm{Gal}_{\widetilde{\mathbb{I}}}$), we find $\tau \in \rho_{\mathbb{I}}(D_p) \cap \mathbb{H}$ such that $\tau = \left(\begin{smallmatrix} t & * \\ 0 & 1 \end{smallmatrix}\right)$. By (Det), the group $\mathbb{H}$ is an open subgroup of $\mathrm{Im}(\rho_{\mathbb{I}})$. Thus we prove the image $\overline{\mathbb{S}}_{\mathfrak{P}}$ of $\mathbb{S}$ in $\mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$ is open in $\mathrm{Im}(\rho_{\mathfrak{P}}) \cap \mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$. Let $\overline{\mathbb{H}}_{\mathfrak{P}}$ be the image of $\mathbb{H}$ in $\mathrm{GL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$. Since $\mathbb{H}$ is open in $\mathrm{Im}(\rho_{\mathbb{I}})$, $\overline{\mathbb{H}}_{\mathfrak{P}}$ is open in $\mathrm{Im}(\rho_{\mathfrak{P}})$. Put $\overline{\mathbb{S}}'_{\mathfrak{P}} = \overline{\mathbb{H}}_{\mathfrak{P}} \cap \mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$. Since $\overline{\mathbb{H}}_{\mathfrak{P}}$ is open in $\mathrm{Im}(\rho_{\mathfrak{P}})$, $\overline{\mathbb{S}}'_{\mathfrak{P}}$ is open in $\mathrm{Im}(\rho_{\mathfrak{P}}) \cap \mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$. On the other hand, set $\mathcal{T}' = \{\tau^s \mid s \in \mathbb{Z}_p\}$. We have $\mathbb{H} = \mathcal{T}' \ltimes \mathbb{S}$ since $\mathcal{T}'$ projects down (under the determinant map) isomorphically to Γ. In the same way, for the image $\overline{\mathcal{T}}'_{\mathfrak{P}}$ of $\mathcal{T}'$ in $\mathrm{GL}_2(\mathbb{I}/\mathfrak{P})$, we have $\overline{\mathbb{H}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}} \ltimes \overline{\mathbb{S}}'_{\mathfrak{P}}$. For $\overline{g}$ in $\overline{\mathbb{H}}_{\mathfrak{P}}$, lifting g to $\mathbb{H}$, $\det g \in \Gamma_{\mathfrak{P}}$, so taking $s \in \mathbb{Z}_p$ with '$\tau^s = \det(g)$', we have $g = \tau^s g_1$ with $g_1 = \tau^{-s} g \in \mathbb{G}$. Then $\overline{g} = \overline{\tau}^s \overline{g}_1$ for $\overline{g}_1 = (g_1 \bmod \mathfrak{P})$ and $\overline{\tau}^s = (\tau^s \bmod \mathfrak{P})$. Thus we have $\overline{\mathbb{S}}_{\mathfrak{P}} = \overline{\mathbb{S}}'_{\mathfrak{P}}$. Then the assertion is clear from this identity. □

Lemma 3.2. *Take a non-CM component $\mathbb{I}$. Let $P \in \mathrm{Spec}(\Lambda)$ be an arithmetic point. Suppose ($Gal_{\mathbb{I}_P}$) for $\rho_{\mathbb{I}}$. If one of the three conditions (1–3) of Lemma 2.9 is satisfied for $\mathbb{G}$ and P, there exists a representation $\rho \cong \rho_{\mathbb{I}}$ (over $\mathbb{I}_P$) such that the projected image $\mathrm{Im}(\rho_{P\mathbb{I}})$ in $\mathrm{GL}_2(\mathbb{I}_P/P\mathbb{I}_P)$ contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ and $\mathrm{Im}(\rho)$ still satisfies the condition (B) of Lemma 1.3.*

For each arithmetic point $P \in \mathrm{Spec}(\Lambda)$, $\mathbb{I}_P$ is étale over Λ_P; so, $\widetilde{\mathbb{I}}_P = \mathbb{I}_P$.

Proof. We pick a prime divisor $\mathfrak{P}$ of $\widetilde{\mathbb{I}}$ over P, and consider the Hecke eigenform $f_{\mathfrak{P}}$ associated to $\mathfrak{P}$; so, $f_{\mathfrak{P}}|T(l) = a_{\mathfrak{P}}(l) f_{\mathfrak{P}}$ for primes l, where $a_{\mathfrak{P}}(l) = (T(l) \bmod \mathfrak{P}) \in \overline{\mathbb{Q}}_p$. Let $f^\circ_{\mathfrak{P}}$ be the new form in the automorphic representation generated by $f_{\mathfrak{P}}$. By Proposition 5.1, $f^\circ_{\mathfrak{P}}$ does not have complex multiplication. Then by a result of Ribet [Rib85], the Galois representation $\rho_{\mathfrak{P}}$ associated to the non-CM new form $f^\circ_{\mathfrak{P}}$ has image containing an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, up to conjugation by an element in $\mathcal{B}(\kappa(\mathfrak{P}))$ (because of the Iwasawa decomposition of $\mathrm{GL}(2)$). Conjugating $\rho_{\mathfrak{P}}$ by an upper triangular matrix, we may assume that $\mathrm{Im}(\rho_{\mathfrak{P}})$ contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ (and the condition (B) in Lemma 1.3 is intact). To show the lemma, we may replace $\mathbb{G}$ by an open subgroup of $\mathbb{G}$ as long as the replacement still satisfies one of the three conditions (1–3) of Lemma 2.9. We may thus replace $\mathbb{G}$ by $\mathbb{S}$ in the proof of Lemma 3.1. Hence the reduction map $\mathbb{S} \to \overline{\mathbb{S}}_{\mathfrak{P}}$ is surjective, and $\overline{\mathbb{S}}_{\mathfrak{P}}$ is open in $\mathrm{Im}(\rho_{\mathfrak{P}})$. Thus $\overline{\mathbb{S}}_{\mathfrak{P}} \cap \mathrm{SL}_2(\mathbb{Z}_p)$ is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. This fullness of $\rho_{\mathfrak{P}}$ holds for all prime divisors $\mathfrak{P}|P$ in $\widetilde{\mathbb{I}}$. Then the result follows from Lemma 2.9 applied to this $\mathbb{S}$. □

By Theorem 2.12 combined with the above lemma, we can choose a representative $\rho_{\mathbb{I}}$ in its isomorphism class over $Q(\mathbb{I})$ so that we have a non-trivial conductor $\mathfrak{c}$ with $G \supset \Gamma_\Lambda(\mathfrak{c})$ and an effective divisor $(L) \subset \mathrm{Spec}(\Lambda)$ such that $(\Gamma_\Lambda(L) : \Gamma_\Lambda(\mathfrak{c}))$ is finite. This proves Theorem I in the introduction except for the uniqueness of (L) depending only on the isomorphism class of $\rho_{\mathbb{I}}$ in $\mathrm{GL}_2(\widetilde{\mathbb{I}})$ for the normalization $\widetilde{\mathbb{I}}$ of $\mathbb{I}$. In the rest of this section, we discuss the uniqueness of $\mathfrak{c}_P$ (under an appropriate modification of $\rho_{\mathbb{I}}$ if $\overline{\rho}$ is reducible). Then we define $L := L(\mathbb{I})$ as a generator of $\bigcap_P \mathfrak{c}_P$ for P running over all prime divisors of Λ.

Lemma 3.3. *Let the notation be as above and P be a prime divisor of Λ. Take a non-CM component $\mathbb{I}$ of $\mathbf{h}$ with normalization $\widetilde{\mathbb{I}}$, and suppose we have an associated Galois representation $\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widetilde{\mathbb{I}})$ whose image contains $\Gamma_\Lambda(\mathfrak{a})$ for a non-zero Λ-ideal $\mathfrak{a}$. Let $\mathfrak{c}$ be the conductor of the intersection $\mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\Lambda)$. Assume that $\rho_{\mathbb{I}}$ leaves an $\widetilde{\mathbb{I}}_P$-lattice $\mathcal{L}_P \subset Q(\mathbb{I})^2$ stable. Then the localization $\mathfrak{c}_P$ depends only on $\mathcal{L}_P$ up to scalars. If $\rho_{\mathfrak{P}}$ is absolutely irreducible for all prime divisors $\mathfrak{P} \in \mathrm{Spec}(\widetilde{\mathbb{I}})$ over P, then $\mathfrak{c}_P$ is independent of the choice of $\mathcal{L}_P$.*

The point of this lemma is that whatever the choice of $u \in \mathrm{GL}_2(Q(\mathbb{I}))$ with $u\mathcal{L}_P = \mathcal{L}_P$, as long as $\mathrm{Im}(u \cdot \rho_{\mathbb{I}} u^{-1})$ has non-trivial conductor, its localization at P is equal to $\mathfrak{c}_P$ for the conductor $\mathfrak{c}$ of the original choice $\rho_{\mathbb{I}}$. This lemma proves the uniqueness of (L) in Theorem I under absolute irreducibility of $\overline{\rho}$ (and finishes the proof of Theorem I). In this lemma, the only assumptions are (F) and the existence of $\mathfrak{a}$ (no condition like (Gal_A) is assumed).

Since the lemma concerns only the intersection of $\mathrm{Im}(\rho_{\mathbb{I}})$ with $\mathrm{SL}_2(\Lambda)$, without losing generality, we may regard $\rho_{\mathbb{I}}$ having values in a larger Λ-subalgebra in $\overline{Q}$ than $\widetilde{\mathbb{I}}$. Replacing $\widetilde{\mathbb{I}}$ by the integral closure of Λ in the Galois closure in $\overline{Q}$ of $Q(\mathbb{I})$ over Q, we assume that $\widetilde{\mathbb{I}}$ is a Galois covering of Λ.

Proof. Write $\mathfrak{c}_P = P^m$ in the discrete valuation ring Λ_P. We study dependence on $\mathcal{L}_P$. Write $G = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\Lambda)$, where $\rho_{\mathbb{I}}$ is chosen in the isomorphism class of $\rho_{\widetilde{\mathbb{I}}_P}$ over $\widetilde{\mathbb{I}}_P$ so that G has non-trivial conductor $\mathfrak{c}$. This is just a choice of a starting lattice $\mathcal{L}$, and we want to first prove the ideal $\mathfrak{c}_P = \mathfrak{c}_P(\mathcal{L}) := \mathfrak{c}\Lambda_P$ (for localization Λ_P of Λ at P) is equal to $\mathfrak{c}_P(\mathcal{L}')$ for any other choice $\mathcal{L}' = z\mathcal{L}$ for a scalar matrix $z \in \mathrm{GL}_2(Q(\widetilde{\mathbb{I}}))$. Identifying $\mathcal{L}_P = \widetilde{\mathbb{I}}_P^2$ and writing $\mathcal{L}_P^0 = \Lambda_P^2 \subset \mathcal{L}_P$, we find $\mathcal{L}_P = \mathcal{L}_P^0 \otimes_{\Lambda_P} \widetilde{\mathbb{I}}_P$, and $\mathcal{L}_P^0$ is stable under G.

We have another $\rho'_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widetilde{\mathbb{I}}_P)$ realized on $\mathcal{L}'_P$ with non-trivial conductor $\mathfrak{c}(\mathcal{L}')$; so, writing $\mathcal{Z}$ for the center of the algebraic group $\mathrm{GL}(2)$, we find $h \in \mathcal{Z}(Q(\widetilde{\mathbb{I}}))\mathrm{GL}_2(\widetilde{\mathbb{I}}_P)$ such that $h(\mathcal{L}'_P) = \mathcal{L}_P$ and $h\rho'_{\mathbb{I}}h^{-1} = \rho_{\mathbb{I}}$. We put $H = \mathrm{Im}(\rho'_{\mathbb{I}}) \cap \mathrm{SL}_2(\Lambda)$. Then we have the conductor ideal $\mathfrak{c}' \neq 0$ of H. Thus $G \cap H \supset \Gamma(\mathfrak{c} \cap \mathfrak{c}')$ and $\mathfrak{c} \cap \mathfrak{c}' \neq 0$. This shows $\rho_{\mathbb{I}}$ and $\rho'_{\mathbb{I}}$ are both absolutely irreducible over $G \cap H$. For $\sigma \in \mathrm{Gal}(Q(\widetilde{\mathbb{I}})/Q)$ and $g \in G \cap H$, we have

$$h^\sigma \rho'_{\mathbb{I}}(g) h^{-\sigma} = (h\rho'_{\mathbb{I}}(g)h^{-1})^\sigma = \rho_{\mathbb{I}}(g)^\sigma = \rho_{\mathbb{I}}(g) = h\rho'_{\mathbb{I}}(g)h^{-1}.$$

Thus $h^{-1}h^\sigma$ commutes with $\rho_{\mathbb{I}}|_{G\cap H}$. By absolute irreducibility of $\rho_{\mathbb{I}}|_{G\cap H}$, $h^{-1}h^\sigma$ is a scalar $z_\sigma \in Q(\widetilde{\mathbb{I}})^\times$. Thus $\sigma \mapsto z_\sigma$ is a 1-cocycle of H with values in $Q(\widetilde{\mathbb{I}})^\times$. By Hilbert's theorem 90, $z_\sigma = \zeta^{-1}\zeta^\sigma$ for $\zeta \in Q(\widetilde{\mathbb{I}})^\times$ independent of σ. Then replacing h by $h\zeta^{-1}$, we may assume that $h \in \mathrm{GL}_2(Q)$. Note that $h = zu$ with $u \in \mathrm{GL}_2(\widetilde{\mathbb{I}}_P)$. Since $h \in \mathrm{GL}_2(Q)$, the elementary divisor z of h can be chosen in $\mathrm{GL}_2(Q)$; so, we may assume that z is a scalar matrix in $\mathrm{GL}_2(Q)$; so, $u \in \mathrm{GL}_2(\Lambda_P)$. Thus $G = h \cdot Hh^{-1} \subset \mathrm{SL}_2(\Lambda_P)$, and $\Gamma(\mathfrak{c}) \subset G \supset h\Gamma(\mathfrak{c}')h^{-1} = z\Gamma(\mathfrak{c}')z^{-1} = \Gamma(\mathfrak{c}')$. Since z is a scalar, this implies $\mathfrak{c}_P = \mathfrak{c}'_P$ and hence $(L)_P$ is independent of choice of $\mathcal{L}_P$ up to scalars.

If $\rho_{\mathfrak{P}}$ is absolutely irreducible for all $\mathfrak{P}|P$, the P-adic completion $\widehat{\mathcal{L}}_P = \prod_{\mathfrak{P}|P} \widehat{\mathcal{L}}_{\mathfrak{P}}$ is unique up to scalars by a result of Serre and Carayol [Car94], where $\widehat{\mathcal{L}}_{\mathfrak{P}}$ is the $\mathfrak{P}$-adic completion of $\mathcal{L}_P$. So the independence of $(L)_P$ on $\mathcal{L}$ follows. □

Corollary 3.4. *Let $\mathbb{I}$ be a non-CM component and pick $\rho_{\mathbb{I}}$ with values in $\mathrm{GL}_2(\widetilde{\mathbb{I}})$. Let P be a prime divisor of Λ, and assume (Gal$_{\widetilde{\mathbb{I}}}$). Suppose one of the following three conditions:*

1. *we have $\sigma \in D_p$ such that $\mathrm{Ad}(\overline{\rho}(\sigma))$ has three distinct eigenvalues in $\mathbb{F}_p$;*
2. *we have $\sigma, \upsilon \in D_p$ such that $\overline{\rho}(\sigma)$ has two distinct eigenvalues in $\mathbb{F}_p$ and $\overline{\rho}(\upsilon)$ is a non-trivial unipotent element in $\mathrm{SL}_2(\mathbb{F})$;*
3. *we have $\sigma, \upsilon \in D_p$ such that $\overline{\rho}(\sigma)$ has two distinct eigenvalues in $\mathbb{F}_p$ and $\rho_{\mathfrak{P}}(\upsilon)$ is a non-trivial unipotent element in $\mathrm{SL}_2(\kappa(\mathfrak{P}))$ for all prime divisors $\mathfrak{P}|P$ of $\widetilde{\mathbb{I}}$.*

Assume that $\mathrm{Im}(\rho_{\mathbb{I}})$ has conductor $\mathfrak{c}$. Then $P \nmid \mathfrak{c}_P$ for a prime divisor P of $\mathrm{Spec}(\Lambda)$ if and only if $\overline{\mathbb{G}}_{\mathfrak{P}}$ for all prime divisors $\mathfrak{P}|P$ in $\widetilde{\mathbb{I}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$, up to conjugation.

Proof. We may assume that $\overline{\rho}(\sigma)$ and $\rho_{\mathbb{I}}(\upsilon)$ are upper triangular by (Gal$_{\widetilde{\mathbb{I}}}$). We replace $\mathbb{G}$ by its open p-profinite subgroup $\{g \in \mathbb{G} \mid (g \bmod \mathfrak{m}_{\mathbb{I}}) \in \mathcal{U}(\widetilde{\mathbb{I}}/\mathfrak{m}_{\widetilde{\mathbb{I}}})\}$. Then $\mathbb{G}$ is p-profinite, and all the assumptions are intact. In particular, it is still normalized by $\rho(\sigma)$ in assumptions (1–3) and contains $\rho(\upsilon)$ for υ in assumptions (2) and (3). By this modification, the assumptions of Lemma 2.9 are satisfied. Indeed, we may take $j = \lim_{n\to\infty} \rho(\sigma)^{p^n}$, and the unipotent part of $\rho(\upsilon)$ (which is found in $\mathbb{G}$ by a similar argument proving Lemma 1.4) does the job for υ in Lemma 2.9(2–3). Thus we can apply Lemma 2.9 in this setting. The direction ($\Rightarrow$) is plain; so, we assume that $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ for all $\mathfrak{P}|P$. Then by Lemma 3.2, $\overline{\mathbb{G}}_P$ contains an open subgroup of $\mathrm{SL}_2(A_0)$. Then we find $\alpha \in \mathcal{B}(\mathbb{I}_P)$ such that for $\rho' := \alpha\rho_{\mathbb{I}}\alpha^{-1}$, $\mathrm{Im}(\rho')$ has conductor $\mathfrak{c}'$ prime to P. Since $\rho_{\mathbb{I}}$ and ρ' are equivalent under $\mathrm{GL}_2(\mathbb{I}_P)$, by the above lemma, we find $\mathfrak{c}_P = \mathfrak{c}'_P$. Thus we get $P \nmid \mathfrak{c}$. □

When $\rho_{\mathfrak{P}}$ is reducible for some $\mathfrak{P}|P$, we have $\overline{\rho} \cong \left(\begin{smallmatrix}\overline{\theta} & 0\\ 0 & \overline{\psi}\end{smallmatrix}\right)$ for a character $\overline{\psi}$ unramified at p. In this case, we need to explore if we can define an optimal level $L(\mathbb{I})$. Our idea is to take $\rho_{\mathbb{I}}$ among its isogeny class with the deepest level at $\mathfrak{P}$. As already explained, this choice should be given by the representation realized by $\mathcal{L}_{\mathrm{can}} \otimes_{\mathbb{I}} \widetilde{\mathbb{I}}_{\mathfrak{P}}$. We call a prime divisor $\mathfrak{P}$ of $\mathbb{I}$ *reducible* if $\rho_{\mathfrak{P}}$ is reducible.

Lemma 3.5. *Let $\mathbb{I}$ be a non-CM component with normalization $\widetilde{\mathbb{I}}$ and put $\mathbb{G} = \mathrm{SL}_2(\widetilde{\mathbb{I}}) \cap \mathrm{Im}(\rho_{\mathbb{I}})$. Suppose one of the conditions (1–3) in Corollary 3.4 and (R) and (F) for $\rho_{\mathbb{I}}$. Suppose that there is no quadratic field $M_{/\mathbb{Q}}$ such that $\overline{\rho}$ is isomorphic to an induced representation from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$. Let P be a prime divisor of Λ with a reducible prime divisor $\mathfrak{P}$ of $\widetilde{\mathbb{I}}$ above P, and assume (Gal$_{\widetilde{\mathbb{I}}_P}$). Then we can find $\alpha \in \mathcal{B}(Q(\mathbb{I}))$ such that $\alpha\mathbb{G}\alpha^{-1} \cap \mathcal{U}(\Lambda)$ is equal to $\left(\begin{smallmatrix}1 & \mathfrak{u}\\ 0 & 1\end{smallmatrix}\right)$ for a Λ-ideal $\mathfrak{u}$ prime to P and $\alpha\mathbb{G}\alpha^{-1} \subset \mathrm{SL}_2(\widetilde{\mathbb{I}}_P)$. Moreover, defining $\mathfrak{c}_P$ by a Λ_P-ideal given by $\Lambda_P \cap \widetilde{\mathbb{I}}_P \cdot \mathfrak{n}_t^{(\alpha)}$ for $\mathfrak{n}_t^{(\alpha)} = \left\{u \in \widetilde{\mathbb{I}}_P \mid \left(\begin{smallmatrix}1 & 0\\ u & 1\end{smallmatrix}\right) \in \alpha\mathbb{G}\alpha^{-1}\right\}$, the Λ_P-ideal $\mathfrak{c}_P \subset \Lambda_P$ is independent of the choice of α.*

Under the circumstances in the lemma, for each prime divisor P over which we have no reducible prime divisor $\mathfrak{P}|P$ of $\mathbb{I}$, we put $\mathfrak{c}_P = \Lambda_P$. Then, abusing the language slightly, we set $(L(\mathbb{I}))$ to be the principal ideal $\bigcap_P \mathfrak{c}_P$. Non-existence of quadratic fields M as in the lemma is equivalent to the fact that $\overline{\theta}^{-1}\overline{\psi}$ is not a quadratic character (as we will see later in the proof of Theorem 8.8), and if $\overline{\theta}^{-1}\overline{\psi}|_{I_p}$ has order $\geqslant 3$, plainly condition (1) of Corollary 3.4 is satisfied.

Proof. We may replace $\mathbb{G}$ by $\{g \in \mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\widetilde{\mathbb{I}}) \mid (g \bmod \mathfrak{m}_{\widetilde{\mathbb{I}}}) \in \mathcal{U}(\widetilde{\mathbb{I}}/\mathfrak{m}_{\widetilde{\mathbb{I}}})\}$. Then $\mathbb{G}$ is a p-profinite subgroup of $\mathrm{SL}_2(\widetilde{\mathbb{I}})$. We proceed as in the proof of Lemma 2.9 looking into both $\mathcal{M}(\mathbb{G})$ and $\mathcal{M}_1(\mathbb{G})$ described above Theorem 1.1. Pick another prime divisor $\mathcal{P} \in \mathrm{Spec}(\Lambda)$ such that the image

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

of $\rho_{\mathcal{P}\mathbb{I}} = (\rho_{\mathbb{I}} \bmod \mathcal{P}\mathbb{I})$ contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ (any arithmetic prime does the job by Lemma 3.2). Then the derived group $\overline{\mathbb{G}}'_{\mathcal{P}}$ of the image $\overline{\mathbb{G}}_{\mathcal{P}}$ in $\mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathcal{P}\widetilde{\mathbb{I}})$ of $\mathbb{G}$ contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. In the same manner as in the proof of Lemma 2.9, we find that $\mathbb{U} := \mathbb{G} \cap \mathcal{U}(\widetilde{\mathbb{I}})$ contains the non-trivial image of $\mathbb{U}' = \mathbb{G}' \cap \mathcal{U}(\widetilde{\mathbb{I}})$ in $\mathcal{U}(\widetilde{\mathbb{I}}_{\mathcal{P}}/\mathcal{P}\widetilde{\mathbb{I}}_{\mathcal{P}})$, and for the Λ-module $\mathfrak{n}' = \{u \in \widetilde{\mathbb{I}} \mid \left(\begin{smallmatrix}1 & u\\ 0 & 1\end{smallmatrix}\right) \in \mathbb{G}\}$, the $\widetilde{\mathbb{I}}_{\mathcal{P}}$-ideal $\widetilde{\mathbb{I}}_{\mathcal{P}} \cdot \mathfrak{n}'$ is prime to $\mathcal{P}$. Then picking $b \in \mathfrak{n}'$ with non-trivial image in $\widetilde{\mathbb{I}}_{\mathcal{P}}/\mathcal{P}\widetilde{\mathbb{I}}_{\mathcal{P}}$, we find $\beta = \left(\begin{smallmatrix}b^{-1} & 0\\ 0 & 1\end{smallmatrix}\right) \in \mathcal{B}(\widetilde{\mathbb{I}}_{\mathcal{P}})$ such that $\beta\mathbb{G}\beta^{-1} \cap \mathcal{U}(\Lambda)$ contains U with $\overline{U} \neq 1$, and $\beta\mathbb{G}\beta^{-1}$ has conductor $\mathfrak{c}_\beta \neq 0$. Put $\mathfrak{n}'_t = \{u \in Q(\mathbb{I}) \mid \left(\begin{smallmatrix}1 & 0\\ u & 1\end{smallmatrix}\right) \in \beta\mathbb{G}\beta^{-1}\} \subset \widetilde{\mathbb{I}}$.

We now work over the ring $D = \widetilde{\mathbb{I}}_P \cap \widetilde{\mathbb{I}}_{\mathcal{P}} \subset Q(\mathbb{I})$. The ring D is semi-local of dimension 1 whose localizations are all discrete valuation rings, hence it is a principal ideal domain (cf. [Bou98, VII.3.6]). Let $\mathfrak{n}_0 = \{u \in \widetilde{\mathbb{I}} \mid \left(\begin{smallmatrix}1 & u\\ 0 & 1\end{smallmatrix}\right) \in \mathbb{G}\}$. Then we find $a \in D$ with $D \cdot \mathfrak{n}_0 = (a)$. We put $\alpha = \left(\begin{smallmatrix}a^{-1} & 0\\ 0 & 1\end{smallmatrix}\right) \in \mathcal{B}(Q(\mathbb{I}))$. Let $\mathfrak{N} = \mathbb{I} \cdot \mathfrak{n}_t$ for $\mathfrak{n}_t = \{u \in Q(\mathbb{I}) \mid \left(\begin{smallmatrix}1 & 0\\ u & 1\end{smallmatrix}\right) \in \alpha\mathbb{G}\alpha^{-1}\}$, and put $\mathfrak{n} = \{u \in Q(\mathbb{I}) \mid \left(\begin{smallmatrix}1 & u\\ 0 & 1\end{smallmatrix}\right) \in \alpha\mathbb{G}\alpha^{-1}\}$ which is contained in D because $D \cdot \mathfrak{n}_0 = (a)$. In any case, $\alpha\mathbb{G}\alpha^{-1}$ has conductor $\mathfrak{c}_\alpha \neq 0$. If $\mathfrak{P}'|P$ and $\mathrm{Im}(\rho_{\mathfrak{P}'})$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ (for A_0 with respect to $\kappa(\mathfrak{P}')$), then $a \in \widetilde{\mathbb{I}}^{\times}_{\mathfrak{P}'}$ and $\mathfrak{n}_{\mathfrak{P}'} = \widetilde{\mathbb{I}}_{\mathfrak{P}'}$. If $\rho_{\mathfrak{P}'}$ is absolutely irreducible but not full, the only possibility is $\rho_{\mathfrak{P}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \lambda$ (by Lemma 2.1 or Lemma 8.4), where M is a quadratic field and $\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \kappa(\mathfrak{P}')^\times$ is a character. Then $\overline{\rho}$ must be an induced representation from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$, which is prohibited by our assumption. Thus the conjugation by α has the following effect for $\mathfrak{P}|P$ and $\mathfrak{P}'|P$:

- for $\mathfrak{P}'$ with irreducible $\rho_{\mathfrak{P}'}$, we have $\mathfrak{n}_{\mathfrak{P}'} = \widetilde{\mathbb{I}}_{\mathfrak{P}'}$;
- for $\mathfrak{P}$ with reducible $\rho_{\mathfrak{P}}$, it maximizes $\mathfrak{n}_{\mathfrak{P}}$ to $\mathfrak{n}_{\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}}$ for $\mathfrak{P}$, and $\mathfrak{u}$ becomes prime to P;
- for $\mathfrak{P}$ with reducible $\rho_{\mathfrak{P}}$, it minimizes $\mathfrak{n}_{t,\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}} \cdot \mathfrak{n}_t$.

Thus $\mathfrak{u}, \mathfrak{n}, \mathfrak{n}_t \subset D$ with $D\mathfrak{u} = D$, and we still have $\alpha\mathbb{G}\alpha^{-1}$ in $\mathrm{SL}_2(D) \subset \mathrm{SL}_2(\widetilde{\mathbb{I}}_P)$. Therefore $G := \alpha\mathbb{G}\alpha^{-1} \cap \mathrm{SL}_2(\Lambda)$ has the maximal upper unipotent subgroup of the form

$$U(\mathfrak{u}) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathfrak{u} \right\} \tag{3.1}$$

for an ideal $\mathfrak{u} \subset \Lambda$ prime to P. We put $\mathfrak{C}_\alpha = (\mathbb{I} \cdot \mathfrak{n}_t) \cap \Lambda$ for $\mathfrak{n}_t$ defined for this $\alpha\mathbb{G}\alpha^{-1}$.

We want to show that $\mathfrak{C}_{\alpha,P} := \widetilde{\mathbb{I}}_P \cdot \mathfrak{C}_\alpha$ is independent of the choice of a and $\mathcal{P}$. Choose another point $\mathcal{P}'$ such that the image of $\rho_{\mathcal{P}'\mathbb{I}} = (\rho_{\mathbb{I}} \bmod \mathcal{P}'\mathbb{I})$ contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. Put $D' = \widetilde{\mathbb{I}}_P \cap \widetilde{\mathbb{I}}_{\mathcal{P}'} \cap \widetilde{\mathbb{I}}_{\mathcal{P}}$, and choose a generator $(b) = D' \cdot \mathfrak{n}$. Then for $\alpha' = \left(\begin{smallmatrix}b^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)$, $\alpha'\alpha^{-1} \in \mathcal{B}(\widetilde{\mathbb{I}}_P)$ as $a\widetilde{\mathbb{I}}_P = \widetilde{\mathbb{I}}_P \cdot \mathfrak{n} = b\widetilde{\mathbb{I}}_P$. Since $\alpha'\alpha^{-1} \in \mathcal{B}(\widetilde{\mathbb{I}}_P)$ is diagonal, we find $\mathfrak{C}_{\alpha,P} = \mathfrak{C}_{\alpha',P}$. Thus $\mathfrak{c}_P = \mathfrak{C}_{\alpha,P}$ is independent of the choice of $(a, \mathcal{P})$. For any other prime divisor P' with absolutely irreducible $\rho_{\mathfrak{P}'}$ for all $\mathfrak{P}'|P'$, we choose $\gamma \in \mathcal{B}(\widetilde{\mathbb{I}}_{P'})$ so that $\gamma\mathbb{G}\gamma^{-1}$ contains $\Gamma_\Lambda(\mathfrak{a}) \neq 1$. Let $\mathfrak{c}_\gamma$ be the conductor ideal of $\gamma\mathbb{G}\gamma^{-1}$. Then, as we have seen, under non-existence of the quadratic field M, $\mathrm{Im}(\rho_{\mathfrak{P}'})$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ for all $\mathfrak{P}'|P'$, and by Lemma 2.9, $\mathfrak{c}_{\gamma,P'} = \Lambda_{P'}$. Thus our definition of $\mathfrak{c}_{P'} = \Lambda_{P'}$ is legitimate, and $\mathfrak{c}_{P'} = \mathfrak{c}_{\gamma,P'} = \Lambda_{P'}$. Then $(L(\mathbb{I}))$ is the principal ideal $\bigcap_{P'} \mathfrak{c}_{P'}$, which is thus independent of our choice of the pair $(a, \mathcal{P})$. $\square$

In this reducible case, assuming that there is no quadratic field $M/\mathbb{Q}$ such that $\overline{\rho}$ is isomorphic to an induced representation from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$, we define $(L(\mathbb{I}))$ as in the above proof.

Corollary 3.6. *Let the notation and the assumption be as in Lemma 3.5. Normalize $\rho_{\mathbb{I}}$ as in Lemma 3.5. Let $P \in \mathrm{Spec}(\Lambda)$ be a prime divisor prime to (p) such that $\rho_{\mathfrak{P}}$ is reducible for some prime divisor $\mathfrak{P}|P$ of $\widetilde{\mathbb{I}}$. Then we have the following.*

(1) *For $\mathfrak{c}$ defined after Lemma 3.5, we have $\mathfrak{c}_P = \Lambda_P \cdot \mathfrak{u}_t$, where $\mathfrak{u}_t = \{c \in \Lambda \mid \left(\begin{smallmatrix}1 & 0\\ c & 1\end{smallmatrix}\right) \in \mathrm{Im}(\rho_{\mathbb{I}})\}$.*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

(2) *For the conductor* $\mathfrak{c}'$ *of* $\mathbb{G}$, *we have* $\mathfrak{c}_P = \mathfrak{c}'_P$.

(3) *The localization* $\mathfrak{c}_P$ *is equal to* $(\bigcap_{\mathfrak{P}|P} \mathfrak{a}_{\mathfrak{P}}) \cap \Lambda_P$ *for the minimal* $\widetilde{\mathbb{I}}_{\mathfrak{P}}$*-ideal* $\mathfrak{a}_{\mathfrak{P}}$ *such that the reduction* $(\rho_{\mathbb{I}} \bmod \mathfrak{a}_{\mathfrak{P}})$ *has values in* $\mathcal{B}(\widetilde{\mathbb{I}}_{\mathfrak{P}}/\mathfrak{a}_{\mathfrak{P}})$ *(up to conjugation).*

Proof. We first prove (1) and (3). By the proof of the above lemma, $\mathfrak{c}_P = (\widetilde{\mathbb{I}}_P \cdot \mathfrak{n}_t) \cap \Lambda_P$, which is equal to $(\Lambda_P \cdot \mathfrak{n}_t) \cap \Lambda_P$ since $\mathfrak{n}_t$ is a Λ-module. Thus $\widetilde{\mathbb{I}}_P \mathfrak{c}_P \subset \bigcap_{\mathfrak{P}|P} \mathfrak{a}_{\mathfrak{P}}$. Let $\rho_{\mathfrak{i}} = (\rho_{\mathbb{I}} \bmod \mathfrak{i})$ for an ideal $\mathfrak{i}$ of $\widetilde{\mathbb{I}}_{\mathfrak{P}}$. Suppose that $\mathfrak{a}_{\mathfrak{P}} \supsetneq \mathfrak{c}_{\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}} \mathfrak{c}_P$, for $\mathfrak{i} = \mathfrak{a}_{\mathfrak{P}} \mathfrak{P}$, consider $\rho_{\mathfrak{i}}$. Note that $\mathbb{G}$ acts on $\mathfrak{s}_{\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}} \cdot \mathcal{M}^0(\mathbb{G}) \subset \mathfrak{s}'_{\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}} \cdot \mathcal{M}^0_1(\mathbb{G})$ by adjoint action. Consider the image $\bar{\mathfrak{s}}_{\mathfrak{b}}$ of $\mathfrak{s}_{\mathfrak{P}}$ in $\mathfrak{sl}_2(\widetilde{\mathbb{I}}_{\mathfrak{P}}/\mathfrak{b})$ for an $\widetilde{\mathbb{I}}_{\mathfrak{P}}$-ideal $\mathfrak{b}$. Then we have an exact sequence of $\widetilde{\mathbb{I}}_{\mathfrak{P}}[\widetilde{\mathbb{G}}]$-modules $0 \to \overline{V} \to \bar{\mathfrak{s}}_{\mathfrak{i}} \to \bar{\mathfrak{s}}_{\mathfrak{a}_{\mathfrak{P}}} \to 0$ for $\widetilde{\mathbb{G}} = \mathrm{Im}(\rho'_{\mathbb{I}})$. Then $\overline{V}$ is a $\kappa(\mathfrak{P})$ vector space of dimension at most 3. If $\overline{V}$ is made up of upper triangular matrices, $\bar{\mathfrak{s}}_{\mathfrak{i}} \subset \mathfrak{B}(\widetilde{\mathbb{I}}_{\mathfrak{P}}/\mathfrak{i})$, and $\rho_{\mathfrak{i}}$ has values in $\mathcal{B}(\widetilde{\mathbb{I}}_{\mathfrak{P}}/\mathfrak{i})$, a contradiction to the minimality of $\mathfrak{a}_{\mathfrak{P}}$. Thus we have $0 \neq X = \left(\begin{smallmatrix} 0 & 0 \\ v & 0 \end{smallmatrix}\right) \in \overline{V} \cap {}^t\mathfrak{U}(\widetilde{\mathbb{I}}_{\mathfrak{P}}/\mathfrak{i})$. We also have $Y = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{n}$. Then $0 \neq [X, Y] = \left(\begin{smallmatrix} v & 0 \\ 0 & -v \end{smallmatrix}\right)$. This shows that $\dim_{\kappa(\mathfrak{P})} \overline{V} = 3$. By Nakayama's lemma, we find $V = \mathrm{Ker}(\mathfrak{s}_{\mathfrak{P}} \to \bar{\mathfrak{s}}_{\mathfrak{a}_{\mathfrak{P}}}) = \mathfrak{a}_{\mathfrak{P}} \cdot \mathfrak{sl}_2(\widetilde{\mathbb{I}}_{\mathfrak{P}})$. This shows $\mathfrak{a}_{\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}} \mathfrak{n}_t \supset \widetilde{\mathbb{I}}_{\mathfrak{P}} \mathfrak{u}_t$ for $\mathfrak{u}_t = \mathfrak{n}_t \cap \Lambda$.

To show $\mathfrak{a}_{\mathfrak{P}} = \widetilde{\mathbb{I}}_{\mathfrak{P}} \mathfrak{u}_t$, replace $Q(\mathbb{I})$ by its Galois closure over Q and $\widetilde{\mathbb{I}}$ by the integral closure in the Galois closure. Thus $\widetilde{\mathbb{I}}/\Lambda$ is a Galois covering with finite Galois group $\mathfrak{g}$. Then $\mathfrak{a}_{\mathfrak{P}} = \mathfrak{P}^{\varepsilon(\mathfrak{P})}$. We take $\varepsilon = \max(\varepsilon(\mathfrak{P}))_{\mathfrak{P}|P}$ and write $P^{\epsilon} = \mathfrak{P}^{\varepsilon} \cap \Lambda$ which is independent of the choice of $\mathfrak{P}$. Let $P^{\epsilon} \widetilde{\mathbb{I}}_{\mathfrak{P}} = \mathfrak{P}^e$. Replace $\mathbb{G}$ by $\{g \in \mathbb{G} \mid (g \bmod P^{\epsilon}) \in \mathcal{B}(\widetilde{\mathbb{I}}_P/P^{\epsilon}\widetilde{\mathbb{I}}_P)\}$. Then by the above argument, the kernel $V = \mathrm{Ker}(\mathfrak{s}_{P^{\epsilon}} \to \bar{\mathfrak{s}}_{P^{\epsilon}})$ is given by $P^{\epsilon} \cdot \mathfrak{sl}_2(\widetilde{\mathbb{I}}_P)$. Thus $\mathfrak{n}_t$ has v with non-zero image in $\mathfrak{P}^e/\mathfrak{P}^{e+1}$ for all $\mathfrak{P}|P$. By Nakayama's lemma again, we have $V = \widetilde{\mathbb{I}}_P v = P^{\epsilon} \cdot {}^t\mathfrak{U}(\widetilde{\mathbb{I}}_P)$; so, $\widetilde{\mathbb{I}}_P v$ is a $\mathfrak{g}$-module, and $\mathfrak{u}_t \subset H^0(\mathfrak{g}, \widetilde{\mathbb{I}}_P v) =: \mathfrak{u}'_t$. We have an exact sequence $0 \to PV \to V \to \overline{V} \to 0$. Taking $\mathfrak{g}$-invariant, we have another exact sequence $0 \to H^0(\mathfrak{g}, PV) \to H^0(\mathfrak{g}, V) \to H^0(\mathfrak{g}, \overline{V}) \to 0$ as V and $\overline{V}$ are a $\mathbb{Q}_p$-vector spaces. This shows $\widetilde{\mathbb{I}}_P \mathfrak{u}'_t = P^{\epsilon} \widetilde{\mathbb{I}}_P$. Thus $\mathfrak{u}'_t \widetilde{\mathbb{I}}_P \cap \Lambda_P = \mathfrak{n}_t \widetilde{\mathbb{I}}_P \cap \Lambda_P$, which implies $\mathfrak{u}'_t = \widetilde{\mathbb{I}}_P \mathfrak{n}_t \cap \Lambda_P = \Lambda_P \mathfrak{u}_t$, by definition. Then we have $\mathfrak{c}_P = \Lambda_P \mathfrak{u}_t = P^{\epsilon} \Lambda_P$. By our construction, we get $\mathfrak{c}_P = P^{\epsilon} \widetilde{\mathbb{I}}_P = \bigcap_{\mathfrak{P}|P} \mathfrak{a}_{\mathfrak{P}} \cap \Lambda_P$, proving (1) and (3).

We prove (2). Since we normalized $\mathbb{G}$ by conjugating by α as in the proof of Lemma 3.5, by (3.1), for $G := \mathbb{G} \cap \mathrm{SL}_2(\Lambda)$, we have $G \cap \mathcal{U}(\Lambda) = U(\mathfrak{u}) = \left\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathfrak{u}\right\}$ for an ideal $\mathfrak{u} \subset \Lambda$ prime to P. By a simple computation, for $c \in \mathfrak{u}_t$, we have

$$\begin{aligned}
&\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 1+bc & b \\ c & 1 \end{pmatrix}, \\
&\begin{pmatrix} 1+bc & b \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & -(1+bc)^{-1}b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+bc & 0 \\ c & 1-bc(1+bc)^{-1} \end{pmatrix}, \\
&\begin{pmatrix} 1 & 0 \\ -c(1+bc)^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1+bc & 0 \\ c & 1-bc(1+bc)^{-1} \end{pmatrix} = \begin{pmatrix} 1+bc & 0 \\ 0 & (1+bc)^{-1} \end{pmatrix}.
\end{aligned} \tag{3.2}$$

Thus $\mathcal{M}_1(G)$ contains $\mathfrak{A} := \left\{\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \mid a \in (p) \cap \mathfrak{u}\mathfrak{u}_t, b \in (p) \cap \mathfrak{u}, c \in \mathfrak{u}_t\right\}$. This shows the existence of $\mathfrak{c}''$ with $\mathfrak{c}''_P = \mathfrak{u}_{t,P} = \mathfrak{c}_P$ such that $\Gamma_\Lambda(\mathfrak{c}'') \subset G$. Thus $\mathfrak{c}'' \subset \mathfrak{c}'$. By (1) and (3), it is clear that $\mathfrak{c}''_P \supset \mathfrak{c}'_P$. This finishes the proof of (2). □

4. Eisenstein components

We now describe explicitly the congruence between the Eisenstein component and the cuspidal component (a description of Eisenstein ideal in the big Hecke algebra) via the theory of Λ-adic form.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

We first define the Eisenstein component of the space of Λ-adic forms. Let $\mathcal{M}(N,\chi_1;\Lambda_W)$ (respectively $\mathcal{S}(N,\chi_1;\Lambda_W)$) be the space of p-ordinary Λ_W-adic modular forms (respectively p-ordinary Λ_W-adic cusp forms). Thus $\mathcal{M}(N,\chi_1;\Lambda_W)$ (respectively $\mathcal{S}(N,\chi_1;\Lambda_W)$) is a collection of all formal q-expansions $F(q)=\sum_{n=0}^{\infty}a(n,F)(T)q^n\in\Lambda_W[[q]]$ such that $f_P=\sum_{n=0}^{\infty}(a(n,F) \bmod P)q^n$ gives rise to a modular form in $\mathcal{M}_{k+1}^{\mathrm{ord}}(\Gamma_0(Np^{r(P)+1}),\varepsilon_P\chi_{k(P)})$ (respectively $\mathcal{S}_{k+1}^{\mathrm{ord}}(\Gamma_0(Np^{r(P)+1}),\varepsilon_P\chi_{k(P)})$) for all arithmetic points P, where $p^{r(P)}$ is the order of ε_P. Again $F\mapsto f_P$ induces an isomorphism

$$\mathcal{M}(N,\chi_1;\Lambda_W)\otimes_{\Lambda_W}\Lambda_W/P\cong\mathcal{M}_{k+1}^{\mathrm{ord}}(\Gamma_0(Np^{r(P)+1}),\chi_k\varepsilon_P;W[\varepsilon_P])$$

for all arithmetic points (see [Hid11a, Theorem 3.2.15 and Corollary 3.2.18] or [Hid93, § 7.3]). This implies that $\mathcal{M}(N,\chi_1;\Lambda_W)$ and $\mathcal{S}(N,\chi_1;\Lambda_W)$ are free of finite rank over Λ_W, and the Λ_W-module $\mathcal{M}(N,\chi_1;\Lambda_W)$ (respectively $\mathcal{S}(N,\chi_1;\Lambda_W)$) is naturally a faithful module over $\mathbf{H}$ (respectively $\mathbf{h}$). The above specialization map is compatible with the Hecke operator action. Recall the quotient field Q of Λ, and take an algebraic closure $\overline{Q}$ of Q. We can extend scalars to an extension A/Λ_W inside $\overline{Q}$ to define $\mathcal{S}(N,\chi_1;A)=\mathcal{S}(N,\chi_1;\Lambda_W)\otimes_{\Lambda_W}A$ and $\mathcal{M}(N,\chi_1;A)=\mathcal{M}(N,\chi_1;\Lambda_W)\otimes_{\Lambda_W}A$. If $A=\mathbb{I}$ is finite over Λ_W, associating the family $\{f_P\}_{P\in\mathrm{Spec}(\mathbb{I})}$ to a form $F\in\mathcal{M}(N,\chi_1;\mathbb{I})$, we may regard these as spaces of 'analytic families of slope 0 of modular forms' with coefficients in $\mathbb{I}$ (we also call them the space of $\mathbb{I}$-adic p-ordinary cusp forms and the space of $\mathbb{I}$-adic p-ordinary modular forms, respectively). See [Hid93, ch. 7], [Hid11a, ch. 3] and [Hid86a] for these facts.

Let $Q_W=Q(\Lambda_W)$ (and regard Q_W as a subfield of $\overline{Q}$ when W is finite over $\mathbb{Z}_p$). Then we have

$$\mathcal{M}(N,\chi_1;Q_W)=\mathcal{S}(N,\chi_1;Q_W)\oplus\mathcal{E}(N,\chi_1;Q_W)$$

as modules over $\mathbf{H}$. The space $\mathcal{E}(N,\chi_1;Q_W)$ is spanned by Λ-adic Eisenstein series. Assuming that N is cube-free, we make explicit the Eisenstein series: for any character $\psi:(\mathbb{Z}/M_1\mathbb{Z})^\times\to W^\times,\theta:(\mathbb{Z}/M_2\mathbb{Z})^\times\to W^\times$ with $\psi\theta=\chi_1$, $M_1M_2|Np$, $p|M_2$ and $p\nmid M_1$, there exists a unique Λ-adic Eisenstein series in $\mathcal{M}(N,\chi_1;Q_W)$ defined by its q-expansion

$$a(\theta,\psi)(T)+\sum_{n=1}^{\infty}\biggl(\sum_{0<d|n,p\nmid d}\theta(d)\psi\Bigl(\frac{n}{d}\Bigr)\langle d\rangle(T)\biggr)q^n,$$

where $\langle d\rangle(T)=t^{\log_p(d)/\log_p(\gamma)}$, $a(\theta,\psi)=0$ if ψ is non-trivial, and otherwise, writing $\mathbf{1}_M$ for the trivial character modulo M, $a(\theta,\mathbf{1}_{M_1})=\frac{1}{2}G(T)\in Q_W$ with

$$G(\gamma^k-1)=(1-\theta_{k+1}(p)p^k)L^{(M_1)}(-k,\theta_{k+1})\quad\text{for all } 0\leqslant k\in\mathbb{Z}.$$

As a convention, we put $\theta(d)=0$ if d has a non-trivial common factor with M_2 and that $\psi(d)=0$ if d has a non-trivial common factor with M_1, and also θ_k is the character of $(\mathbb{Z}/M_2p\mathbb{Z})^\times$ given by $\theta_k=\theta\omega^{1-k}$. We define $L^{(M_1)}(s,\theta_{k+1})=\sum_{n=1}^{\infty}\theta_{k+1}(n)n^{-s}$ for this possibly imprimitive θ_{k+1}. The existence of the above Eisenstein series is proven under $M_1M_2\mid Np$ (cf. [Hid86a, Theorem 7.2] or [Oht03, § 1.4]). Counting the number of pairs (θ,ψ), we prove that they span over Q_W a Hecke stable subspace $\mathcal{E}(N,\chi_1;Q_W)$ in $\mathcal{M}(N,\chi_1;Q_W)$ complementary to $\mathcal{S}(N,\chi_1;Q_W)$ if N is cube-free (e.g. [Hid86b, § 5]).

Our next goal is to extend Ohta's construction of Eisenstein series to imprimitive ones assuming that N is cube-free. In this way, we explicitly make a canonical Hecke eigenbasis of the Eisenstein component, which enables us to split Ohta's residue exact sequence (4.1) in Proposition 4.2 and to compute the characteristic power series of the Eisenstein congruence module in Corollary 4.3.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

Let us prepare some notation to state Ohta's exact sequence. For a profinite group G, we write $W[[G]] = \varprojlim_H W[G/H]$ for the continuous group algebra, where H runs over open subgroups of G. In particular, for the multiplicative group $\Gamma = 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$, we can identify $W[[\Gamma]]$ with Λ_W by sending $\gamma \in \Gamma$ to t. Let $C_r = C_r(N)$ be the set of all cusps of $X_r := X_1(Np^{r+1})(\mathbb{C})$, and consider the formal linear span $W[C_r] = \{\sum_{s\in C_r} a_s s \mid a_s \in W\}$. Write simply $\Gamma_r := \Gamma_1(Np^{r+1})$. Since the Hecke correspondence $T_{r,s}(\alpha) \subset X_1(Np^r) \times X_1(Np^s)$ associated to the double coset $\Gamma_s\alpha\Gamma_r$ for $\alpha \in \mathrm{GL}_2(\mathbb{Q})$ (with $\det(\alpha) > 0$) gives rise to a correspondence on $C_r \times C_s$ for $r, s \geqslant 0$, the Hecke correspondence acts on $W[C_r]$. In particular, $W[C_r]$ is equipped with the action of $T(l)$, $T(l,l)$ in [Shi71, ch. 3] and $U(q)$ $(q \mid Np)$, $\langle z\rangle = z_p\cdot[\Gamma_r\sigma_z\Gamma_r]$ for $z = (z_p, z_N) \in \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$ with $z_p \in \mathbb{Z}_p^\times$, where $\sigma_z \in \mathrm{SL}_2(\mathbb{Z})$ with $\sigma_z \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & z \end{smallmatrix}\right) \bmod Np^r$. The coset $[q] = [\Gamma(Np^r)\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(Np^r/q)]$ for a prime $q \mid N$ gives rise to a linear map $[q] : W[C_r(N)] \to W[C_r(N/q)]$.

These operators are computed explicitly, choosing a standard representative set $A_{Np^r}/\sim$ (see below for A_{Np^r}) for the cusps $C_r(N) := \Gamma_1(Np^r)\backslash\mathbf{P}^1(\mathbb{Q}) \subset X_r(\mathbb{C})$ in [Oht03, § 2.1], where the action of $T(l)$ $(l \nmid Np)$ is denoted by $T^*(l)$ and $U(q)$ $(q|Np)$ is denoted by $T^*(q)$ in Ohta's paper. The covering map $X_s \twoheadrightarrow X_r$ for $s > r$ induces a projection $\pi_{s,r} : W[C_s] \twoheadrightarrow W[C_r]$, and we define $W[[C_\infty(N)]] := \varprojlim_r W[C_r(N)]$. Since Hecke operators $T(l)$, $l\cdot T(l,l) = \langle l\rangle$ for $l \nmid Np$, $U(q)$, $\langle z\rangle$ and $[q]$ are compatible with the projection $\pi_{s,r}$, these operators act on $W[[C_\infty(N)]]$. We let the group $\mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$ act on $W[[C_\infty]]$ by the character $l \mapsto l\cdot T(l,l)$ for primes l diagonally embedded in $\mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. Thus $W[[C_\infty(N)]]$ is a module over $W[[\mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times]] = \varprojlim_r W[(\mathbb{Z}/Np^r\mathbb{Z})^\times]$ via the action of $\langle z\rangle$ and hence is a module over $\Lambda_W = W[[\Gamma]]$ as $\Gamma \subset \mathbb{Z}_p^\times$. Then we confirm $T(l), T(l,l), U(q) \in \mathrm{End}_{W[[\Gamma]]}(W[[C_\infty(N)]])$ and that $[q] : W[[C_\infty(N)]] \to W[[C_\infty(N/q)]]$ are $W[[\Gamma]]$-linear maps. Then the p-adic projector $e = \lim_{n\to\infty} U(p)^{n!}$ is well defined on $W[C_r]$ and on $W[[C_\infty]]$. Recalling the identification $W[[\Gamma]]$ with $\Lambda_W = W[[T]]$ by $\gamma = 1 + p \mapsto t$, we endow $e \cdot W[[C_\infty]]$ with a Λ_W-module structure. On $e \cdot W[[C_\infty]]$, Hecke operators act Λ_W-linearly. As proved in [Oht99, Proposition 4.3.14], $e \cdot W[[C_\infty]]$ is free of finite rank over Λ_W (and the rank is given explicitly there). Ohta's choice of the action of $\mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$ is one time twist of our action by the p-adic cyclotomic character; so, the definition of $E(\theta, \psi)$ looks a bit different from ours, but our definition is equivalent to that of [Oht03] with this twist. Supposing that $p \nmid \varphi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times|$, we can decompose

$$e \cdot W[[C_\infty]] = \bigoplus_\psi e \cdot W[[C_\infty]][\psi],$$

where $e \cdot W[[C_\infty]][\psi]$ is the ψ-eigenspace of a character $\psi : (\mu_{p-1} \times (\mathbb{Z}/N\mathbb{Z})^\times) \to W^\times$ regarding $(\mu_{p-1} \times (\mathbb{Z}/N\mathbb{Z})^\times) \subset \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. Then from a result of Ohta [Oht03, (2.4.6)], assuming $p \geqslant 5$, for a prime divisor $P \in \mathrm{Spec}(\Lambda_W)$ prime to $(\varphi(N)) = \varphi(N)\Lambda_W$, we deduce a P-localized version of the canonical exact sequence of Hecke equivariant maps in [Oht03, (2.4.6)],

$$0 \to \mathcal{S}(N, \chi_1; \Lambda_W)_P \to \mathcal{M}(N, \chi_1; \Lambda_W)_P \xrightarrow{\mathrm{Res}} e \cdot W[[C_\infty]][\chi_1]_P \to 0, \tag{4.1}$$

where the last map Res is canonical and called the residue map in [Oht03]. This sequence is valid without localization if $p \nmid \varphi(N)$. Thus as Hecke modules, $e \cdot W[[C_\infty]][\chi_1] \otimes_{\Lambda_W} Q \cong \mathcal{E}(N, \chi_1; Q)$.

We extend this definition of $e \cdot W[[C_\infty]]$. Take a prime q outside pN and consider the $\mathbb{C}$-points of the elliptic Shimura curve $\mathbb{X}(N; q^j) = \mathrm{GL}_2(\mathbb{Q})\backslash(\mathrm{GL}_2(\mathbb{A}^{(\infty)}) \times (\mathbb{C} - \mathbb{R}))/\Delta(Nq^j)$ and its connected component $X(N; q^j) = \mathrm{SL}_2(\mathbb{Q})\backslash(\mathrm{SL}_2(\mathbb{A}^{(\infty)}) \times \mathfrak{H})/\Delta(Nq^j) \cap \mathrm{SL}_2(\mathbb{A}^{(\infty)})$, where

$$\begin{gathered}\Delta(Nq^j) = \widehat{\Gamma}_1(N) \cap \widehat{\Gamma}(q^j), \widehat{\Gamma}(q^j) = \{x \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \mid x \equiv 1 \bmod q^j M_2(\widehat{\mathbb{Z}})\}, \\ \widehat{\Gamma}_1(N) = \left\{x \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \;\middle|\; x \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \bmod NM_2(\widehat{\mathbb{Z}})\right\}.\end{gathered} \tag{4.2}$$

Note that $\mathbb{X}(N;q^j)$ is isomorphic to a disjoint union of copies of $X(N;q^j)$ indexed by $(\mathbb{Z}/q^j\mathbb{Z})^\times$. We write $\mathbf{C}(N;q^j)$ (respectively $C(N;q^j)$) be the set of cusps of $\mathbb{X}(N;q^j)$ (respectively $X(N;q^j)$). Then we have $C(Np^r;q^j) \cong \{(A_N/\sim) \times A_{q^j}\}/\{\pm 1\}$, where

$$A_N = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in (\mathbb{Z}/N\mathbb{Z})^2 \,\middle|\, x(\mathbb{Z}/N\mathbb{Z}) + y(\mathbb{Z}/N\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z} \right\}$$

with $\binom{x}{y} \sim \binom{x'}{y'} \Leftrightarrow y = y'$ and $x \equiv x' \bmod y(\mathbb{Z}/N\mathbb{Z})$. If $\{\pm 1\}$ acts freely on A_N, we have

$$C(N;q^j) \cong ((A_N/\sim) \times A_{q^j})/\{\pm 1\} \cong ((A_N/\sim)/\{\pm 1\}) \times A_{q^j}.$$

Replacing the auxiliary level N by Np^r for sufficiently large r (noting $p \geqslant 5$), we may assume that $\{\pm 1\}$ acts freely on A_{Np^r}. Thus for $r \gg 0$, we have

$$\mathbf{C}(Np^r;q^j) \cong \bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} ((A_{Np^r}/\sim) \times A_{q^j})/\{\pm 1\} \cong \bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} ((A_{Np^r}/\sim)/\{\pm 1\} \times A_{q^j}).$$

As before (see [Oht03, § 2.1]), $\mathrm{GL}_2(\mathbb{Z}_q)$ acts on A_{q^j} by natural left multiplication on column vectors. Then $u \in \mathrm{GL}_2(\mathbb{Z}_q)$ acts on $\bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} A_{q^j}$ via this multiplication but also permuting indices in $(\mathbb{Z}/q^j\mathbb{Z})^\times$ via multiplication by $\det(u)$. The set $\mathbf{C}(Np^r;q^j)$ of cusps inherits the $\mathrm{GL}_2(\mathbb{Z}_q)$-action from the curve $\mathbb{X}(Np^r;q^j)$, and this action is compatible with the action (including permutation of the components) on $\bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} A_{q^j}$. Consider $W[[\mathbf{C}(Np^\infty;q^j)]] = \varprojlim_r W[\mathbf{C}(Np^r;q^j)]$, which is naturally a Λ_W-module in the same manner as for $W[[C_\infty(N)]]$ through the action of $\mathbb{Z}_p^\times$ on $(A_{Np^r}/\sim)$. Then we define $V_q = \varinjlim_j W[[\mathbf{C}(Np^\infty;q^j)]]$, where we regard

$$W[[\mathbf{C}(Np^\infty;q^j)]] = \bigoplus_{(\mathbb{Z}/q^j\mathbb{Z})^\times} W[[C_\infty(N)]][A_{q^j}]$$

as a space of $W[[C_\infty]]$-valued functions on $\bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} A_{q^j}$, and by the pull-back of the projection $\bigsqcup_{(\mathbb{Z}/q^{j+1}\mathbb{Z})^\times} A_{q^{j+1}} \twoheadrightarrow \bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} A_{q^j}$, we have taken the *inductive* limit. The idempotent e is well defined on V_q, and we have $e \cdot V_q = \varinjlim_j e \cdot W[[\mathbf{C}(Np^\infty;q^j)]]$.

On the pro-curve $\mathbb{X}(Np^r;q^\infty) = \varprojlim_j \mathbb{X}(Np^r;q^j) \cong \mathrm{GL}_2(\mathbb{Q})\backslash(\mathrm{GL}_2(\mathbb{A}^{(\infty)}) \times (\mathbb{C} - \mathbb{R}))/\Delta(Nq^\infty)$ for $\Delta(Nq^\infty) = \bigcap_j \Delta(Nq^j) = \{x \in \Delta(N) \mid x_q = 1\}$, $\mathrm{GL}_2(\mathbb{Q}_q)$ acts by right multiplication, which induces the (correspondence) action of $\mathrm{GL}_2(\mathbb{Q}_q)$ on the cusps and induces a left action of $\mathrm{GL}_2(\mathbb{Q}_q)$ on V_q. This $\mathrm{GL}_2(\mathbb{Q}_q)$-action induces the action of the maximal open compact subgroup $\mathrm{GL}_2(\mathbb{Z}_q)$ already described on $\bigsqcup_{(\mathbb{Z}/q^j\mathbb{Z})^\times} A_{q^j}$. Plainly V_q is a smooth representation of $\mathrm{GL}_2(\mathbb{Q}_q)$ with coefficients in Λ_W. At each finite q-level, $e \cdot W[[\mathbf{C}(Np^\infty;q^j)]]$ is free of finite rank over Λ_W as proved by Ohta in [Oht99, § 4.3]. Though the curve $X_1(Np^r)$ is specifically dealt with in [Oht99, § 4.3], the argument for $\mathbb{X}(Np^r;q^j)$ is the same, or actually for a suitable choice of $g \in \mathrm{GL}_2(\mathbb{Q}_q)$ (such that $g^{-1}\widehat{\Gamma}(q^j)_q g \supset \widehat{\Gamma}_1(q^{2j})_q$ for the principal congruence subgroup $\widehat{\Gamma}(q^j)_q \subset \mathrm{GL}_2(\mathbb{Z}_q)$), the right multiplication by g induces a Γ-equivariant covering $X_1(Np^rq^{2j}) \xrightarrow{g} \mathbb{X}(Np^r;q^j)^\circ$ for any geometrically connected component $\mathbb{X}(Np^r;q^j)^\circ$; so, Ohta's result actually implies this finiteness. We have

$$H^0(\widehat{\Gamma}(q^j)_q, e \cdot V_q) = e \cdot W[[\mathbf{C}(Np^\infty;q^j)]],$$

which is free of finite rank over Λ_W. Thus $e \cdot V_q \otimes_{\Lambda_W} Q_W$ is a finitely generated admissible smooth representation of $\mathrm{GL}_2(\mathbb{Q}_q)$, and $e \cdot V_q$ is a Λ_W-lattice stable under the $\mathrm{GL}_2(\mathbb{Q}_q)$-action.

Over the pairs of characters (θ,ψ) defined modulo M_1 and M_2 respectively, we confirm that $\mathcal{E}(N,\chi_1;Q)$ is a direct sum of Hecke eigenspaces spanned by $E(\theta,\psi)$. Let $P\in\mathrm{Spec}(\Lambda_W)$ be a prime divisor. Assuming $p\nmid\varphi(N)$ if P is above $(p)\subset\Lambda$, it is easy to see that systems of the Hecke eigenvalues of $E(\theta,\psi)$ are distinct modulo the prime divisor P. Thus $e\cdot W[[C_\infty]][\chi_1]_P=\bigoplus_{(\theta,\psi)}\Lambda_{W,P}e(\theta,\psi)$ for an eigenbasis $e(\theta,\psi)$ with the same eigenvalues as $E(\theta,\psi)$. Ohta showed

$$\mathrm{Res}(E(\theta,\psi))=A(T;\theta,\psi)e(\theta,\psi)\quad\text{for } A(T;\theta,\psi)\in\Lambda_W,\tag{4.3}$$

where $A(T;\theta,\psi)\in\Lambda_W$ is given as follows [Oht03, 2.4.10]. Taking the power series $G(T;\xi)\in\Lambda_W$ so that $G(\gamma^s-1;\xi)=L_p(-s,\xi\omega)$ $(\gamma=1+p)$ for the Kubota–Leopoldt p-adic L-function $L_p(s,\xi)$ with a primitive even Dirichlet character ξ, $A(T;\theta,\psi)$ is given by, up to units in Λ_W,

$$\begin{cases}T'\cdot G(T;\theta\psi^{-1}\omega)\prod_{l|N}\{\omega(l)l^{-1}(\langle l\rangle(T)-\theta\psi^{-1}\omega(l)l^{-1})\} & \text{if } (\theta,\psi)=(\omega_{M_2}^{-1},\mathbf{1}_{M_1}),\\ G(T;\theta\psi^{-1}\omega)\prod_{l|N,l\nmid\mathfrak{C}(\theta\psi^{-1})}\{\omega(l)l^{-1}(\langle l\rangle(T)-\theta\psi^{-1}\omega(l)l^{-1})\} & \text{otherwise,}\end{cases}\tag{4.4}$$

where $T'=t-\gamma^{-1}$ and $\mathfrak{C}(\xi)$ is the conductor of the Dirichlet character ξ. Here ψ_{M_1} is a Dirichlet character modulo M_1. In the exceptional case $(\theta,\psi)=(\omega^{-1},\mathbf{1}_1)$ (which is equivalent to the case of $(\omega^{-2},\mathbf{1}_1)$ in Ohta's paper), as is well known, the Eisenstein ideal is trivial and $A(T;\omega^{-1},\mathbf{1}_1)\in\Lambda^\times$.

Definition 4.1. (1) Let $\mathbb{L}_{N,\chi_1}$ be the product $\prod_{(\theta,\psi),\theta\psi=\chi_1}A(T;\theta,\psi)$ for the pairs (θ,ψ) running over all characters with $M_1M_2\mid Np$ except for the pair induced by $(\omega^{-1},\mathbf{1}_1)$.

(2) Put $\overline{\theta}=\theta \bmod \mathfrak{m}_W$ and $\overline{\psi}=\psi \bmod \mathfrak{m}_W$. Put $L(\overline{\theta},\overline{\psi}):=\prod_{(\theta,\psi)}A(T;\theta,\psi)$ in $\mathbb{I}$, where (θ,ψ) runs over pairs of characters defined modulo M_1p and M_2, respectively, with $M_1M_2\mid N$ having reduction $(\overline{\theta},\overline{\psi})$ modulo p as characters of $\mathbb{Z}_p^\times\times(\mathbb{Z}/N\mathbb{Z})^\times$.

Letting $\sigma\in D_p$ act on $W[[T]]$ by $(\sum_n a_nT^n)^\sigma=\sum_n a_n^\sigma T^n$, we know that $A(T;\theta,\psi)^\sigma=A(T;\theta^\sigma,\psi^\sigma)$; so, $\mathbb{L}_{N,\chi_1}$ is Galois invariant, and hence $\mathbb{L}_{N,\chi_1}\in\Lambda=\mathbb{Z}_p[[T]]$. The following proposition is basically proven in [Oht03, Theorem 1.5.5]. Since in the statement in [Oht03], he assumes $N|\mathfrak{C}(\theta)\mathfrak{C}(\psi)$, we give a proof under cube-freeness of N via the theory of admissible representation of $\mathrm{GL}_2(\mathbb{Q}_q)$.

Proposition 4.2. *Let the notation be as above. Suppose $p\geqslant 5$ and that N is cube free. Let P be a prime divisor of Λ_W prime to $(\mathbb{L}_{N,\chi_1})\subset\Lambda_W$ and $\varphi(N)\Lambda_W$. After tensoring the localization $\Lambda_{W,P}$ at the prime P, Ohta's exact sequence (4.1) is split as a sequence of $\mathbf{H}_P$-modules.*

Proof. By assumption, if $(\theta,\psi)\neq(\omega^{-1},\mathbf{1}_1)$, $P\nmid A(T;\theta,\psi)$ in $W[[T]]$. Thus $A(T;\theta,\psi)\in\Lambda_{W,P}^\times$. So, if $N=1$, we can define the Hecke equivariant section: $e\cdot W[[C_\infty]][\chi_1]\to\mathcal{M}(N,\chi_1;\Lambda_W)$ by $e(\theta,\psi)\mapsto E(\theta,\psi)$ for $(\theta,\psi)\neq(\omega^{-1},\mathbf{1}_1)$, and $e(\omega^{-1},\mathbf{1}_1)\mapsto t\cdot E(\omega^{-1},\mathbf{1}_1)$ otherwise $(t'=t-\gamma^{-1})$. This gives rise to a section over $\Lambda_{W,P}$ of $\mathbf{H}_P$-modules.

We proceed by induction on the number of prime factors of N. Suppose we have a section

$$e\cdot W[[C_\infty(N/q)]]_P\to\mathcal{M}(N/q,\chi_1;\Lambda_{W,P})$$

for $\mathcal{M}(N/q,\chi_1;\Lambda_{W,P})=\mathcal{M}(N/q,\chi_1;\Lambda_W)\otimes_{\Lambda_W}\Lambda_{W,P}$. Take (θ,ψ) with $M_1M_2|N/q$. We claim that

(C) *the space V spanned by $e(\theta,\psi)|[q]$ and $e(\theta,\psi)$ in $W[[C_\infty(N)]]_P$ has rank 2 over $\Lambda_{W,P}$, and is a direct summand of $e\cdot W[[C_\infty(N)]]_P$.*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

To prove this claim (C), we use the admissible representation $(e\cdot V_q)\otimes_\Lambda Q$ of $\mathrm{GL}_2(\mathbb{Q}_q)$ defined for the prime to q-part $N^{(q)}$ of N (in place of N) whose detailed description is given just before stating the proposition. Then $e(\theta,\psi)$ generates a principal series representation $\pi_q \subset e\cdot V_q\otimes_{\Lambda_W} Q_W$ isomorphic to $\pi(\theta_q,\widehat{\psi}_q)$ over Q_W, where $\widehat{\psi}_q : \mathbb{Q}_q^\times \to \Lambda^\times$ is the unramified character sending the prime q to $\psi(q)\langle q\rangle$, and θ_q is just the $\theta|_{\mathbb{Q}_q^\times}$ regarding θ as an idele character. Then by the well-known theory of admissible representations if $\kappa(P)$ has characteristic 0 and by Vigneras' modulo p representation theory of admissible representations (see [Vig89, Theorem 3]) if $P|(p)$, an old-new congruence at q occurs only when the ratio $(\widehat{\psi}_q/\theta_q)(q)$ is congruent to $q^{\pm 1}$ modulo P (for the maximal ideal P of $\Lambda_{W,P}$). This cannot happen if P is over (p) because $\langle q\rangle = \zeta t^{\log_p(q)/\log_p(\gamma)}$ for a root of unity ζ and $t^s \equiv (1+T^{p^m})^u = 1+uT^{p^m}+\cdots \bmod p$ if $s=p^m u$ with $u\in\mathbb{Z}_p^\times$.

If $\kappa(P)$ has characteristic 0, regarding $P\in \mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}(\mathbb{I},\overline{\mathbb{Q}}_p)$, we have $P(t)=u$ with $|u-1|_p<1$. Then $P(\widehat{\psi}_q\theta_q^{-1}(q)-q^{\pm 1}) = \psi\theta^{-1}(q)u^{\log_p(q)/\log_p(\gamma)}-q^{\pm 1}=0$ implies $u=\gamma^{\pm 1}\zeta$ for $\zeta\in\mu_{p^\infty}(\overline{\mathbb{Q}}_p)$. We have $P=(t-\gamma^{\pm 1}\zeta)$; so, $\psi\theta^{-1}\omega^{\mp 1}(q)q^{\pm 1}\zeta' - q^{\pm 1}=0$ for another p-power root of unity ζ'; hence, $\mu_{p^\infty}\ni\zeta'=\theta\psi^{-1}\omega^{\pm 1}(q)$. Since $P\nmid(\langle q\rangle(T)-\theta\psi^{-1}\omega(l)q^{-1})$ (which is a factor of $\mathbb{L}_{N,\chi_1}$), we find that $P=(t-\zeta'\gamma)$. Since P is now an arithmetic prime of weight 2 and N is cube-free, we know that $\mathbf{H}$ and $\mathbf{H}_{2,\varepsilon}$ are reduced algebras by [Hid13a, Corollaries 1.2 and 1.3] (in [Hid13a], only the cuspidal Hecke algebra is dealt with, but the proof is the same for $\mathbf{H}$). Thus $\mathbf{H}_P$ is an algebra direct sum of the Eisenstein part and the cuspidal part; so, the exact sequence has to split.

Thus hereafter, we may assume that $(\widehat{\psi}_q/\theta_q)(q)\not\equiv q^{\pm 1} \bmod P$. By the well-known theory of admissible representations if $\kappa(P)$ has characteristic 0 and by Vigneras' modulo p representation theory of admissible representations (see [Vig89, Theorem 3]) if $P|(p)$, $\pi(\theta_q,\widehat{\psi}_q) \bmod P\Lambda_{W,P}$ is irreducible. The vectors $e(\theta,\psi)$ and $e(\theta,\psi)|[q]$ modulo $P\Lambda_{W,P}$ in the irreducible $\overline{\pi}_q := (\pi_q \bmod P\Lambda_{W,P})$ are linearly independent. This shows the above claim (C).

To make a section, first assume that q is prime to N/q. Letting (θ_1,ψ) be the pair with θ_1 which is θ regarded as a character modulo M_1q, we have $e(\theta_1,\psi)=e(\theta,\psi)-\theta_q(q)e(\theta,\psi)|[q]$ up to units in $\Lambda_{W,P}$ by the argument in the previous section. Similarly $e(\theta,\psi_1)=e(\theta,\psi)-\widehat{\psi}_q(q)e(\theta,\psi)|[q]$ for ψ_1 which is ψ regarded as a character modulo M_1q. Then

$$\mathrm{Res}(E(\theta_1,\psi)) = \mathrm{Res}(E(\theta,\psi)-\theta_q(q)E(\theta,\psi)|[q]) = \mathrm{Res}(E(\theta,\psi))-\theta_q(q)\mathrm{Res}(E(\theta,\psi))|[q],$$
$$\mathrm{Res}(E(\theta,\psi_1)) = \mathrm{Res}(E(\theta,\psi)-\widehat{\psi}_q(q)E(\theta,\psi)|[q]) = \mathrm{Res}(E(\theta,\psi))-\widehat{\psi}_q(q)\mathrm{Res}(E(\theta,\psi))|[q].$$

Thus the section of level N/q extends to the level N.

Note that N is cube-free. Thus the remaining case is when $q^2|N$. If $\mathfrak{C}(\theta)$ and $\mathfrak{C}(\psi)$ are both prime to q, by the irreducibility of $\overline{\pi}_q$, $e(\theta,\psi), e(\theta,\psi)|[q]$ and $e(\theta,\psi)|[q]^2$ span a three-dimensional subspace in $\overline{\pi}_q$. Thus we have $e(\theta_1,\psi_1)=e(\theta,\psi_1)-\theta(q)e(\theta,\psi_1)$ which does not vanish in $\overline{\pi}_q$. Then $e(\theta_1,\psi_1)\mapsto E(\theta_1,\psi_1)$ gives a section on (θ_1,ψ_1)-eigenspace. If $q|\mathfrak{C}(\theta)$ but $q\nmid\mathfrak{C}(\psi)$, we define $e(\theta_1,\psi)=e(\theta,\psi_1)-\theta(q)e(\theta,\psi_1)$, and if $q\nmid\mathfrak{C}(\theta)$ but $q|\mathfrak{C}(\psi)$, $e(\theta,\psi_1)=e(\theta,\psi_1)-\widehat{\psi}(q)e(\theta,\psi_1)$, and the same argument works well. If $q|\mathfrak{C}(\theta)$ and $q|\mathfrak{C}(\psi)$ but one of the characters is imprimitive at another prime q', we apply our argument to q' in place of q, and we get the section. The case where $N|\mathfrak{C}(\theta)\mathfrak{C}(\psi)$ is covered by Ohta's result that is explained at the beginning of the proof. □

Let $\mathbf{E}$ be the image of $\mathbf{H}$ in $\mathrm{End}_\Lambda(\mathcal{E}(N,\chi_1;\Lambda_W))$ and define $\mathcal{C}_{\mathbf{E}}=\mathbf{h}\otimes_{\mathbf{H}}\mathbf{E}\cong(\mathbf{h}\oplus\mathbf{E})/\mathbf{H}$ (the Eisenstein congruence module). As long as $p\nmid\varphi(N)$ and $\overline{\theta}$ ramifies at p, $\rho_{\mathfrak{m}}\cong\overline{\theta}\oplus\overline{\psi}$ and (M_1,M_2) determine a unique maximal ideal $\mathfrak{m}=\mathfrak{m}(\overline{\theta},\overline{\psi};M_1,M_2)$ of $\mathbf{H}$ (and $\mathbf{E}$). Since $(\overline{\theta},\overline{\psi};M_1,M_2)$ determines $(\theta,\psi;M_1,M_2)$ uniquely, we have $\mathbf{E}_{\mathfrak{m}}=\Lambda_W$ (as $(\overline{\theta},\overline{\psi})$ determines (θ,ψ) by $p\nmid\varphi(N)$).

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

Corollary 4.3. *If $p \nmid 6\varphi(N)$, N is cube-free and $\overline{\theta}$ ramifies at p, then we have* $\mathrm{Char}_{\Lambda_W}(\mathcal{C}_{\mathfrak{m}}) = (A(T;\theta,\psi))$ *in Λ_W for the localization $\mathcal{C}_{\mathbf{E}_{\mathfrak{m}}}$ of $\mathcal{C}_{\mathbf{E}}$ at $\mathfrak{m} = \mathfrak{m}(\overline{\theta},\overline{\psi};M_1,M_2)$, where $A(T;\theta,\psi)$ is defined for θ_1 mod M_1p and ψ mod M_2.*

Proof. We have a pairing $\mathbf{H} \times \mathcal{M}(N,\chi_1;\Lambda_W)$ given by $(h,f) = a(1, f \mid h)$. If we define

$$\widetilde{\mathcal{M}}(N,\chi_1;\Lambda_W) = \{f \in \mathcal{M}(N,\chi_1;Q_W) \mid a(n,f) \in \Lambda_W \text{ for all } n > 0\}$$

then, as is well known (see [Hid86a, § 2]), this pairing $\mathbf{H} \times \widetilde{\mathcal{M}}(N,\chi_1;\Lambda_W)$ is perfect; i.e. as Λ_W-modules, $\mathrm{Hom}_{\Lambda_W}(\mathbf{H},\Lambda_W) \cong \widetilde{\mathcal{M}}(N,\chi_1;\Lambda_W)$ and $\mathrm{Hom}_{\Lambda_W}(\widetilde{\mathcal{M}}(N,\chi_1;\Lambda_W),\Lambda_W) \cong \mathbf{H}$ by sending the linear form: $\sum_n a(n,F)q^n \mapsto a(n,F)$ (indexed by n) to the Hecke operator $T(n)$. However, by definition, $\widetilde{\mathcal{M}}(N,\chi_1;\Lambda_W)/\mathcal{M}(N,\chi_1;\Lambda_W) \hookrightarrow Q_W/\Lambda_W$ by $f \mapsto a(0,f)$, and the inclusion $f \mapsto a(0,f)$ is Γ-equivariant. The group Γ acts on the constant term by the character: $\Gamma \ni z \mapsto z^{-1} \in W^\times$ (as by our choice of the action, weight 1 corresponds to the trivial action). This shows that after inverting $T' = t - \gamma^{-1}$, the pairing is perfect between $\mathcal{M}(N,\chi_1;A)$ and $\mathbf{H} \otimes_{\Lambda_W} A$ over the principal ideal domain $A := \Lambda_W[1/T'\varphi(N)]$. The Λ_W-perfectness of the pairing on $\mathbf{h} \times \mathcal{S}(N,\chi_1;\Lambda_W)$ holds in the same way as in the case of $\mathbf{H}$ without inverting T (or $\varphi(N)$). We have an integral $\mathbf{H}$-linear map $I : e \cdot W[[C_\infty]][\chi_1] \to \mathcal{M}(N,\chi_1;\Lambda_W)$ given by $I(e(\theta,\psi)) = E(\theta,\psi)$ if (θ,ψ) is not induced by $(\omega^{-1},\mathbf{1}_1)$ and $I(e(\theta,\psi)) = T'E(\theta,\psi)$ otherwise. Let $\mathfrak{m} = \mathfrak{m}(\theta,\psi;M_1,M_2)$, regard it as a maximal ideal of $\mathbf{H}$, and assume $\theta\psi^{-1}(p) \neq 1$. By [Oht03, Lemma 1.4.9], the multiplicity of the Hecke eigenvalues of $E(\theta,\psi)$ is equal to 1 even modulo $\mathfrak{m}_\Lambda$. Thus after localization at $\mathfrak{m}$,

$$W[[C_\infty]]_{\mathfrak{m}}\left[\frac{1}{\varphi(N)}\right] \cong W[[T]]\left[\frac{1}{\varphi(N)}\right]e(\theta,\psi) \cong \mathbf{E}_{\mathfrak{m}}\left[\frac{1}{\varphi(N)}\right]$$

as $\mathbf{H}_{\mathfrak{m}}$-modules. Then we have

$$\mathrm{Res} \circ I\left(e \cdot W[[C_\infty]]_{\mathfrak{m}}\left[\frac{1}{\varphi(N)}\right]\right) \cong \frac{W[[T]][1/\varphi(N)]}{A(T;\theta,\psi)W[[T]][1/\varphi(N)]}e(\theta,\psi) =: C_{\mathbf{E}_{\mathfrak{m}}}.$$

Putting $\mathcal{S} = \mathcal{S}(N,\chi_1;Q_W) \cap \mathcal{M}(N,\chi_1;A)$ and $\mathcal{E} = \mathcal{E}(N,\chi_1;Q_W) \cap \mathcal{M}(N,\chi_1;A)$ in $\mathcal{M}(N,\chi_1;Q_W)$, we have the following exact sequence of $\mathbf{H}_{\mathfrak{m}}$-modules,

$$0 \to \mathcal{E}_{\mathfrak{m}} \oplus \mathcal{S}_{\mathfrak{m}} \to \mathcal{M}(N,\chi_1;\Lambda_W)_{\mathfrak{m}} \to C \to 0 \quad \text{with } C \cong C_{\mathbf{E}_{\mathfrak{m}}} \text{ as } \mathbf{H}_{\mathfrak{m}}\text{-modules.} \tag{4.5}$$

Defining an A-dual module M^* by $M^* = \mathrm{Hom}_A(M,Q_W/A)$ for any torsion A–module M of finite type, we have $M \cong M^*$ (non-canonically) as A-modules, by the following lemma applied to the principal ideal domain A. Noting that $\mathbf{H}_{\mathfrak{m}} \otimes_{\Lambda_W} A$ (respectively $(\mathbf{h}_{\mathfrak{m}} \oplus \mathbf{E}_{\mathfrak{m}}) \otimes_{\Lambda_W} A$) is the A-dual of $\mathcal{M}(N,\chi_1;A)_{\mathfrak{m}}$ (respectively $\mathcal{S}_{\mathfrak{m}} \oplus \mathcal{E}_{\mathfrak{m}}$) and again applying the following lemma to the exact sequence (4.5) tensored A over Λ_W, we have an $\mathbf{H}_{\mathfrak{m}}$-linear isomorphism $(C_{\mathbf{E}_{\mathfrak{m}}})^* \cong \mathcal{C}_{\mathbf{E}_{\mathfrak{m}}} \otimes_{\Lambda_W} A$; so, we get $\mathrm{Char}_{\Lambda_W}(\mathcal{C}_{\mathbf{E}_{\mathfrak{m}}}) = \mathrm{Char}_{\Lambda_W}(C_{\mathbf{E}_{\mathfrak{m}}}) = (A(T;\theta,\psi))$ in A. Since non-divisibility $T' \nmid \mathrm{Char}_{\Lambda_W}(C_{\mathbf{E}_{\mathfrak{m}}})\,\mathrm{Char}_{\Lambda_W}(\mathcal{C}_{\mathbf{E}_{\mathfrak{m}}})$ is known, we have $\mathrm{Char}_{\Lambda_W}(\mathcal{C}_{\mathbf{E}_{\mathfrak{m}}}) = \mathrm{Char}_{\Lambda_W}(C_{\mathbf{E}_{\mathfrak{m}}}) = (A(T;\theta,\psi))$ in Λ_W as desired if $p \nmid \varphi(N)$. □

Lemma 4.4. *Let A be a principal ideal domain with quotient field K. For each A-module M, we define $M^* = \mathrm{Hom}_A(M,K/A)$ and $M^\vee = \mathrm{Hom}_A(M,A)$. For an exact sequence $0 \to M \to N \to T \to 0$ of A-free modules M and N of finite rank with A-torsion quotient T, we have a canonical exact sequence of A-modules $0 \to N^\vee \to M^\vee \to T^* \to 0$ and an isomorphism $T^* \cong T$ as A-modules.*

Proof. Since A is a principal ideal domain, we have the following facts:

(1) $M \mapsto M^*$ is a perfect duality with $M \cong (M^*)^*$ canonically for A-modules of finite type;
(2) if an A-module T is torsion of finite type, $T \cong T^*$ as A-modules non-canonically;
(3) if an A-module T is torsion of finite type, $\mathrm{Ext}^1_A(K/A, T) \cong T$.

By perfect duality, we have an exact sequence $0 \to L^* \to N^* \to T^* \to 0$ of A-modules. Applying the covariant functor $X \mapsto \mathrm{Hom}_A(K/A, X)$ to this exact sequence and noting isomorphisms

$$\mathrm{Hom}_A(K/A, M^*) \cong \mathrm{Hom}_A(K/A, \mathrm{Hom}_A(M, K/A)) \cong \mathrm{Hom}_A(M \otimes_A K/A, K/A) \cong M^\vee$$

and $\mathrm{Ext}^1_A(K/A, T^*) \cong T^*$, we get the exact sequence $0 \to N^\vee \to M^\vee \to T^* \to 0$. □

5. CM components

We study when a CM component of $\mathrm{Spec}(\mathbf{h})$ is a Gorenstein ring. The result is used to determine the characteristic ideal of the congruence module of the CM component and other non-CM components. The characteristic ideal is expected to give the level of non-CM components in the connected component containing the CM component. We first quote the following fact from [Hid13a, § 3] (or [Hid11b, (CM1–3) in § 1]).

Proposition 5.1. *Let* $\mathrm{Spec}(\mathbb{J})$ *be a reduced irreducible component of* $\mathrm{Spec}(\mathbf{h})$ *as in the introduction. Write* $\widetilde{\mathbb{J}}$ *for the integral closure of* $\mathbb{J}$ *in its quotient field. The following five conditions are equivalent:*

(CM1) *$\mathcal{F}$ is a CM family with $\rho_{\mathbb{J}} \cong \rho_{\mathbb{J}} \otimes \left(\frac{M/\mathbb{Q}}{}\right)$ for a quadratic field M with discriminant D;*
(CM2) *the prime p splits in M, and we have $\rho_{\mathbb{J}} \cong \mathrm{Ind}^{\mathbb{Q}}_M \Psi_{\mathbb{J}}$ for a character $\Psi_{\mathbb{J}} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \widetilde{\mathbb{J}}^\times$ with prime-to-p conductor $\mathfrak{C} = \mathfrak{C}(\Psi_{\mathbb{J}})$ unramified outside $\mathfrak{C}\mathfrak{p}$; we have $D \cdot N(\mathfrak{C})|N$;*
(CM3) *for all arithmetic points P of $\mathrm{Spec}(\mathbb{J})(\overline{\mathbb{Q}}_p)$, f_P is a binary Hecke eigen theta series of the norm form of an imaginary quadratic extension $M/\mathbb{Q}$ with prime-to-p conductor $N(\mathfrak{C})D$;*
(CM4) *for some arithmetic point P of $\mathrm{Spec}(\mathbb{J})(\overline{\mathbb{Q}}_p)$, f_P is a binary Hecke eigen theta series of the norm form of an imaginary quadratic extension $M/\mathbb{Q}$ with prime-to-p conductor $N(\mathfrak{C})D$;*
(CM5) *for some arithmetic prime P, ρ_P is an induced representation of a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ with prime-to-p conductor $\mathfrak{C}$, where M is a quadratic extension of $\mathbb{Q}$.*

A binary Hecke eigen theta series of the norm form of an imaginary M is called a *CM theta series.*

See § 10 for a description of the prime-to-p conductor of Galois representations. We write $\mathfrak{C}(\xi)$ (respectively $C(\rho)$) for the prime-to-p conductor of a Galois character ξ (respectively a two-dimensional Galois representation ρ). We say a Hecke eigenform f has conductor $C(f)$ if the automorphic representation generated by f has conductor $C(f)$; so, f itself could be an old form. Recall that the prime-to-p part C of this conductor $C(f)$ is equal to the prime-to-p conductor $C(\rho_f)$ of the p-adic Galois representation associated to f. We say that $\mathbb{J}$ has CM (or is a CM component) by M if one of the above equivalent conditions is satisfied by an imaginary quadratic field M. In the rest of this section, we fix a CM component $\mathbb{J}$ of $\mathbf{h}$ having CM by an imaginary quadratic field M. For $\Psi_{\mathbb{J}}$ as in (CM2) and a complex conjugation $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we put

$$\begin{gathered}\overline{\psi} = (\Psi_{\mathbb{J}} \bmod \mathfrak{m}_{\mathbb{J}}), \quad \overline{\psi}^c(\sigma) = \overline{\psi}(c\sigma c^{-1}), \quad \overline{\psi}^- = \overline{\psi}/\overline{\psi}^c, \\ C = C(\rho_{\mathbb{J}}) = C(\mathrm{Ind}^{\mathbb{Q}}_M \Psi_{\mathbb{J}}) = N(\mathfrak{C}(\Psi_{\mathbb{J}}))D, \quad \mathfrak{C} = \mathfrak{C}(\Psi_{\mathbb{J}}), \quad \mathfrak{c} = \mathfrak{C}(\overline{\psi}^-), \quad \mathfrak{c}' = \mathfrak{C} \cap \overline{\mathfrak{C}}\end{gathered} \tag{5.1}$$

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

for $\overline{\mathfrak{C}} = \mathfrak{C}^c$, where $N(\mathfrak{a})$ is the norm of a fractional ideal $\mathfrak{a}$ of M and $C(\Psi_{\mathbb{J}})$ is the prime-to-p conductor. Then $\mathfrak{c} = \overline{\mathfrak{c}}$, and $\mathfrak{c}$ is a factor of $\mathfrak{c}'$ but may not be equal to $\mathfrak{c}'$.

Let $\mathrm{Spec}(\mathbf{h}^M_{\mathrm{cm}})$ be the minimal closed subscheme of $\mathrm{Spec}(\mathbf{h})$ containing all reduced irreducible components having CM by a fixed imaginary quadratic field M. We take the connected component $\mathrm{Spec}(\mathbb{T})$ of $\mathrm{Spec}(\mathbf{h})$ containing $\mathrm{Spec}(\mathbb{J})$. Let $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ be the union of all reduced CM components inside $\mathrm{Spec}(\mathbb{T})$. Note that $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ could contain components having CM by different imaginary quadratic fields. We would like to know when $\mathbb{T}_{\mathrm{cm}}$ is a Gorenstein ring or more strongly a local complete intersection. This can be answered by proving $\mathbb{T}_{\mathrm{cm}}$ is isomorphic to the continuous group algebra $W[[Z_p]]$ for an appropriate ray class group Z_p of M (see Lemma 5.5). Such an identification could fail if either $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ intersects with $\mathrm{Spec}(\mathbf{h}^M_{\mathrm{cm}})$ and $\mathrm{Spec}(\mathbf{h}^K_{\mathrm{cm}})$ for different fields K and M or $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ contains a union of two copies of $\mathrm{Spec}(W[[Z_p]])$; i.e. new and old (or old and old) CM components coming from a primitive CM component. Here the word 'primitive' is used in the sense of [Hid86a, p. 252 in § 3]. Thus we look for sufficient conditions to preclude these bad cases in terms of level and the prime-to-p conductor of $\overline{\rho}$. We start with a result that is simple but crucial for the Gorenstein-ness of the CM local ring given in Proposition 5.7.

Proposition 5.2. *Let A be a p-profinite local integral domain for $p > 2$. Let M and K be two distinct quadratic fields in $\overline{\mathbb{Q}}$. Suppose that we have continuous characters $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to A^\times$ and $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to A^\times$ with absolutely irreducible $\mathrm{Ind}^{\mathbb{Q}}_M \varphi$ over $Q(A)$ such that $\mathrm{Ind}^{\mathbb{Q}}_M \varphi \cong \mathrm{Ind}^{\mathbb{Q}}_K \phi$. Write φ^σ for the character $\mathrm{Gal}(\overline{\mathbb{Q}}/M) \ni \tau \mapsto \varphi(\sigma\tau\sigma^{-1})$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ inducing the generator of $\mathrm{Gal}(M/\mathbb{Q})$. If the representations $\mathrm{Ind}^{\mathbb{Q}}_M \varphi \cong \mathrm{Ind}^{\mathbb{Q}}_K \phi$ are ordinary at p, then we have:*

1. *φ and ϕ are both of finite order;*
2. *we have $\varphi^\sigma = (\frac{MK/M}{})\varphi$; so, φ^- given by $\varphi(\varphi^\sigma)^{-1} =: \varphi^{1-\sigma}$ is equal to $(\frac{MK/M}{})$;*
3. *if p does not ramify in $MK/\mathbb{Q}$, φ and ϕ are both unramified at p;*
4. *if φ ramifies at a prime factor of p, then p splits in M, φ is unramified at another prime factor of p, p ramifies in K and ϕ is unramified at p;*
5. *if K is real and $\mathrm{Ind}^{\mathbb{Q}}_M \varphi$ is odd, M is imaginary and ϕ ramifies at exactly one real place.*

Conversely, if φ^- has order 2 and M is imaginary, we have two quadratic fields K, K' distinct from M with $KM = K'M$ and finite order characters ϕ, ϕ' such that $\mathrm{Ind}^{\mathbb{Q}}_M \varphi \cong \mathrm{Ind}^{\mathbb{Q}}_K \phi \cong \mathrm{Ind}^{\mathbb{Q}}_{K'} \phi'$.

Here the word 'ordinary' means that the representation restricted to a decomposition group at p is isomorphic to an upper triangular representation with an unramified one-dimensional quotient. In our case, the restriction of, say, $\mathrm{Ind}^{\mathbb{Q}}_M \varphi$ to a decomposition group at p is the direct sum $\varphi \oplus \varphi^\sigma$ (for σ as in (2)) or $\mathbf{1} \oplus (\frac{M/\mathbb{Q}}{})$ for the identity character $\mathbf{1}$. Then ordinarity implies that φ is at least unramified at one prime in M over p.

Proof. Suppose $\mathrm{Ind}^{\mathbb{Q}}_M \varphi \cong \mathrm{Ind}^{\mathbb{Q}}_K \phi$. We first prove assertion (2). Let N be the prime-to-p Artin conductor of $\mathrm{Ind}^{\mathbb{Q}}_M \varphi$. For any prime l outside Np inert in K and split in M (such primes have positive density), we have

$$0 = \mathrm{Tr}(\mathrm{Ind}^{\mathbb{Q}}_K \phi(\mathrm{Frob}_l)) = \mathrm{Tr}(\mathrm{Ind}^{\mathbb{Q}}_M \varphi(\mathrm{Frob}_l)) = \varphi(\mathfrak{l}) + \varphi(\mathfrak{l}^\sigma)$$

for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ inducing a generator of $\mathrm{Gal}(M/\mathbb{Q})$. Thus we have $\varphi^-(\mathrm{Frob}_l) = -1$ if l is inert in K and split in M (note here that $-1 \neq 1$ because $p > 2$). For any other primes q outside Np inert in K and split in M, $\varphi^-(\mathrm{Frob}_l) = -1 = \varphi^-(\mathrm{Frob}_q)$. Since $\mathrm{Frob}_l\mathrm{Frob}_q^{-1}$ fix MK, by moving q, Chebotarev density tells us that φ^- factors through $\mathrm{Gal}(MK/M)$. Since $\mathrm{Ind}^{\mathbb{Q}}_M \varphi$ is

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

absolutely irreducible, we have $\varphi \neq \varphi^\sigma$ (i.e. $\varphi^- \neq 1$). Thus we conclude $\varphi = (\frac{MK/M}{})\varphi^\sigma$. This proves (2).

We now deal with assertions (3) and (4). By the remark preceding this proof, we may assume that φ is unramified at one prime factor $\mathfrak{p}^\sigma$ of p. If there is only one prime factor in M over p, this forces φ^σ to be unramified at p. If there are two factors of p in M, either φ is also unramified at $\mathfrak{p}$ or K ramifies at p by (2). If K ramifies at p, there is only one prime factor in K over p, this forces ϕ to be unramified at p. Thus if $MK/\mathbb{Q}$ is unramified at p, $(\frac{MK/M}{})$ is unramified at p, and φ and ϕ are both unramified at p. This proves (3) and (4).

To show (1), first suppose that φ ramifies at a prime factor $\mathfrak{p}|p$. Thus p ramifies in K and splits in M. Then $(\frac{MK/M}{})$ ramifies at two primes $\mathfrak{p}$ and $\mathfrak{p}^\sigma$, and therefore φ has to be unramified at $\mathfrak{p}^\sigma$. In short, φ ramifies at $\mathfrak{p}$ and is unramified at $\mathfrak{p}^\sigma$. Since p ramifies in K, ordinarity of $\mathrm{Ind}_K^{\mathbb{Q}}\phi$ forces ϕ to be unramified at p; so, ϕ factors through a finite ray class group $Cl_K(\mathfrak{f}')$ for an ideal $\mathfrak{f}'$ prime to p. Thus $\mathrm{Ind}_M^{\mathbb{Q}}\varphi \cong \mathrm{Ind}_K^{\mathbb{Q}}\phi$ has finite image; so, φ has finite order.

Next suppose that φ is unramified at p. Then φ factors through the finite ray class group $Cl_M(\mathfrak{f})$ of M modulo $\mathfrak{f}$ for the prime-to-p conductor $\mathfrak{f}$ of φ. Now $\mathrm{Ind}_M^{\mathbb{Q}}\varphi$ has finite image, and we conclude that ϕ is of finite order (this proves (1)).

To prove (5), now assume that M is imaginary and write $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for complex conjugation. Since $\mathrm{Ind}_M^{\mathbb{Q}}\varphi$ is automatically odd (as M is imaginary), we have $\mathrm{Tr}(\mathrm{Ind}_M^{\mathbb{Q}}\varphi(c)) = 0$. Regard ϕ as an idele character of $K_{\mathbb{A}}^\times$. Then

$$0 = \mathrm{Tr}(\mathrm{Ind}_M^{\mathbb{Q}}\varphi(c)) = \mathrm{Tr}(\mathrm{Ind}_K^{\mathbb{Q}}\phi(c)) = \begin{cases} \phi(-1_\infty) + \phi(-1_{\infty'}) & \text{if } K \text{ is real,} \\ 0 & \text{otherwise,} \end{cases}$$

where ∞ is an infinite place of K and ∞' is the other, and $1_{\infty'}$ is the identity of the ∞'-component $K_{\infty'}^\times = \mathbb{R} \subset K_{\mathbb{A}}^\times$. Thus ϕ ramifies at exactly one infinite place of K if K is real. Since $\mathrm{Ind}_M^{\mathbb{Q}}\varphi$ is odd, we see that ϕ ramifies at exactly one infinite place of K if K is real. If M and K are both real, $\varphi^\sigma/\varphi = (\frac{MK/M}{})$ is unramified at the two infinite places; so, either φ ramifies at the two infinite places or is unramified at the two infinite places; so, this is impossible (finishing the proof of (5)).

Suppose now that φ^- has order 2 and that M is imaginary, to prove the converse. Then the splitting field of φ^- is a quadratic extension L/M. Since $(\varphi^-)^\sigma = (\varphi^-)^{-1} = \varphi^-$, $L^\sigma = L$; so, $L/\mathbb{Q}$ is an abelian extension of degree 4. This also shows that $\mathrm{Ind}_M^{\mathbb{Q}}\varphi^-$ is reducible: $\mathrm{Ind}_M^{\mathbb{Q}}\varphi^- = \eta \oplus \xi$ for two characters $\eta, \xi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\eta/\xi = (\frac{M/\mathbb{Q}}{})$. Since M is imaginary, for any complex conjugation c, $\eta(c) = ((M/\mathbb{Q})/c)\xi(c) = -\xi(c)$. Since $\xi(c)$ and $\eta(c)$ are ± 1, we conclude one of them is -1, say, $\eta(c) = -1$. If one of ξ and η has order 4, the other also has order 4. Since $\xi^2 = \eta^2$ is an even character, its splitting field $K \subset L$ is a real quadratic field; so, $M \neq K$ and $L = MK$, a contradiction (as $\mathrm{Gal}(L/\mathbb{Q})$ has to be cyclic of order 4). Thus L is not a cyclic extension; so, again it is a composite of two distinct quadratic fields M and K. Thus ξ and η have order 2. Write $\rho := \mathrm{Ind}_M^{\mathbb{Q}}\varphi$. As is well known, we have $\mathrm{Ad}(\rho) \cong \mathrm{Ind}_M^{\mathbb{Q}}\varphi^- \oplus (\frac{M/\mathbb{Q}}{})$ and $\mathrm{End}_{Q(A)}(\rho) \cong \mathrm{Ad}(\rho) \oplus \mathbf{1} \cong \eta \oplus \xi \oplus (\frac{M/\mathbb{Q}}{}) \oplus \mathbf{1}$ for the trivial representation $\mathbf{1}$. Therefore we find $\rho \otimes \xi \cong \rho$ and $\rho \otimes \eta \cong \eta$. Thus for the fixed field $K_?$ of Ker(?) for $? = \xi, \eta$, we have $L = MK_\eta = K_\eta K_\xi = K_\xi M$, and there exist characters $\phi_? : \mathrm{Gal}(\overline{\mathbb{Q}}/K_?) \to Q(A)^\times$ such that $\rho \cong \mathrm{Ind}_{K_\eta}^{\mathbb{Q}}\phi_\eta \cong \mathrm{Ind}_{K_\xi}^{\mathbb{Q}}\phi_\xi$ (e.g. [Hid00, Lemma 2.15]). Then by (1), $\phi_?$ has finite order, and we take $K = K_\eta$ (respectively $K' = K_\xi$) and $\phi = \phi_\eta$ (respectively $\phi' = \phi_\xi$). □

Corollary 5.3. *Suppose $p > 2$. Let M and K be distinct imaginary quadratic fields in which p splits. If $P \in \mathrm{Spec}(\mathbf{h}_{\mathrm{cm}}^M) \cap \mathrm{Spec}(\mathbf{h}_{\mathrm{cm}}^K)$ is a prime divisor, we have $P \cap \mathbb{Z}_p[[T]] = (T)$.*

Proof. Since ρ_P has to be induced from M and K, we have $\mathrm{Ind}_M^{\mathbb{Q}}\varphi \cong \mathrm{Ind}_K^{\mathbb{Q}}\phi$. Since p has to be split both in K and M, ϕ and φ are unramified at p by Proposition 5.2(3), and by (Gal), regarding $[\gamma, \mathbb{Q}_p] \in I_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/M)$, we have $t = \varphi([\gamma, \mathbb{Q}_p]) = 1$; so, $T = 0$ in $\mathbf{h}/P$; i.e. $T \in P$. □

Let $\mathbb{T}_P$ be the localization of $\mathbb{T}$ at a prime divisor $P \in \mathrm{Spec}(\mathbb{T})$ and write $\rho_{\mathbb{T}_P}$ for $\rho_{\mathfrak{a}}$ for $\mathfrak{a} = \mathrm{Ker}(\mathbb{T} \to \mathbb{T}_P^{\mathrm{red}})$. Let $u(q)$ for primes $q|Np$ be the image of $U(q)$ in $\mathbb{T}_P$. Similarly, we write $a(l) \in \mathbb{J}$ for the image of $T(l)$ or $U(l)$ in $\mathbb{J}$. We have $\boldsymbol{\kappa} := \det(\rho_{\mathbb{T}_P}) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to W[[T]]$. By [Hid11a, Proposition 4.3.1], we have $\det(\rho_{\mathbb{T}_P})([u, \mathbb{Q}]) = \chi_1(u)t^{\log_p(u_p)/\log_p(\gamma)}$ for $u \in \widehat{\mathbb{Z}}^\times$. Consider the projection $\langle\cdot\rangle : \mathrm{Im}(\det(\rho_{\mathbb{T}_P})) \twoheadrightarrow \mathrm{Im}(\det(\rho_{\mathbb{T}_P}))_p$ for the maximal p-profinite subgroup $\mathrm{Im}(\det(\rho_{\mathbb{T}_P}))_p$ of $\mathrm{Im}(\det(\rho_{\mathbb{T}_P}))$, and put $\langle\boldsymbol{\kappa}\rangle = \langle\cdot\rangle \circ \boldsymbol{\kappa}$; so, $\boldsymbol{\kappa} = \chi_1\langle\boldsymbol{\kappa}\rangle$. We define $\rho'_{\mathbb{T}_P} = \rho_{\mathbb{T}_P} \otimes \sqrt{\langle\boldsymbol{\kappa}\rangle}^{-1}$, where the square root is supposed to have values in the p-profinite part $\mathrm{Im}(\det(\rho_{\mathbb{T}_P}))_p$. Note that $\sqrt{\langle\boldsymbol{\kappa}\rangle}$ has values in $W[[T]]^\times$ and that $\rho'_{\mathbb{T}_P}$ has values in $\mathrm{GL}_2(\mathbb{T}_P)$, since $p > 2$.

Lemma 5.4. *Let the notation be as above (in particular, P is a prime divisor of $\mathbb{T}$). Suppose $p > 2$. Put $\chi^{(p)} = \chi|_{(\mathbb{Z}/N\mathbb{Z})^\times}$ for the prime-to-p part of χ. Assume that W is a sufficiently large valuation ring finite flat over $\mathbb{Z}_p$. Let $\mathbb{T}'_P$ be the subring of $\mathbb{T}_P$ generated by $\{\mathrm{Tr}(\rho_{\mathbb{T}_P}(\sigma))\}_{\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ over $W[[T]]_P$. Then $\mathbb{T}'_P$ is generated by $\{\mathrm{Tr}(\rho'_{\mathbb{T}_P}(\sigma))\}_{\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ over $W[[T]]_P$. Further suppose that the prime-to-p conductor of $\rho_{\mathbb{T}_P}$ coincides with the prime-to-p conductor $C(\rho_P)$ of ρ_P. If $N = C(\rho_P)$, we have:*

1. *$\mathbb{T}_P$ is reduced, and if $C(\overline{\rho}) = N$, $\mathbb{T}$ is reduced;*
2. *the total quotient rings $Q(\mathbb{T}_P)$ and $Q(\mathbb{T}'_P)$ coincide;*
3. *if $\kappa(P)$ has characteristic 0 or $p \nmid \varphi(N)$, $\mathbb{T}_P = \mathbb{T}'_P[u(p)]$ under absolute irreducibility of ρ_P;*
4. *if ρ_P is absolute irreducible, we have $\mathbb{T}_P = \mathbb{T}'_P$ under one of the following conditions:*
   - (a) *$\kappa(P)$ has characteristic 0 and $u(p)^2 \not\equiv \chi^{(p)}(p) \bmod P$;*
   - (b) *$\kappa(P)$ has characteristic 0 and $T \notin P$;*
   - (c) *$\chi_1|_{\mathbb{Z}_p^\times}$ is non-trivial.*

Later we compute the congruence module of a CM component of the ring $\mathbb{T}'$ in terms of anticyclotomic Katz p-adic L-functions. The relation between $\mathbb{T}$ and $\mathbb{T}'$ is clarified by this lemma.

Proof. For a continuous representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R)$ with a p-profinite local W-algebra R, let ξ be the unique square root character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $1 + \mathfrak{m}_R$ of the projection of $\det(\rho)$ to $1 + \mathfrak{m}_R$. Let R_t (respectively R'_t) be the subring of R generated topologically over W by the value of $\mathrm{Tr}(\rho)$ (respectively $\mathrm{Tr}(\rho \otimes \xi^{-1})$). The subring R_t contains $2\det(\rho(\sigma)) = \mathrm{Tr}(\rho(\sigma))^2 - \mathrm{Tr}(\rho(\sigma^2))$. Since $p > 2$, we have $\det(\rho(\sigma)) \in R_t$, and thus R_t contains the values of ξ, and hence $R'_t \subset R_t$. Furthermore, if R'_t contains the value of ξ, we have $R'_t \supset R_t$ as $\mathrm{Tr}(\rho \otimes \xi^{-1}) = \xi^{-1}\mathrm{Tr}(\rho)$. Since $W[[T]]$ contains the value of $\sqrt{\langle\boldsymbol{\kappa}\rangle}$, the subrings of $\mathbb{T}_P$ generated over $W[[T]]_P$ by $\{\mathrm{Tr}(\rho_{\mathbb{T}_P}(\sigma))\}_{\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ and $\{\mathrm{Tr}(\rho'_{\mathbb{T}_P}(\sigma))\}_{\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ are the same. This shows that $\mathbb{T}'_P$ is generated by $\{\mathrm{Tr}(\rho'_{\mathbb{T}_P}(\sigma))\}_{\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ over $W[[T]]_P$.

Since the argument proving (1) is identical for $\mathbb{T}$ and $\mathbb{T}_P$, we give here the one for $\mathbb{T}_P$. Since $N = C(\rho_P)|C(\rho_{\mathbb{T}})|N$ by Lemma 10.2(1) and (4), we conclude $C(\rho_P) = C(\rho_{\mathbb{T}}) = N$. For any prime $P' \in \mathrm{Spec}(\mathbb{T}_P)$, $P' \supset P$, and we have $N = C(\rho_P)|C(\rho_{P'})|N$; so, $C(\rho_{P'}) = N$. Since the nilradical of $\mathbb{T}$ comes from q-old forms for $q|N$ (i.e. the nilradical acts faithfully on the space of q-old forms for $q|N$; see [Hid86a, Corollary 3.3]), it has to be trivial. Thus we conclude the assertion (1) for $\mathbb{T}_P$.

We now look into the subring $\mathbb{T}'_P$ of $\mathbb{T}_P$ generated by $\{\mathrm{Tr}(\rho_{\mathbb{T}_P}(\sigma))\}_{\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ over $W[[T]]_P$ more carefully. Since $\mathbb{T}'_P$ contains the value $\mathrm{Tr}(\rho_{\mathbb{T}_P})$ at the l-Frobenius element for all primes $l\nmid Np$, by the Chebotarev density theorem, $\mathrm{Tr}(\rho_{\mathbb{T}_P})$ has values in $\mathbb{T}'_P$. Thus, we have a representation $\widetilde{\rho}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{GL}_2(Q(\mathbb{T}'_P))$ with $\mathrm{Tr}(\widetilde{\rho})=\mathrm{Tr}(\rho_{\mathbb{T}_P})$ by the theory of pseudo representation. The projection of this representation to each simple factor of $Q(\mathbb{T}'_P)$ is absolutely irreducible. Since $u(q)=0$ or a unit in each irreducible component of $\mathrm{Spec}(\mathbb{T})$ (because of [Miy89, Theorem 4.6.17]), we have $u(q)=0$ or a unit in the entire $\mathbb{T}$. Thus, as for (2), (3) and (4), we may assume that $u(q)\in\mathbb{T}^\times$. Under this assumption, for an arithmetic $P'\in\mathrm{Spec}(\mathbb{T})$, $H^0(I_q,\rho_{P'})\cong\kappa(P')$ (cf. [Hid11a, Theorem 4.2.7]). Thus $H_0(I_q,Q(\mathbb{T}'^{\mathrm{red}}))\cong Q(\mathbb{T}'^{\mathrm{red}})$, which implies $H_0(I_q,Q(\mathbb{T}'_P))\cong Q(\mathbb{T}'_P)$. Take an element $\phi_q\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which induces $[q,\mathbb{Q}_q]$ on the maximal abelian extension $\mathbb{Q}_q^{ab}$ of $\mathbb{Q}_q$. Since $u(q)$ is the eigenvalue of $\widetilde{\rho}(\phi_q)$ on $H_0(I_q,Q(\mathbb{T}'_P))\cong Q(\mathbb{T}'_P)$, we have $u(q)\in Q(\mathbb{T}'_P)$. This proves (2).

Hereafter we assume absolute irreducibility of ρ_P. Then we have $\widetilde{\rho}$ with values in $\mathrm{GL}_2(\mathbb{T}'_P)$, and we take a $\mathbb{T}'_P$–free lattice $L(\widetilde{\rho})\subset Q(\mathbb{T}'_P)^2$ stable under $\widetilde{\rho}$. By definition, $\mathbb{T}_P$ is generated over $W[[T]]_P$ by the image $t(l)$ of $T(l)$ for $l\nmid Np$ and the image $u(q)$ of $U(q)$ for $q|Np$. Since $t(l)=\mathrm{Tr}(\rho_{\mathbb{T}_P}(\mathrm{Frob}_l))=\mathrm{Tr}(\widetilde{\rho}(\mathrm{Frob}_l))$, by Chebotarev density, to show (3) and (4), we need to see if $u(q)$ is contained in $\mathbb{T}'_P$. We may assume that $u(q)\in\mathbb{T}_P^\times$; then, under the assumption $N=C(\rho_P)$, we have $H_0(I_q,\rho_{\mathbb{T}_P})$ has rank 1 on which ϕ_q acts by $u(q)$ (e.g. [Hid11a, Theorem 4.2.7 (2–3)]).

Suppose $q\neq p$, and take any arithmetic prime P' of $\mathrm{Spec}(\mathbb{T})$. Then, because of $u(q)\in\mathbb{T}^\times$, the local p-component of the automorphic representation $\pi_{P'}$ generated by $f_{P'}$ is either a Steinberg representation or in the principal series of the form $\pi(\alpha,\beta)$ with β unramified at q. In the Steinberg case, as $u(q)\not\equiv 0 \bmod P'$, χ_1 is unramified at q, and the q divides N exactly once. Then for any other arithmetic point P'' of $\mathrm{Spec}(\mathbb{T})$, $\pi_{P''}$ is Steinberg at q and we have the identity $C_q(\rho_{P''})=q$. We conclude that either the local component of $\pi_{P''}$ at p is Steinberg for all arithmetic $P''\in\mathrm{Spec}(\mathbb{T})$ (Steinberg case) or in principal series for all arithmetic $P''\in\mathrm{Spec}(\mathbb{T})$ (Principal case).

In the Steinberg case, we write $\rho_{\mathbb{T}}|_{D_q}\cong\left(\begin{smallmatrix}\epsilon & *\\ 0 & \delta\end{smallmatrix}\right)$ with $\epsilon/\delta=\mathcal{N}_q$ for the cyclotomic character $\mathcal{N}_q:\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)\to\mathbb{Z}_p^\times$; so, we have $\boldsymbol{\kappa}=\mathcal{N}_q\delta^2$ and $\epsilon/\delta(\phi_q)=q\neq 1$. Let $A:=\widetilde{\rho}(\phi_q)\langle\boldsymbol{\kappa}\rangle^{-1/2}(\phi_q)$. Taking W so that it contains $\sqrt{q}$, the operator A has two distinct eigenvalues $a=\sqrt{q}^{-1}, b=\sqrt{q}$ in $W^\times$. Note that $a\not\equiv b \bmod P$ (by the assumption that either $\kappa(P)$ has characteristic 0 or $p\nmid\varphi(N)$). In the principal case, since $u(q)\neq 0$, we may write $\rho_{\mathbb{T}}|_{D_q}\cong\left(\begin{smallmatrix}\epsilon & 0\\ 0 & \delta\end{smallmatrix}\right)$ with unramified δ, and $\epsilon|_{I_q}=\chi_1$ is non-trivial with conductor $\mathfrak{C}_q(\chi_1)$ dividing N exactly (by Lemma 10.2(2) combined with [Hid11a, Theorem 4.2.7(3)]). Thus we can find $\sigma\in I_q$ such that $\widetilde{\rho}(\sigma)$ has two eigenvalues $a=1,b$ in $W^\times$. Again we may assume $a\not\equiv b \bmod P$ by our assumption. Put $A:=\widetilde{\rho}(\sigma)$ in the principal series case. Write ρ'' for $\widetilde{\rho}\otimes\langle\boldsymbol{\kappa}\rangle^{-1/2}$ in the Steinberg case and for $\widetilde{\rho}$ in the principal case. Now we argue in the two cases (the Steinberg case and the principal series case) at the same time. Take a $\mathbb{T}'_P$-free ρ''-stable $\mathbb{T}'_P$-lattice $L(\rho'')\subset\rho''$. The matrix A acts on $L(\rho'')$ by two distinct eigenvalues a,b in $W^\times$ with $a\not\equiv b \bmod P$. By adding '$[a]$', we indicate the a-eigenspace of the operator A; so, $L(\rho'')[a]\cong\mathbb{T}'_P\cong L(\rho'')[b]$. Then on the a-eigenspace $L(\rho'')[a]\cong\mathbb{T}'_P$, ϕ_q acts by $u(q)\langle\boldsymbol{\kappa}\rangle^{-1/2}(\phi_q)$ in the Steinberg case and by $u(q)$ in the principal series case, and hence $u(q)\in\mathbb{T}'_P$. This shows (3).

It remains to prove (4). By (3), we have $\mathbb{T}_P=\mathbb{T}'_P[u(p)]$. Let $\mathbb{T}'\subset\mathbb{T}'_P$ be the p-profinite ring generated by the trace of $\rho_{\mathbb{T}_P}$ over $W[[T]]$. Now we have $\det(\rho_{\mathbb{T}_P})([p,\mathbb{Q}_p])=\chi^{(p)}(p)\in W\subset\mathbb{T}'$ as $\det(\rho_{\mathbb{T}_P})(\chi^{(p)})^{-1}$ factors through $\mathrm{Gal}(\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q})$ in which $[p,\mathbb{Q}_p]=1$. Thus we have $a:=\mathrm{Tr}(\rho_{\mathbb{T}_P}(\phi_p))=u(p)+u(p)^{-1}\chi^{(p)}(p)\in\mathbb{T}'\subset\mathbb{T}'_P$, and $u(p)$ satisfies $X^2-aX+\chi^{(p)}(p)=0$. We conclude $u(p) \in \mathbb{T}'_P$ if $a^2 - 4\chi^{(p)}(p) = (u(p) - u(p)^{-1}\chi^{(p)}(p))^2$ is non-zero and a square in $\mathbb{T}'_P$. By [Hid11c], $u(p)$ is transcendental over W, and hence $a^2 - 4\chi^{(p)}(p) \neq 0$ always.

First assume $a^2 - 4\chi^{(p)}(p) \not\equiv 0 \bmod P$ and $\kappa(P)$ has characteristic 0. Since $u(p) \in Q(\mathbb{T}'_P)$, $u(p)$ is in the integral closure $\widetilde{\mathbb{T}}'_P$ of $\mathbb{T}'_P$ in $Q(\mathbb{T}'_P)$. Since $\widetilde{\mathbb{T}}'_P/\mathbb{T}'_P$ is a torsion $\mathbb{T}'_P$-module of finite type, the support of $\widetilde{\mathbb{T}}'_P/\mathbb{T}'_P$ in $\mathrm{Spec}(\mathbb{T}'_P)$ is made up of only finitely many closed points. Thus by extending scalars, we may assume that $\widetilde{\mathbb{T}}'_P/\widetilde{P}' = K$ for $K = Q(W)$ for all maximal ideals $\widetilde{P}'$ of $\widetilde{\mathbb{T}}'_P$ in the support of $\widetilde{\mathbb{T}}'_P/\mathbb{T}'_P$. In other words, for any prime $\widetilde{P}' \subset \widetilde{\mathbb{T}}'_P$ over P', $\widetilde{\mathbb{T}}'_P/\widetilde{P}' = \mathbb{T}'_P/P' = K$, and in particular, $\kappa(P) = \kappa(\widetilde{P})$. Let α be the image of $u(p) - u(p)^{-1}\chi^{(p)}(p)$ in $\kappa(P)$. By our assumption, $\alpha \in W \subset \kappa(P)$. Then regard $\alpha \in W \subset \mathbb{T}'$ and consider $\alpha^{-2}(u(p) - u(p)^{-1}\chi^{(p)}(p))^2 = \alpha^{-2}(a^2 - 4\chi^{(p)}(p)) \in \mathbb{T}'$, which is in $1 + (P \cap \mathbb{T}')$. Since $p > 2$, $1 + (P \cap \mathbb{T}')$ is p-profinite, and $(1 + (P \cap \mathbb{T}'))^2 = 1 + (P \cap \mathbb{T}')$. Thus $a^2 - 4\chi^{(p)}(p)$ is a square in $\mathbb{T}'_P$, which implies $u(p) \in \mathbb{T}'_P$.

Now assume that $a^2 - 4\chi^{(p)}(p) \equiv 0 \bmod P$. If $T \notin P$, by (Gal), we find $\sigma \in I_p$ such that the eigenvalue of $\widetilde{\rho}(\sigma)$ is 1 and $z \in W^\times$ with $z \not\equiv 1 \bmod P$. Then if W is sufficiently large containing $z \bmod P$ in $\kappa(P)$, we can split the $\widetilde{\rho}$-representation module $(\mathbb{T}'_P)^2$ into the product of two eigenspaces of $\widetilde{\rho}(\sigma)$. We have eigenspace decomposition $L(\widetilde{\rho}) = L(\widetilde{\rho})[1] \oplus L(\widetilde{\rho})[z]$ under $\widetilde{\rho}(\sigma)$. Then $u(p)$ acts on $L(\widetilde{\rho})[1] = H^0(I_p, L(\widetilde{\rho})) \cong \mathbb{T}'_P$ as a $\mathbb{T}'_P$-linear operator (the action of Frob_p); so, $u(p) \in \mathbb{T}'_P$.

If $\chi_1|_{\mathbb{Z}_p^\times}$ is non-trivial, we can again find $\sigma \in I_p$ such that the eigenvalue of $\widetilde{\rho}(\sigma)$ is $a = 1$ and $b \in W^\times$ with $a \not\equiv b \bmod P$. Then under the notation introduced in the proof for $q \neq p$, we have $L(\widetilde{\rho})[a] \cong \mathbb{T}'_P \cong L(\widetilde{\rho})[b]$. Since $u(p)$ is the eigenvalue of Frob_p on $L(\rho')[a]$, we get $u(p) \in \mathbb{T}'_P$. This finishes the proof of the last assertion (4). □

We will identify in § 7 the characteristic ideal of the congruence module between the CM component $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}) \subset \mathrm{Spec}(\mathbb{T})$ and its complement with the ideal generated by the anticyclotomic Katz measure in [Kat78, HT93] (interpolating anticyclotomic Hecke L-values). Since the anticyclotomic Katz measure is a measure on the anticyclotomic class group, we need to relate class group $Z := Cl_M(\mathfrak{C}\mathfrak{p}^\infty)$ and its anticyclotomic counter part $Cl_M^-(\mathfrak{c}'p^\infty)$ ($\mathfrak{c}' = \mathfrak{C} \cap \overline{\mathfrak{C}}$). This is what we do now. Consider the ray class group $Cl_M(\mathfrak{C}\mathfrak{p}^r)$ modulo $\mathfrak{C}\mathfrak{p}^r$, and put

$$Z = \varprojlim_r Cl_M(\mathfrak{C}\mathfrak{p}^r), \quad \text{and} \quad \mathfrak{Z} = \varprojlim_r Cl_M(\mathfrak{c}'p^r). \tag{5.2}$$

On $\mathfrak{Z}$, complex conjugation c acts as an involution.

Let Z_p (respectively $\mathfrak{Z}_p$) be the Sylow p-part of Z (respectively $\mathfrak{Z}$). We have a natural inclusion $(\mathfrak{O}_{\mathfrak{p}}^\times \times \mathfrak{O}_{\overline{\mathfrak{p}}}^\times)/\mathfrak{O}^\times$ into $\mathfrak{Z}$. Let $Z^- = \mathfrak{Z}/\mathfrak{Z}^{1+c}$ (the maximal quotient on which c acts by -1). We have the projections

$$\pi : \mathfrak{Z} \twoheadrightarrow Z \quad \text{and} \quad \pi^- : \mathfrak{Z} \to Z^-.$$

The projection π^- induces an isogeny $\mathfrak{Z}^{1-c} = \{zz^{-c} \mid z \in \mathfrak{Z}\} \to Z^-$ whose kernel and cokernel are killed by 2. In particular, assuming $p > 2$, π^- induces an isomorphism between the maximal p-profinite subgroups $Z_p^- \subset Z^-$ and $\mathfrak{Z}_p^{1-c} \subset \mathfrak{Z}^{1-c}$; namely, we have $\pi^- : \mathfrak{Z}_p^{1-c} \cong Z_p^-$ if $p > 2$. Similarly, π induces $\pi : \mathfrak{Z}_p^{1-c} \cong Z_p$ if $p > 2$. Assume now $p > 2$. Thus we have $\iota : Z_p \cong Z_p^-$ by first lifting $z \in Z_p$ to $\widetilde{z} \in \mathfrak{Z}_p^{1-c}$ and taking its square root and then projecting down to $\pi^-(\widetilde{z}^{1/2})$. The isomorphism ι identifies the maximal torsion-free quotients of the two groups Z_p and Z_p^- which we write as Γ_M. This ι also induces W-algebra isomorphism $W[[Z_p]] \cong W[[Z_p^-]]$ which is again written by ι. Then we have $Z = Z^{(p)} \times Z_p$ with finite group $Z^{(p)}$ of order prime to p. Identify $Z_p = \mathrm{Gal}(M_p/M)$ (respectively $Z^{(p)} = \mathrm{Gal}(M_Z^{(p)}/M)$) for an abelian extension M_p/M (respectively $M_Z^{(p)}/M$) by the Artin symbol.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

LEMMA 5.5. *The algebra $W[[Z_p]]$ is a local complete intersection and hence Gorenstein over Λ_W.*

Proof. The natural map $\Gamma \subset \mathbb{Z}_p^\times \to Z$ induces a $W[[\Gamma]]$-algebra structure on $W[[Z_p]]$. Identifying $W[[\Gamma]]$ with Λ_W by $\gamma \mapsto t$, we regard $W[[Z_p]]$ as a Λ_W-algebra. Writing Z_p/Γ as a product of cyclic groups $C_1 \times \cdots \times C_r$ with $|C_j| = q_j$ for a p-power q_j and picking $z_j \in Z_p$ whose image generates C_j, we have $z_j^{q_j} \in \Gamma$ which we regard as an element $[z_j^{q_j}]$ of $\Gamma \subset W[[\Gamma]] = \Lambda_W$. Then we have an isomorphism $\Lambda_W[T_1, \dots, T_r]/((1+T_j)^{q_j} - [z_j^{q_j}])_j$ for the polynomial ring $\Lambda_W[T_1, \dots, T_r]$ and its ideal $((1+T_j)^{q_j} - [z_j^{q_j}])_j$ generated by $(1+T_j)^{q_j} - [z_j^{q_j}] \in \Lambda_W[T_1, \dots, T_r]$ for $j = 1, 2, \dots, r$. This shows that $W[[Z_p]]$ is a p-profinite local complete intersection over the regular ring Λ_W (and is hence a Gorenstein Λ_W-algebra; see [Mat86, Theorem 21.3]). □

We regard $W[[Z_p^-]]$ as a Λ_W-algebra by the isomorphism ι. Let $\mathbb{T}$ be a connected component of $\mathbf{h}$ containing a CM component $\mathbb{J}$ with $C(\rho_\mathbb{J}) = N$. Recall the character $\Psi_\mathbb{J} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \widetilde{\mathbb{J}}^\times$ as in (CM2) in Proposition 5.1. By class field theory, we may regard $\Psi_\mathbb{J}$ as a character $\Psi_\mathbb{J} : Z \to \widetilde{\mathbb{J}}^\times$. Taking W sufficiently large so that $W = \widetilde{\mathbb{J}} \cap \overline{\mathbb{Q}}_p$, then $\Psi_\mathbb{J}|_{Z^{(p)}}$ has values in $W^\times \subset \widetilde{\mathbb{J}}^\times$. Define $\Psi_\mathbb{T} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[Z_p]]^\times$ by a homomorphism given by $\Psi_\mathbb{T}(\sigma) = \Psi_\mathbb{J}(\sigma|_{M_Z^{(p)}})\sigma|_{M_p} \in W[[Z_p]]$, where we regard $\Psi_\mathbb{J}(\sigma|_{M_Z^{(p)}}) \in W \subset W[[Z_p]]$. Define $\Psi'_\mathbb{T} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[Z_p^-]]$ by $\Psi'_\mathbb{T} = \iota \circ \Psi_\mathbb{T}$. By Lemma 5.4 combined with [Hid86a, § 7] (or [Hid93, § 7.6]), there exist algebra homomorphisms $\Theta : \mathbb{T} \to W[[Z_p]]$ and $\Theta^- : \mathbb{T} \to W[[Z_p^-]]$ given by $\Theta(\mathrm{Tr}(\rho_\mathbb{T}(\mathrm{Frob}_l)) = \mathrm{Tr}(\mathrm{Ind}_M^\mathbb{Q} \Psi_\mathbb{T}(\mathrm{Frob}_l))$ and $\Theta^-(\mathrm{Tr}(\rho'_\mathbb{T}(\mathrm{Frob}_l)) = \mathrm{Tr}(\mathrm{Ind}_M^\mathbb{Q} \Psi'_\mathbb{T}(\mathrm{Frob}_l))$ for all primes $l \nmid N(\mathfrak{C})p$, where $\rho'_\mathbb{T} = \rho_\mathbb{T} \otimes \sqrt{\langle \boldsymbol{\kappa} \rangle}^{-1}$ as in Lemma 5.4. The above identities uniquely determine these homomorphisms by Lemma 5.4(2). We check that Θ (and hence Θ^-) is a Λ_W-algebra homomorphism. We summarize in the following lemma.

LEMMA 5.6. *Let the notation be as above, and assume $p > 2$. Then:*

(1) $\Theta^- \circ \rho'_\mathbb{T} \cong \mathrm{Ind}_M^\mathbb{Q} \Psi'_\mathbb{T}$ *over* $Q(\mathbb{T})$;
(2) $\iota : Z_p \cong Z_p^-$ *canonically;*
(3) *if $N = C(\rho_\mathbb{J})$ for a CM component $\mathbb{J}$, the following diagram of Λ_W-algebras is commutative.*

$$\begin{array}{ccc} \mathbb{T} & \xrightarrow{\Theta} & W[[Z_p]] \\ \| \downarrow & & \downarrow \iota \\ \mathbb{T} & \xrightarrow[\Theta^-]{} & W[[Z_p^-]] \end{array}$$

Proof. The only fact we need to verify is the identity $\rho'_\mathbb{T} \cong \mathrm{Ind}_M^\mathbb{Q} \Psi'_\mathbb{T}$ over $Q(\mathbb{T})$. Let $\langle \Psi' \rangle$ be the projection of $\Psi'_\mathbb{T}$ to the p-profinite part of the image $\mathrm{Im}(\Psi'_\mathbb{T})$. Since $\rho_\mathbb{T}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)} = \mathrm{Ind}_M^\mathbb{Q} \Psi_\mathbb{T}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)} = \Psi \oplus \Psi^c$, we have $\boldsymbol{\kappa} := \det(\rho_\mathbb{T}) = \det(\mathrm{Ind}_M^\mathbb{Q} \Psi_\mathbb{T}) = \Psi^{1+c}$ over $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$, where $\Psi^{1+c}(\sigma) = \Psi(\sigma c \sigma c^{-1})$. Thus $\langle \boldsymbol{\kappa} \rangle|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)}$ is equal to $\langle \Psi_\mathbb{T} \rangle^{1+c}$. Since $\rho'_\mathbb{T} = \rho_\mathbb{T} \otimes \sqrt{\langle \boldsymbol{\kappa} \rangle}^{-1}$, we have $\Theta^- \circ \rho'_\mathbb{T} \cong \mathrm{Ind}_M^\mathbb{Q}(\Psi_\mathbb{T} \langle \Psi_\mathbb{T} \rangle^{-(1+c)/2}) = \mathrm{Ind}_M^\mathbb{Q}(\psi_\mathbb{T} \cdot \langle \Psi_\mathbb{T} \rangle^{(1-c)/2})$, where $\psi_\mathbb{T} = \Psi_\mathbb{T}/\langle \Psi_\mathbb{T} \rangle$ (the prime-to-p part of $\Psi_\mathbb{T}$). By the construction of ι and the definition $\Psi'_\mathbb{T} = \iota \circ \Psi_\mathbb{T}$, we confirm $\Psi'_\mathbb{T} = \psi_\mathbb{T} \cdot \langle \Psi_\mathbb{T} \rangle^{(1-c)/2}$. □

Fix a CM irreducible component $\mathrm{Spec}(\mathbb{J})$ of $\mathrm{Spec}(\mathbf{h})$, and let $\mathrm{Spec}(\mathbb{T})$ be the connected component of $\mathrm{Spec}(\mathbf{h})$ containing $\mathrm{Spec}(\mathbb{J})$. Let $\mathfrak{C}$ be the prime-to-p conductor of the associated character $\Psi_\mathbb{J}$. Regard the character $\Psi_\mathbb{J}$ as a $\mathbb{Z}_p$-algebra homomorphism of $\mathbb{Z}_p[[Z]]$ into $\mathbb{J}$. Then

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

the algebra homomorphism $\Psi_{\mathbb{J}}$ restricted to $\mathbb{Z}_p[Z^{(p)}]$ has values in $\mathbb{J} \cap \overline{\mathbb{Q}}_p$, which is a discrete valuation ring finite flat over $\mathbb{Z}_p$. By extending scalars, we assume $\overline{\mathbb{Q}}_p \cap \mathbb{J} = W$.

Proposition 5.7. *Let $\mathbb{J}$ be a CM component $\mathrm{Spec}(\mathbb{J}) \subset \mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$, and let $\overline{\psi} = \Psi_{\mathbb{J}} \bmod \mathfrak{m}_{\mathbb{J}}$. Assume $p > 2$ and the following two conditions:*

(i) *$\overline{\psi}^-$ has order > 2, and $\overline{\psi}$ is ramified at $\mathfrak{p}$ (and unramified at $\mathfrak{p}^c$) with $\mathfrak{C} = \mathfrak{C}(\overline{\psi}^-)$;*
(ii) *$C(\overline{\rho}) = N$ for $\overline{\rho} = \rho_{\mathbb{J}} \bmod \mathfrak{m}_{\mathbb{J}} = \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$.*

Then we have:

(1) *$\mathbb{T}$ is a Gorenstein ring, and $\mathbb{T}_{\mathrm{cm}}$ is a local complete intersection canonically isomorphic to $W[[Z_p]]$ for the maximal p-profinite quotient Z_p of $Z = \varprojlim_n Cl_M(\mathfrak{C}\mathfrak{p}^n)$;*
(2) *writing $\rho_{\mathbb{T}_{\mathrm{cm}}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \boldsymbol{\psi}$ (respectively $\overline{\rho} = \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$) for a character $\boldsymbol{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[Z_p]]^\times$ (respectively $\overline{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to (W/\mathfrak{m}_W)^\times$), the ring $\mathbb{T}_{\mathrm{cm}}$ with universal character $\boldsymbol{\psi}$ is isomorphic to the universal deformation ring of $\overline{\psi}$ over W for characters unramified outside $\mathfrak{C}\mathfrak{p}$;*
(3) *each CM component $\mathbb{J}$ of $\mathbb{T}$ is canonically isomorphic to $W[[\Gamma_M]]$ and hence $\widetilde{\mathbb{J}} = \mathbb{J}$, where Γ_M is the maximal torsion-free quotient of Z.*

Proof. If $\overline{\rho} = \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$, $\overline{\rho}$ determines the pair of characters $\{\overline{\psi}, \overline{\psi}^c\}$. By (i) (and Proposition 5.2), $\overline{\rho}$ is absolutely irreducible and is not isomorphic to any induced representations from any other quadratic field. Since $C(\overline{\rho}) = N(\mathfrak{C}(\overline{\psi}))D$, $N = C(\overline{\rho})$ and $N = N(\mathfrak{C})D$ implies $\mathfrak{C}(\overline{\psi}) = \mathfrak{C}$.

Let $(R, \widetilde{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to R^\times)$ be the universal couple with the universal character unramified outside $\mathfrak{p}\mathfrak{C}$ deforming $\overline{\psi}$ over W. This couple $(R, \widetilde{\psi})$ is characterized by the following universal property: for any local pro-artinian W-algebra A with residue field $\mathbb{F}$ and any character $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to A^\times$ unramified outside $\mathfrak{p}\mathfrak{C}$ with $\varphi \bmod \mathfrak{m}_A = \overline{\psi}$ (for the maximal ideal $\mathfrak{m}_A$ of A), there exists a unique W-algebra homomorphism $\iota : R \to A$ such that $\varphi = \iota \circ \widetilde{\psi}$. Such a pair (A, φ) is called a deformation of $\overline{\psi}$ (see [Maz89] for general theory of Galois deformation).

We now show $R \cong W[[Z_p]]$ by class field theory. To see this, we pick a deformation $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to A^\times$ of $\overline{\psi}$ unramified outside $\mathfrak{p}\mathfrak{C}$; thus, A is a local aritinian W-algebra sharing the residue field $\mathbb{F}$ with W and $\varphi \bmod \mathfrak{m}_A = \overline{\psi}$ for the maximal ideal $\mathfrak{m}_A$ of A. Let ψ be the Teichmüller lift of $\overline{\psi}$; so, $\varphi' = \varphi\psi^{-1}$ has p-power order. For a prime $\mathfrak{l}|\mathfrak{C}$, by class field theory, the image $I_{\mathfrak{l}}^{ab}$ of the inertia group $I_{\mathfrak{l}} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/M)$ in the Galois group of the maximal abelian extension of M over M is isomorphic to the multiplicative group $\mathfrak{O}_{\mathfrak{l}}^\times$ of the $\mathfrak{l}$-adic integer ring of $M_{\mathfrak{l}}$. Since φ' has p-power order and $p \neq l$, φ' must be trivial on $1 + \mathfrak{l}\mathfrak{O}_{\mathfrak{l}} \subset \mathfrak{O}_{\mathfrak{l}}^\times$. Thus the $\mathfrak{l}$-conductor of φ' is at most $\mathfrak{l}$, and hence $\varphi = \varphi'\psi$ factors through Z. Thus φ' factors through the maximal p-profinite quotient Z_p and extends to a unique W-algebra homomorphism $\iota = \iota_\varphi : W[[Z_p]] \to A$ such that $\iota|_{Z_p} = \varphi'$. Since Z_p is the maximal p-profinite quotient of Z, by class field theory, we have the corresponding subfield $\widetilde{M}$ of the ray class field modulo $\mathfrak{p}^\infty\mathfrak{C}$ such that $\mathrm{Gal}(\widetilde{M}/M) \cong Z_p$ by Artin symbol. Writing the inclusion $Z_p \subset W[[Z_p]]$ as $\gamma \mapsto [\gamma]$ and identifying $\mathrm{Gal}(\widetilde{M}/M) = Z_p$, define a character $\boldsymbol{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[Z_p]]$ by $\boldsymbol{\psi}(\sigma) = \psi(\sigma)[\sigma|_{\widetilde{M}}]$. Then by our construction $\iota \circ \boldsymbol{\psi} = \varphi$; so, $(W[[Z_p]], \boldsymbol{\psi})$ satisfies the universal property of $(R, \widetilde{\psi})$ for deformations φ of $\overline{\psi}$.

For an ideal $\mathfrak{a}$ of $\mathbb{T}$, write $\rho_{\mathfrak{a}} = \rho_{\mathbb{T}} \bmod \mathfrak{a}$ by abusing the symbol slightly. If $\rho_{\mathfrak{a}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \psi'$ for a character $\psi' : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to A^\times$ for a local ring A containing $\mathbb{T}/\mathfrak{a}$, ψ' has values in $(\mathbb{T}/\mathfrak{a})^\times$ (by (i) and Hensel's lemma). Then we have $C(\overline{\rho})|C(\rho_{\mathfrak{a}})|C(\rho_{\mathbb{T}}) = C(\rho_{\mathbb{J}}) = C(\overline{\rho})$ by (ii). Thus $C(\overline{\rho}) = C(\rho_{\mathfrak{a}})$. Write $\mathfrak{C}'$ for the prime-to-p conductor of ψ'. Then $N(\mathfrak{C}')D = C(\rho_{\mathfrak{a}}) = C(\overline{\rho}) = N(\mathfrak{C})D$. One of ψ' or ψ'^c must be a deformation of $\overline{\psi}$, and one of them ramifies at $\mathfrak{p}$. Let ψ'

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

be the character ramifying at $\mathfrak{p}$. Then ramification of ψ' at $\mathfrak{p}$ forces $\psi' \equiv \overline{\psi}$ mod $\mathfrak{m}$, as $\overline{\psi}$ is the unique choice ramifying at $\mathfrak{p}$. Then we find $\mathfrak{C} = \mathfrak{C}(\overline{\psi})|\mathfrak{C}'$; so, $\mathfrak{C} = \mathfrak{C}'$. Thus ψ' factors through Z. By Proposition 5.2, (i) implies that the local ring of $\mathbb{T}$ contains CM components of a single imaginary quadratic field M deforming $\overline{\psi}$. This shows that the reduced part $\mathbb{T}_{\mathrm{cm}}^{\mathrm{red}}$ of $\mathbb{T}_{\mathrm{cm}}$ is the surjective image of $W[[Z_p]]$ for a canonical morphism $\pi : W[[Z_p]] \to \mathbb{T}_{\mathrm{cm}}^{\mathrm{red}}$ with $\mathrm{Ind}_M^{\mathbb{Q}}(\pi \circ \boldsymbol{\psi}) \cong \rho_{\mathbb{T}_{\mathrm{cm}}^{\mathrm{red}}}$. Since $N = C(\overline{\rho})$, $\mathbb{T}$ kills any old forms of level N and hence $\mathbb{T}$ is reduced (by Lemma 5.4(1)). Thus $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ is reduced, and hence $\mathbb{T}_{\mathrm{cm}}$ is the surjective image of $W[[Z_p]]$ under π.

Pick an irreducible component $\mathrm{Spec}(\mathbb{J}) \subset \mathrm{Spec}(W[[Z_p]])$. Then we have a continuous character $\Psi_{\mathbb{J}} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{J}^\times$ with $\Psi_{\mathbb{J}} \equiv \overline{\psi}$ mod $\mathfrak{m}_{\mathbb{J}}$ such that $\rho_{\mathbb{J}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi_{\mathbb{J}}$. From $\mathfrak{C} = \mathfrak{C}(\overline{\psi})|\mathfrak{C}(\Psi_{\mathbb{J}})|\mathfrak{C}$, we conclude $\mathfrak{C}(\Psi_{\mathbb{J}}) = \mathfrak{C}$. Thus ramification of $\Psi_{\mathbb{J}}$ is completely determined by $\overline{\psi}$; so, we have $W[[T]]$-algebra homomorphism $\Theta : \mathbb{T} \to \mathbb{J}$ associated to $\Psi_{\mathbb{J}}$. Since Θ gives rise to a CM component, it factors through $\mathbb{T}_{\mathrm{cm}}$ and makes the following diagram commutative.

$$\begin{array}{ccc} \mathbb{T}_{\mathrm{cm}} & \xrightarrow{\Theta} & \mathbb{J} \\ \uparrow & & \Vert \\ W[[Z_p]] & \longrightarrow & \mathbb{J} \end{array}$$

Thus $W[[Z_p]] \to \mathbb{T}_{\mathrm{cm}}$ is non-trivial over all irreducible components of $\mathrm{Spec}(W[[Z_p]])$; so, it is injective, and $\rho_{\mathbb{T}_{\mathrm{cm}}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \boldsymbol{\psi}$. This proves the assertion (2).

By Lemma 5.5, $\mathbb{T}_{\mathrm{cm}} \cong W[[Z_p]]$ is a complete intersection. Each irreducible component of $\mathrm{Spec}(W[[Z_p]])$ is given by $\mathrm{Spec}(W[[\Gamma_M]])$, and hence any CM component of $\mathbb{T}$ is canonically isomorphic to $W[[\Gamma_M]]$. Since $W[[\Gamma_M]]$ is integrally closed, we have $\widetilde{\mathbb{J}} = \mathbb{J}$. This proves (3).

Taking inertia group $I_p = I_{\mathfrak{p}}$, Gorenstein-ness of $\mathbb{T}$ follows from Theorem 7.1 in the following section as $\overline{\rho}$ is absolutely irreducible and $\overline{\rho}|_{I_{\mathfrak{p}}} \cong \overline{\psi}|_{I_{\mathfrak{p}}} \oplus \overline{\psi}^c|_{I_{\mathfrak{p}}}$ with $\overline{\psi}$ ramified at $\mathfrak{p}$ and $\overline{\psi}^c$ unramified at $\mathfrak{p}$. This finishes the proof of (1). $\square$

6. p-Adic Hecke L-functions

In this section, we assume that W contains a Witt vector ring $W(\overline{\mathbb{F}}_p)$ for an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$; so, $\mathbb{F} = \overline{\mathbb{F}}_p$ in this section. We recall Katz's theory in [Kat78] (and [HT93]) of p-adic L-functions. We fix a prime-to-p conductor ideal $\mathfrak{C}$ of an imaginary quadratic field $M \subset \overline{\mathbb{Q}}$ in which p splits into $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ ($\overline{\mathfrak{p}} = \mathfrak{p}^c$ for the generator c of $\mathrm{Gal}(M/\mathbb{Q})$) for $\mathfrak{p} = \{\alpha \in \mathfrak{O} \mid |i_p(\alpha)|_p < 1\}$. We write the embedding $M \subset \overline{\mathbb{Q}}$ as $i : M \hookrightarrow \overline{\mathbb{Q}}$.

Let $\lambda : M_{\mathbb{A}}^\times / M^\times \to \mathbb{C}^\times$ be a type A_0 Hecke character (of conductor $\mathfrak{C}(\lambda)|\mathfrak{C}p^\infty$). Then λ has values in $\overline{\mathbb{Q}}$ on the finite part $M_{\mathbb{A}(\infty)}^\times$ of $M_{\mathbb{A}}^\times$. For the ray class group $\mathfrak{Z}$ modulo $\mathfrak{C}p^\infty$ of M, write $\widehat{\lambda} : \mathfrak{Z} \to \overline{\mathbb{Q}}_p^\times$ for the p-adic avatar of λ. Let $-D$ be the discriminant of M so that $M = \mathbb{Q}[\sqrt{-D}]$, and put $2\delta = \sqrt{-D}$. The alternating form $(x, y) = \mathrm{Tr}_{M/Q}(xy^c/\sqrt{-D})$ induces the principal polarization on the elliptic curve $E(\mathfrak{O})$ defined over $\mathcal{W} = i_p^{-1}(W)$ with complex multiplication by $\mathfrak{O}$ with complex uniformization $E(\mathfrak{O})(\mathbb{C}) \cong \mathbb{C}/\mathfrak{O}$. A choice of Néron differential on $E(\mathfrak{O})_{/\mathcal{W}}$ produces its complex period and p-adic period $(\Omega_\infty, \Omega_p) \in (\mathbb{C}^\times \times W^\times)$. Katz constructed in [Kat78] (see also [HT93] where the case $\mathfrak{C} \neq 1$ is treated) a measure φ with values in W on the ray class group $\mathfrak{Z}$ modulo $\mathfrak{C}p^\infty$ characterized by the formula

$$i_p^{-1}\left(\frac{\int_{\mathfrak{Z}} \widehat{\lambda}\, d\varphi}{\Omega_p^{k+2\kappa}}\right) = (\mathfrak{O}^\times : \mathbb{Z}^\times)\frac{c(\lambda)\pi^\kappa L(0,\lambda)}{\mathrm{Im}(\delta)^\kappa \Omega_\infty^{k+2\kappa}}(1-\lambda(\mathfrak{p}))(1-\lambda(\overline{\mathfrak{p}})N(\mathfrak{p})^{-1})\prod_{\mathfrak{L}|\mathfrak{C}}(1-\lambda(\mathfrak{L})) \in \mathcal{W} \quad (6.1)$$

for all Hecke characters λ modulo $\mathfrak{C}p^\infty$. Here $L(s,\lambda)$ is the primitive complex L-function of λ, and we use the convention that $\lambda(\mathfrak{L}) = 0$ for a prime $\mathfrak{L}$ (of M) if $\mathfrak{L}$ divides the conductor of λ, and if $\mathfrak{L}$ is prime to the conductor of λ, $\lambda(\mathfrak{L})$ is the value of the primitive character associated to λ. Here the infinity type of λ is $ki + \kappa(i - c)$ for integers k and κ satisfying either $k > 0$ and $\kappa \geqslant 0$ or $k \leqslant 1$ and $\kappa \geqslant 1 - k$, $c(\lambda) \neq 0$ is a simple algebraic constant involving the root number of λ and the value of its Γ-factor as specified in [HT93, Theorem 4.1]. Identifying $W[[\mathfrak{Z}]]$ with the measure algebra under convolution product, we may regard $\varphi \in W[[\mathfrak{Z}]]$. Strictly speaking, the measure φ slightly depends on a choice of $\mathfrak{F}$ in the following decomposition.

Definition 6.1. We decompose $\mathfrak{C}$ into a product $\mathfrak{F}\mathfrak{F}_c\mathfrak{I}$ such that $\mathfrak{I}$ is a product of inert and ramified primes over $\mathbb{Q}$ and $\mathfrak{F}\mathfrak{F}_c$ for a product of primes split over $\mathbb{Q}$ with $\mathfrak{F} \subset \mathfrak{F}_c^c$ and $\mathfrak{F} + \mathfrak{F}_c = \mathfrak{O}$.

By the interpolation formula (6.1) and the description of $c(\lambda)$ in [HT93, Theorem 4.1], the measure is independent of $\mathfrak{F}$ up to units in $W[[\mathfrak{Z}]]$.

Fix a CM component $\mathbb{J}$ of $\mathbf{h}^M_{\mathrm{cm}}$. Since we work under the assumptions of Proposition 5.7, we have $\widetilde{\mathbb{J}} = \mathbb{J}$. Then the associated character $\Psi_{\mathbb{J}}$ has values in $\mathbb{J}^\times$. Take its anticyclotomic projection $\Psi^-_{\mathbb{J}}$, and write $\mathfrak{C}$ for the conductor of $\Psi^-_{\mathbb{J}}$, we may regard $\Psi^-_{\mathbb{J}}$ as a character $\Psi^-_{\mathbb{J}} : Z^- \to \mathbb{J}^\times$, which induces W-algebra homomorphism $\Psi^-_{\mathbb{J}} : W[[Z^-]] \to \mathbb{J}$. We then write $L_p(\Psi^-_{\mathbb{J}}) \in \mathbb{J}$ for the image under $\Psi^-_{\mathbb{J}} : W[[Z^-]] \to \mathbb{J}$ of $\varphi^- = \pi^-_*(\varphi)$. Decompose $Z^- = \Delta^- \times \Gamma^-_M$ for the maximal finite subgroup Δ^- and the maximal torsion-free quotient Γ^-_M. Via $\iota : Z_p \cong Z^-_p$, we identify $\Gamma_M = \Gamma^-_M$. By this projection $\Psi^-_{\mathbb{J}} : W[[Z^-]] \to \mathbb{J}$, we identify $\mathbb{J} = W[[\Gamma^-_M]] = W[[\Gamma_M]]$, and in this sense, $L_p(\Psi^-_{\mathbb{J}})$ is a branch of the anticyclotomic Katz measure $\pi^-_*(\varphi) = \varphi^- \in W[[Z^-]]$. We have a canonical decomposition $Z^- = Z^{(p)}_- \times Z^-_p$ for the maximal finite subgroup $Z^{(p)}_-$ of order prime to p. If we fix a character $\overline{\psi}^- : Z^- \to \mathbb{F}^\times$, its Teichmüller lift $\psi^- : Z^- \to W^\times$ factors through $Z^{(p)}_-$. So we have a ψ^--projection $\pi^-_{\psi^-} : W[[Z^-]] \to W[[Z^-_p]]$ sending $(z^{(p)}, z_p) \in Z^- \subset W[[Z^-]]^\times$ to $\psi^-(z^{(p)})z_p \in W[[Z^-_p]]$. We put $L^-(\overline{\psi}^-) = \pi^-_{\psi^-} \circ \varphi^- = \pi^-_{\psi^-,*}\varphi^- \in W[[Z^-_p]] \xrightarrow[\iota^{-1}]{\sim} W[[Z_p]]$. The projection of $L^-(\psi^-)$ to each irreducible component $\mathbb{J}$ of $\mathbb{T}^M_{\mathrm{cm}} \cong W[[Z^-_p]]$ gives rise to $L_p(\Psi^-_{\mathbb{J}}) \in \mathbb{J}$.

7. Congruence modules

Let $\mathrm{Spec}(\mathbb{T})$ be a reduced connected component of $\mathrm{Spec}(\mathbf{h})$. Write $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(Q(\mathbb{T}))$ for the Galois representation associated to this component. We quote the following result from [Hid13a, Theorem 4.1], which is essentially proven in [MW86, Proposition 2 in § 9].

Theorem 7.1. *Let $\mathfrak{P}$ be a prime ideal in $\mathrm{Spec}(\mathbb{T})$. If $\rho_{\mathfrak{P}}$ is absolutely irreducible and $\rho_{\mathfrak{P}}|_{I_p} \cong \left(\begin{smallmatrix}\delta & * \\ 0 & 1\end{smallmatrix}\right)$ with $\delta \neq 1$ for the inertia group $I_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p, then the localization $\mathbb{T}_{\mathfrak{P}}$ is a Gorenstein ring.*

Let J be as in the introduction (the ordinary part of the projective limit of the Tate modules of modular jacobians) on which $\mathbf{h}$ acts, and write $J(\mathbb{T}) = \mathbb{T} \cdot J$. Then the connected–étale exact sequence produces the following commutative diagram of exact rows.

$$\begin{array}{ccccc} J(\mathbb{T})^\circ & \hookrightarrow & J(\mathbb{T}) & \twoheadrightarrow & J(\mathbb{T})^{\mathrm{et}} \\ \wr\downarrow & & \Vert\downarrow & & \wr\downarrow \\ \mathbb{T} & \hookrightarrow & J(\mathbb{T}) & \twoheadrightarrow & \mathrm{Hom}_\Lambda(J(\mathbb{T}),\Lambda) \end{array}$$

Here the vertical arrows are isomorphisms of $\mathbb{T}$-modules. This is shown in [Hid86b] under the condition (R) in the introduction and in [Oht03] without assuming (R). Thus Gorenstein-ness of $\mathbb{T}_{\mathfrak{P}}$ implies freeness of $J(\mathbb{T})_{\mathfrak{P}}$ over $\mathbb{T}_{\mathfrak{P}}$. In particular, if (R) is satisfied and $\overline{\rho} = \rho_{\mathfrak{m}}$ is absolutely irreducible, $\mathcal{L}_{\mathrm{can}}(\mathbb{I}) = J(\mathbb{T}) \otimes_{\mathbb{T}} \mathbb{I}$ is free of rank 2 as claimed in the introduction (so, in this case, ($\mathrm{F}_{\mathrm{can}}$) holds).

Let $\mathrm{Spec}(\mathbb{J}) \subset \mathrm{Spec}(\mathbf{h}^M_{\mathrm{cm}})$ be a CM irreducible component and $\mathrm{Spec}(\mathbb{T})$ be the connected component of $\mathrm{Spec}(\mathbf{h})$ with $\mathrm{Spec}(\mathbb{J}) \subset \mathrm{Spec}(\mathbb{T})$. Assume that $\mathrm{Spec}(\mathbb{T})$ is reduced, and write $\overline{\rho} = \rho_{\mathfrak{m}_{\mathbb{T}}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ for the mod p representation of the component $\mathbb{T}$. Then $\overline{\rho} \cong \mathrm{Ind}^{\mathbb{Q}}_M \overline{\psi}$ for a character $\overline{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \mathbb{F}^\times$. Let ψ be the Teichmüller lift of $\overline{\psi}$. Write $\mathfrak{C} = \mathfrak{C}(\Psi_{\mathbb{J}})$ for the prime-to-p conductor of the associated character $\Psi_{\mathbb{J}} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \widetilde{\mathbb{J}}^\times$; so we assume $\overline{\psi} = (\Psi_{\mathbb{J}} \bmod \mathfrak{m}_{\mathbb{J}})$. Write $\mathrm{Spec}(\mathbb{T}^M_{\mathrm{cm}}) = \mathrm{Spec}(\mathbf{h}^M_{\mathrm{cm}}) \cap \mathrm{Spec}(\mathbb{T})$; so, $\mathrm{Spec}(\mathbb{T}^M_{\mathrm{cm}})$ is the minimal closed subscheme in $\mathrm{Spec}(\mathbb{T})$ containing all components with CM by M. We therefore have the projection maps

$$\mathbb{T} \twoheadrightarrow \mathbb{T}^M_{\mathrm{cm}} \twoheadrightarrow \mathbb{J}$$

where all rings involved are Gorenstein rings if $\overline{\rho}$ is absolutely irreducible and $\overline{\psi}^-$ has order > 2 and is ramified at p (see Proposition 5.7). Recall S, which is the set of split prime factors $\mathfrak{q}$ in M of N but $\mathfrak{q} \nmid N(\mathfrak{C}(\Psi^-_{\mathbb{J}}))$. Consider

$$E_{1,N} = \prod_{\mathfrak{q} \in S} \{(1 - \Psi^-_{\mathbb{J}}(\mathfrak{q}) N(\mathfrak{q})^{-1})(1 - \Psi^-_{\mathbb{J}}(\overline{\mathfrak{q}}) N(\overline{\mathfrak{q}})^{-1})\} \in \mathbb{J} \quad \text{and } E_{1,N} = 1 \text{ if } S = \emptyset. \tag{7.1}$$

Note here that $E_{1,N}$ is the product of Euler factors at $\mathfrak{q} \in \Sigma_{\mathfrak{C}}$ of $L_p(\Psi^-_{\mathbb{J}})$.

Hereafter in this section, we assume that $W \supset W(\overline{\mathbb{F}}_p)$ to have $L^-_p(\overline{\psi}^-) \in W[[Z^-_p]]$ as in § 6.

Theorem 7.2. *Let the notation be as above. Suppose $W \supset W(\overline{\mathbb{F}}_p)$, $p \geqslant 5$, that* $\mathrm{Spec}(\mathbb{T})$ *contains a non-CM minimal primitive component* $\mathrm{Spec}(\mathbb{I})$ *and that $\overline{\rho} \cong \mathrm{Ind}^{\mathbb{Q}}_M \overline{\psi}$ for an imaginary quadratic field M in which p splits. Suppose further that $\overline{\psi}^-$ has order > 2, $\overline{\psi}$ ramifies at $\mathfrak{p}$, and one of the following conditions holds:*

(a) *$p \nmid \varphi(N)$ and $C(\overline{\rho}) = N$;*
(b) *$E_{1,N} \notin \mathfrak{m}_{\mathbb{J}}$ and $p \nmid \Phi(N)$ for the Euler function Φ of M (i.e. $\Phi(N) = N^2 \prod_{\mathfrak{q}|N}(1 - (1/N(\mathfrak{q})))$ for primes $\mathfrak{q}$ in M).*

Then $\mathbb{T}^M_{\mathrm{cm}}$ is canonically isomorphic to $W[[Z^-_p]]$ for the p-profinite part Z^-_p of the anticyclotomic ray class group of conductor $\mathfrak{C}(\overline{\psi}^-)p^\infty$. If we write $L^-(\overline{\psi}^-) \in W(\overline{\mathbb{F}}_p)[[Z^-_p]]$ for the anticyclotomic Katz measure of modulo p branch character $\overline{\psi}^-$ and $\mathrm{Spec}(\mathbb{T}^\perp_{\mathrm{cm}})$ *for the complement of* $\mathrm{Spec}(\mathbb{T}^M_{\mathrm{cm}})$ *in* $\mathrm{Spec}(\mathbb{T})$, *we have $\mathbb{T}^M_{\mathrm{cm}} \otimes_{\mathbb{T}} \mathbb{T}^\perp_{\mathrm{cm}} \cong W[[Z^-_p]]/L^-(\overline{\psi}^-)W[[Z^-_p]]$.*

Remark 7.3. We explain why we need to assume (a) or (b) in the above theorem. Since $C(\overline{\rho})|N$, by the existence of the Teichmüller lift of $\overline{\psi}$ and Galois deformation theory explained in Proposition 5.7(2), $\mathbb{T}^M_{\mathrm{cm}}$ is non-trivial. Taking a component $\mathbb{J}$ of $\mathbb{T}^M_{\mathrm{cm}}$, the main reason for assuming (a) or (b) is to guarantee that $\rho_{\mathbb{J}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q})}$ is minimal at primes $q|N$ split in M and that $\mathbb{J}$ is primitive. In addition, the condition $E_{1,N} \notin \mathfrak{m}_{\mathbb{J}}$ in (b) (which is automatically satisfied under (a) as $E_{1,N} = 1$ in that case) is to guarantee that $\rho_{\mathbb{I}'}|_{I_q}$ is never reducible indecomposable for any irreducible component $\mathrm{Spec}(\mathbb{I}')$ of $\mathrm{Spec}(\mathbb{T})$, where $I_q \subset \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ is the inertia group.

Let us prove this fact. If ρ_P for $P \in \mathrm{Spec}(\mathbb{I}')$ is reducible indecomposable, as is well known (see Lemma 10.1(4)), $\rho_P|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ is isomorphic to $\left(\begin{smallmatrix} \eta\mathcal{N} & * \\ 0 & \eta \end{smallmatrix}\right)$ for the p-adic cyclotomic character $\mathcal{N}$

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

acting on μ_{p^∞} (unramified at q). The character η restricted to I_q is of finite order (see § 10). If η is ramified at q and $\eta|_{I_q} \not\equiv 1 \bmod \mathfrak{m}_{\mathbb{I}'}$, lifting $\eta \bmod \mathfrak{m}_{\mathbb{I}'}$ to a non-trivial character $\overline{\eta}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathbb{T}/\mathfrak{m}_{\mathbb{T}}$ only ramified at q, the semi-simplification of $\overline{\rho} \otimes \overline{\eta}^{-1}$ is unramified; so, $\rho_{\mathbb{I}} \otimes \widetilde{\eta}^{-1}$ has less conductor than $\rho_{\mathbb{I}}$ for the Teichmüller lift $\widetilde{\eta}$ of $\overline{\eta}$. By the minimality of $\mathbb{I}$, this cannot happen; so, we conclude $\eta|_{I_q} \equiv 1 \bmod \mathfrak{m}_{\mathbb{I}'}$. By local class field theory, we may regard $\eta|_{I_q}$ as a character of $\mathbb{Z}_q^\times$. Thus $\eta|_{I_q} \neq 1$ but $\overline{\eta}|_{I_q} = 1$ implies $q \equiv 1 \bmod p$, a contradiction against $p \nmid \varphi(N)$. Hence η is unramified. The $\mathfrak{q}$-factor or $\overline{\mathfrak{q}}$-factor of $E_{1,N}$ is congruent to $1 - (\eta\mathcal{N}/\eta)(\mathrm{Frob}_q)q^{-1} = 0$ modulo $\mathfrak{m}_{\mathbb{J}}$. Since $\rho_{\mathbb{I}} \equiv \rho_{\mathbb{J}} \bmod \mathfrak{m}_{\mathbb{T}}$, we have $E_{1,N} \equiv 0 \bmod \mathfrak{m}_{\mathbb{J}}$ (contradicting $E_{1,N} \notin \mathfrak{m}_{\mathbb{J}}$). Thus $\rho_P|_{I_q}$ for every prime $P \in \mathrm{Spec}(\mathbb{T})$ is semi-simple for all primes $q|N$.

Once semi-simplicity of $\rho_P|_{I_q}$ is proven for all $q|N$, we can apply results in § 10, and the following conditions for primes $q|N$ are equivalent:

(1) $\rho_{\mathbb{I}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ is absolutely irreducible;

(2) $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ is absolutely irreducible.

Indeed, by Lemma 10.3(2), under $p \nmid \varphi(N)$, (1) $\Leftrightarrow$ (2) as $\overline{\rho} = \rho_{\mathbb{I}} \bmod \mathfrak{m}_{\mathbb{I}}$. Moreover from the minimality and primitiveness of $\rho_{\mathbb{I}}$, by Lemma 10.3(4), under $p \nmid \Phi(N)$, $C(\overline{\rho}) = C(\rho_{\mathbb{I}}) = N$; thus (b) $\Rightarrow$ (a). If $N = C(\overline{\rho})$, by Lemma 5.4(1), $\mathbb{T}$ is reduced. Hence $\mathbb{T}$ is reduced under (a) or (b). Then the following condition is equivalent to (1) (or (2)):

(3) $\rho_{\mathbb{J}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ is absolutely irreducible.

Since $N = C(\overline{\rho}) \mid C(\rho_{\mathbb{J}}) = N$, we conclude $N = C(\rho_{\mathbb{J}})$. Therefore, $\overline{\rho}$ and $\rho_{\mathbb{J}}$ must be minimal at prime q splits in M and $\mathbb{J}$ is a primitive component. Then by Lemma 7.9 and Remark 7.8 below, the characteristic power series of the congruence module of $\mathbb{T}$ with respect to $\lambda : \mathbb{T} \to \mathbb{J}$ can be computed exactly as a product of a certain ray class number of M and the Katz p-adic $L_p(\Psi_{\mathbb{J}})$, which is a key to reach the conclusion of the theorem.

We prepare some notation, four lemmas and a proposition for the proof of the theorem. The proof of the theorem will be given at the end of this section. For simplicity, we write the sequence $\mathbb{T} \twoheadrightarrow \mathbb{T}^M_{\mathrm{cm}} \twoheadrightarrow \mathbb{J}$ as $R \xrightarrow{\theta} S \xrightarrow{\mu} A$ and we put $\lambda = \mu \circ \theta : R \to A$. Under the assumption of the theorem (and Remark 7.3), R, S, A are all Gorenstein rings (by Proposition 5.7). Thus we suppose Gorenstein-ness of R, S and A in this section. We write $B = \Lambda$. Since $\mathbb{T}$ is reduced, the total quotient ring $Q(R)$ of R is a product of fields, and we have $Q(R) = Q_S \oplus Q(S)$ for the complementary semi-simple algebra Q_S. Let R_S be the projection of R in Q_S. We have the following (unique) decomposition:

(1) $\mathrm{Spec}(R) = \mathrm{Spec}(R_S) \cup \mathrm{Spec}(S)$, union of closed subschemes inducing $R \hookrightarrow (R_S \oplus S)$ with Λ-torsion module $C_0(\theta, S) := (R_S \oplus S)/R$.

Similarly, we have $Q(S) = Q_A \oplus Q(A)$ and $Q(R) = Q'_A \oplus Q(A)$ as algebra direct sums. Write S_A (respectively R_A) for the projected image of S (respectively R) in Q_A (respectively Q'_A). Then we have:

(2) $\mathrm{Spec}(S) = \mathrm{Spec}(S_A) \cup \mathrm{Spec}(A)$, union of closed subschemes inducing $S \hookrightarrow (S_A \oplus A)$ with Λ-torsion module $C_0(\mu, A) := (S_A \oplus A)/S$.

(3) $\mathrm{Spec}(R) = \mathrm{Spec}(R_A) \cup \mathrm{Spec}(A)$; union of closed subschemes inducing $R \hookrightarrow (R_A \oplus A)$ with Λ-torsion module $C_0(\lambda, A) := (R_A \oplus A)/R$.

Since $\mathbb{T}$ is reduced, S is a reduced algebra, and by Gorenstein-ness, we have

$$\mathrm{Hom}_B(R, B) \cong R, \mathrm{Hom}_B(S, B) \cong S \quad \text{and} \quad \mathrm{Hom}_B(A, B) \cong A \quad \text{as } R\text{-modules.} \tag{7.2}$$

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

Write $\pi_S : R \twoheadrightarrow R_S$ and $\pi : R \to S$ for the two projections and $(\cdot,\cdot)_R : R \times R \to B$ and $(\cdot,\cdot)_S : S \times S \to B$ for the pairing giving the self-duality (7.2). We recall the following lemma [Hid86c, Lemma 1.6].

LEMMA 7.4. *The S-ideal $\mathfrak{b} := \mathrm{Ker}(\pi_S : R \to R_S)$ is principal (and is S-free of rank 1).*

By [Hid88, Lemma 6.3] (or [Hid00, § 5.3.3]), we get the following isomorphisms of R-modules,

$$C_0(\lambda; A) \cong R_A \otimes_R A, \quad C_0(\theta; S) \cong R_S \otimes_R S \quad \text{and} \quad C_0(\mu; A) \cong S_A \otimes_S A. \tag{7.3}$$

Recall the following fact first proved in [Hid88, Theorem 6.6].

LEMMA 7.5. *We have the following exact sequence of R-modules,*

$$0 \to C_0(\mu; A) \to C_0(\lambda; A) \to C_0(\theta; S) \otimes_S A \to 0.$$

By (7.3), the three congruence modules $C_0(\mu; A), C_0(\lambda; A), C_0(\theta; S) \otimes_R A$ are residue rings of R; so, cyclic A-modules. Moreover they are the ring A modulo principal ideals. Write their generators as $Ac_\lambda = A \cap R \subset (R_A \oplus A)$, $Ac_\mu = A \cap S \subset (S_A \oplus A)$ and $Sc_\theta = S \cap R \subset (R_S \oplus S)$. Thus we have $C_0(\lambda; A) = A/c_\lambda A$, $C_0(\mu; A) = A/c_\mu A$ and $C_0(\theta; S) \otimes_S A = A/\overline{c}_\theta A$ for the image $\overline{c}_\theta \in A$ of $c_\theta \in S$. By the above lemma, we conclude the following result.

COROLLARY 7.6. *We have $\overline{c}_\theta \cdot c_\mu = c_\lambda$ up to units in A.*

We have a natural morphism $(\mathbb{Z}/(\mathfrak{C} \cap \mathbb{Z}))^\times \to Cl_M(\mathfrak{C})$ sending ideal (n) for an integer n prime to $\mathfrak{C}$ to its class in $Cl_M(\mathfrak{C})$, and we write $h^-(\mathfrak{C})$ for the order of cokernel of this map. Write $l(\mathfrak{l})$ for the residual characteristic of $\mathfrak{l}$. By a simple computation, we have the following lemma.

LEMMA 7.7. *Write $\mathfrak{C}$ for $\mathfrak{C}(\Psi_{\mathbb{J}})$. Then the ratio*

$$\frac{h^-(\mathfrak{C})}{h(M) \cdot \prod_{\mathfrak{l}|\mathfrak{C}, \mathfrak{l}: \text{ inert prime}} (l(\mathfrak{l}) + 1) \prod_{\mathfrak{l}|\mathfrak{C}, \mathfrak{l}: \text{ split prime with } l(\mathfrak{l}) \mid \mathfrak{C}} (l(\mathfrak{l}) - 1)}$$

is prime to p (if $p \nmid |\mathfrak{O}^\times|/2$ for the integer ring $\mathfrak{O}$ of M), where $h(M)$ is the class number of M. Thus if $\mathbb{J}$ is minimal primitive, $h^-(\mathfrak{C})$ is equal, up to units in W, to

$$h_{\mathrm{i}}(M/\mathbb{Q}) = h(M) \prod_{\mathfrak{l}|\mathfrak{C}, \mathfrak{l}: \text{ inert prime}} (l(\mathfrak{l}) + 1).$$

Since $\rho_{\mathbb{J}}$ is minimal at primes $q|N$ split in M (see Remark 7.3), the q-part $\mathfrak{C}_q(\Psi_{\mathbb{J}})$ is minimal among $\mathfrak{C}_q(\Psi_{\mathbb{J}}\xi)$ for all finite order characters ξ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$; in particular, $\mathfrak{F}_c = \mathfrak{O}$ (by Lemma 10.4). Thus no rational prime split in M divides $\mathfrak{C}$.

Remark 7.8. The number $h_{\mathrm{i}}(M/\mathbb{Q})$ is defined in [Hid09, § 1], and $h_{\mathrm{i}}(M/\mathbb{Q}) L_p(\Psi_{\mathbb{J}}^-)$ (for the element $L_p(\Psi_{\mathbb{J}}^-) \in W(\overline{\mathbb{F}}_p)[[\Gamma_M]]$ giving the Katz p-adic L-function of $\Psi_{\mathbb{J}}^-$) is computed to be a factor of the characteristic power series c_λ in [Hid09, Corollary 3.8] (or (A) in [Hid09, § 1]) assuming $p \geqslant 5$ and:

(1) primitiveness of $\mathbb{J}$ (i.e. $N = N(\mathfrak{C}(\Psi_{\mathbb{J}}))D$);
(2) local minimality at q of $\rho_{\mathbb{J}}$ as long as $\rho_{\mathbb{J}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ is reducible.

The reducibility of $\rho_{\mathbb{J}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ in (2) is equivalent to the fact that the automorphic representation generated by $f_P \in \mathcal{F}_{\mathbb{J}}$ is in the principal series at q, and in this way, the result is stated in [Hid09].

Lemma 7.9. *Let the notation and the assumption be as in Theorem 7.2. Then we have* $c_\mu = h^-(\mathfrak{C}) = h_{\mathfrak{i}}(M/\mathbb{Q})$ *up to units in* $\mathbb{J}$*. Here* $\mathfrak{C}$ *is the prime-to-*p *conductor of* $\Psi_{\mathbb{J}}$ *in (CM2).*

Proof. As explained in Remark 7.3, we have $C(\overline{\rho}) = N$ under the assumptions of Theorem 7.2. If $C(\overline{\rho}) = N = C(\rho_{\mathbb{J}})$, by Proposition 5.7, without localization, $R = \mathbb{T}$, $S = \mathbb{T}_{\mathrm{cm}}$ and $A = \mathbb{J}$ are Gorenstein rings. Since S is isomorphic to the group algebra $W[[Z_p]]$ by Proposition 5.7, the assertion follows from Lemma 1.9 and Lemma 1.11 in [Hid86c]. □

Recall the anticyclotomic Katz p-adic L-function $L_p(\Psi_{\mathbb{J}}^-)$ as in § 6. Identifying $\mathbb{J}$ with $W[[\Gamma_M]]$, $\Psi_{\mathbb{J}}^- : Z^- \to \Gamma_M$ induces a surjective algebra homomorphism $W[[Z_p^-]] \to \mathbb{J}$ and $L_p(\Psi_{\mathbb{J}}^-)$ is the image of the measure $L^-(\overline{\psi}^-)$ in Theorem 7.2. We regard $L_p(\Psi_{\mathbb{J}}^-) \in \mathbb{J}$.

Proposition 7.10. *Under the assumption of Theorem 7.2, we have* $c_\lambda = h^-(\mathfrak{C})L_p(\Psi_{\mathbb{J}}^-)$ *up to units in* $\mathbb{J}$ *for the prime-to-*p *conductor* $\mathfrak{C}$ *of* $\Psi_{\mathbb{J}}$ *in (CM2).*

This is where we need the assumption $p \geqslant 5$ in Theorem 7.2.

Proof. The fixed field $\widetilde{M}/M$ of $\mathrm{Ker}(\Psi^-)$ for $\Psi = \Psi_{\mathbb{J}}$ has Galois group $\mathrm{Gal}(\widetilde{M}/M) \cong \mathrm{Im}(\Psi^-)$. The maximal torsion-free quotient Γ_M of $\mathrm{Gal}(\widetilde{M}/M)$ is a $\mathbb{Z}_p$-free module of rank 1. Fix a decomposition $\mathrm{Gal}(\widetilde{M}/M) = \Delta \times \Gamma_M$ for the maximal finite subgroup Δ of $\mathrm{Gal}(\widetilde{M}/M)$. By Proposition 5.7, the character Ψ^- induces an algebra isomorphism $\Psi_*^- : W[[\Gamma_M]] \cong \mathbb{J}$. Then the maximal p-abelian extension $L/\widetilde{M}$ unramified outside $\mathfrak{p}$ has Galois group X which is naturally a $W[[\mathrm{Gal}(\widetilde{M}/M)]]$-module (in the standard manner of Iwasawa's theory). Let $\psi^- := \Psi^-|_\Delta$ (which has values in $W^\times$), and put $X(\psi^-) = X \otimes_{W[\Delta],\psi_*^-} W$ which is the maximal quotient of X on which Δ acts by ψ^-. Thus $X(\psi^-)$ is naturally a $\mathbb{J}$-module via Ψ_*^-, and it is known to be a torsion $\mathbb{J}$-module of finite type. Let $\mathcal{F}^-(\psi^-)$ be the Iwasawa power series in $\mathbb{J}$ of $X(\psi^-)$; i.e. the characteristic power series of $X(\psi^-)$ as a torsion $\mathbb{J}$-module of finite type (see [Hid00, p. 291] for the characteristic power series). By the proof of the main conjecture over M by Rubin [Rub88] or the proof of its anticyclotomic version by Tilouine and Mazur [Til89, MT90], we know $\mathcal{F}^-(\psi^-) = L_p(\Psi_{\mathbb{J}}^-)$ up to units in $\mathbb{J}$. By [Hid09, Corollary 3.8] (see also Remark 7.8), if $p \geqslant 5$ (and $N = N(\mathfrak{C})D$, which follows from the assumption of Theorem 7.2 as explained in Remark 7.3), we have $h^-(\mathfrak{C})L_p(\Psi_{\mathbb{J}}^-)|c_\lambda$. By [MT90] (and [HT94, Corollary 3.3.7]), we also know $c_\lambda \mid h^-(\mathfrak{C})\mathcal{F}^-(\psi^-)$. Combining all of these, we conclude the equality of the proposition. Since the residual representation $\overline{\rho}$ is absolutely irreducible, actually, the above identity is proven in [Hid09] without using the solution of the main conjecture (and in this way, the anticyclotomic main conjecture is proven in [Hid09] for general CM fields). □

Proof of Theorem 7.2. As explained in Remark 7.3, we have $C = N(\mathfrak{C})D = C(\rho_{\mathbb{J}}) = C(\overline{\rho})$ always under the assumption of the theorem. Then by Proposition 5.7, $\mathbb{T}$, $\mathbb{T}_{\mathrm{cm}}$ and $\mathbb{J}$ are all Gorenstein. By Corollary 7.6, we find that $\overline{c}_\theta = c_\lambda/c_\mu$. By Proposition 7.10, $\overline{c}_\theta = L_p(\Psi_{\mathbb{J}}^-)$ up to units in $\mathbb{J}$. Since $L^-(\overline{\psi}^-)$ has image in $\mathbb{J}$ given by $L_p(\Psi_{\mathbb{J}}^-)$ for all irreducible components $\mathrm{Spec}(\mathbb{J}) \subset \mathrm{Spec}(W[[Z_p]])$ with $\rho_{\mathbb{J}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \Psi_{\mathbb{J}}$. Thus we conclude $c_\theta = L^-(\overline{\psi}^-)$ up to units, proving (1). □

8. Level and p-adic L-functions

Throughout this section we assume the condition (R) and one of the conditions (s) and (v) above Theorem I in the introduction, although in some cases, the conditions follow from the specification of $\overline{\rho}$. Also, as before, we take the base valuation ring W sufficiently large so that

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

each irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbf{h})$ is geometrically irreducible over the quotient field $Q(W)$ of W.

Our proof heavily relies on Lemma 2.9; so, we first verify the assumptions of Lemma 2.9 under (R) and one of (s) and (v). When the condition (s) is satisfied, we replace g in (s) by $j = \lim_{n\to\infty} g^{p^n}$ and conjugating $\mathbb{G}$ by an element in $\mathcal{B}(\mathbb{I})$, we assume that $j = \left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta'\end{smallmatrix}\right)$ with $\zeta, \zeta' \in \mu_{p-1}$. If only (v) is satisfied, we take $\sigma \in D_p$ such that $\overline{\rho}(\sigma)$ has distinct two eigenvalues as in the condition (R), and put $j = \lim_{n\to\infty} g^{q^n}$ for $q = |\mathbb{F}|$; so, again we have $j = \left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta'\end{smallmatrix}\right)$ with $\zeta, \zeta' \in \mu_{q-1}$ normalizing $\mathbb{G}$ and $\rho_{\mathbb{I}}(D_p)$. Hereafter, we exclusively use the symbol j to denote the above element in $\mathrm{Im}(\rho_{\mathbb{I}})$.

Lemma 8.1. *Let $\mathbb{G} = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_{\mathbb{I}}(\mathfrak{m}_{\widetilde{\mathbb{I}}})$ for an irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbf{h})$, and write $\overline{\mathbb{G}}_{\mathfrak{P}}$ for the image of $\mathbb{G}$ in $\mathrm{SL}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$ for each prime divisor $\mathfrak{P} \in \mathrm{Spec}(\widetilde{\mathbb{I}})$. Then the $\kappa(\mathfrak{P})$-span $\bar{\mathfrak{s}}_{\mathfrak{P}}$ of $\mathcal{M}^0_n(\overline{\mathbb{G}}_{\mathfrak{P}}) = \mathcal{M}_n(\overline{\mathbb{G}}_{\mathfrak{P}}) \cap \mathfrak{sl}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$ is equal to $\mathfrak{sl}_2(\kappa(\mathfrak{P}))$ for some $n > 0$ if and only if $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$. Here we recall that $A_0 = \mathbb{Z}_p$ or $\mathbb{F}_p[[T]]$.*

Proof. By (R) and one of (s) and (v), $\mathcal{M}_n(\mathbb{G}) \cap \mathfrak{U}(\mathbb{I})$ surjects down to $\mathcal{M}_n(\overline{\mathbb{G}}_{\mathfrak{P}}) \cap \mathfrak{U}(\kappa(\mathfrak{P}))$ for all $n > 0$. Since the proof is the same for any $n > 0$, we just assume that $n = 1$. Let $P = \mathfrak{P} \cap \Lambda$. Note that $\bar{\mathfrak{n}} = \mathcal{M}_1(\overline{\mathbb{G}}_{\mathfrak{P}}) \cap \mathfrak{U}(\kappa(\mathfrak{P}))$ and $\bar{\mathfrak{n}}_t = \mathcal{M}_1(\overline{\mathbb{G}}_{\mathfrak{P}}) \cap {}^t\mathfrak{U}(\kappa(\mathfrak{P}))$ are Λ/P-modules inside $\mathfrak{sl}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$. Thus either $\bar{\mathfrak{n}} = 0$ or $\bar{\mathfrak{n}}$ is Λ/P-torsion-free of positive rank.

Suppose $\bar{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$. Then $\bar{\mathfrak{n}} \neq 0$ and $\bar{\mathfrak{n}}_t \neq 0$. This implies that $[\bar{\mathfrak{n}}, \bar{\mathfrak{n}}_t] \neq 0$ is a non-trivial torsion-free Λ/P-module of positive rank, and $\mathrm{Ad}(j)$ acts trivially on $[\bar{\mathfrak{n}}, \bar{\mathfrak{n}}_t]$. Thus $\mathcal{M}^0_1(\overline{\mathbb{G}}_{\mathfrak{P}})$ must contain an open Lie-subalgebra of $\mathfrak{sl}_2(A_0)$ (see § 2, Corollary 2.3 and Lemma 2.4); so, $\bar{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$. Since

$$[\mathcal{M}^0_1(\overline{\mathbb{G}}_{\mathfrak{P}}), \mathcal{M}^0_1(\overline{\mathbb{G}}_{\mathfrak{P}})] \subset \mathcal{M}^0(\overline{\mathbb{G}}_{\mathfrak{P}}),$$

$\mathcal{M}^0(\overline{\mathbb{G}}_{\mathfrak{P}})$ (and actually $\mathcal{M}^0_n(\overline{\mathbb{G}}_{\mathfrak{P}})$ for each $n > 0$) span $\mathfrak{sl}_2(\kappa(\mathfrak{P}))$ over $\kappa(\mathfrak{P})$. Then the intersection $\overline{\mathbb{G}}'_{\mathfrak{P}} = \mathrm{SL}_2(\kappa(\mathfrak{P})) \cap (1 + \mathcal{M}(\overline{\mathbb{G}}_{\mathfrak{P}}))$ contains an open subgroup of $\mathrm{SL}_2(A_0)$. The converse is plain as $\mathfrak{sl}_2(A_0)$ contains a basis of $\mathfrak{sl}_2(\kappa(\mathfrak{P}))$ over $\kappa(\mathfrak{P})$. □

Hereafter, suppose that $\mathbb{I}$ is a non-CM component of $\mathbf{h}$. Let $\mathrm{Spec}(\mathbb{T}) \subset \mathrm{Spec}(\mathbf{h})$ be a connected component containing $\mathrm{Spec}(\mathbb{I})$. Let $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(Q(\mathbb{T}))$ be the associated Galois representation. We write $\overline{\rho} = \rho_{\mathfrak{m}_{\mathbb{T}}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ with $\mathbb{F} = \mathbb{T}/\mathfrak{m}_{\mathbb{T}}$ associated to the maximal ideal $\mathfrak{m}_{\mathbb{T}}$ of $\mathbb{T}$. We would like to relate the global level $L = L(\mathbb{I})$ of $\rho_{\mathbb{I}}$ (defined in § 3) with a certain p-adic L-function. By a result of Ribet [Rib85] combined with Proposition 5.1 in the text, $\mathrm{Im}(\rho_{\mathfrak{P}})$ contains an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ up to conjugation. Then by Theorem 2.12, we can pick a representation $\rho \in [\rho_{\mathbb{I}}]$ with values in $\mathrm{GL}_2(\widetilde{\mathbb{I}})$ such that $\mathrm{Im}(\rho) \supset \Gamma(\mathfrak{c})$ with non-trivial $\mathfrak{c}$. If $\overline{\rho}$ is absolutely irreducible, by Theorem 2.12, the global level $L = L(\mathbb{I})$ described just above Lemma 3.3 is well defined. If $\overline{\rho}$ is reducible, assuming the assumption of Lemma 3.5, we pick ρ in the $\mathbb{I}$-isomorphism class made out of $\mathcal{L}_{\mathrm{can}}(\mathbb{I})$ and define $L(\mathbb{I})$ as described after the statement of Lemma 3.5 before its proof. We start with a version of results in [MW86, § 10] and Fischman [Fis02].

Theorem 8.2. *Suppose $\mathrm{Im}(\overline{\rho})$ contains $\mathrm{SL}_2(\mathbb{F}_p)$ for $p \geqslant 7$. Then the global level $L = L(\mathbb{I})$ of $\rho_{\mathbb{I}}$ for every irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbb{T})$ is equal to 1.*

The assertion (1) in Theorem II in the introduction follows from this theorem. By the theory of pseudo representation, we can find a unique $\rho_{\mathbb{T}}$ with values in $\mathrm{GL}_2(\mathbb{T})$ up to isomorphism. Thus we could assume that $\rho_{\mathbb{I}}$ has values in $\mathrm{GL}_2(\mathbb{I})$, though we do not do this.

Proof. Similarly to the proof of Lemma 3.1, writing $\overline{g}$ for the image of $g \in \mathrm{Im}(\rho_{\mathbb{I}})$ in $\mathrm{GL}_2(\widetilde{\mathbb{I}}/\mathfrak{m}_{\widetilde{\mathbb{I}}})$, let

$$\mathbb{K} := \{g \in \mathrm{Im}(\rho_{\mathbb{I}}) \mid \det(g) \in \Gamma\}, \quad \mathbb{L} = \{g \in \mathbb{K} \mid \overline{g} \in \mathcal{U}(\mathbb{F})\} \quad \text{and} \quad \mathbb{H} = \{g \in \mathbb{K} \mid \overline{g} = 1\}$$

for $\Gamma = \{t^s \mid s \in \mathbb{Z}_p\} \subset \Lambda^{\times}$. By the existence of j, similarly to the proof of Lemma 1.4, from (Gal), we find $\tau \in \rho_{\mathbb{I}}(D_p) \cap \mathbb{H}$ such that $\tau = \left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then by (Det) in § 3, the three sets $\mathrm{Im}(\rho_{\mathbb{I}})/\mathbb{K}$, $\mathrm{Im}(\rho_{\mathbb{I}})/\mathbb{L}$ and $\mathrm{Im}(\rho_{\mathbb{I}})/\mathbb{H}$ are finite sets. Then for $\mathcal{T}' = \{\tau^s \mid s \in \mathbb{Z}_p\}$, we have $\mathbb{H} = \mathcal{T}' \ltimes \mathbb{G}$ for $\mathbb{G} = \mathbb{H} \cap \mathrm{SL}_2(\widetilde{\mathbb{I}})$, $\mathbb{K} = \mathcal{T}' \ltimes \mathbb{K}^1$ for $\mathbb{K}^1 = \mathbb{K} \cap \mathrm{SL}_2(\widetilde{\mathbb{I}})$ and $\mathbb{L} = \mathcal{T}' \ltimes \mathbb{L}^1$ for $\mathbb{L}^1 = \mathbb{L} \cap \mathrm{SL}_2(\widetilde{\mathbb{I}})$ (see the proof of Lemma 3.1). Similarly, for the image $\overline{\mathcal{T}}'_{\mathfrak{a}}$ (respectively $\overline{\mathbb{H}}_{\mathfrak{a}}$, $\overline{\mathbb{K}}_{\mathfrak{a}}$, $\overline{\mathbb{L}}_{\mathfrak{a}}$, $\overline{\mathbb{L}}^1_{\mathfrak{a}}$, $\overline{\mathbb{G}}_{\mathfrak{a}}$ and $\overline{\mathbb{K}}^1_{\mathfrak{a}}$) of $\mathcal{T}'$ (respectively $\mathbb{H}$, $\mathbb{K}$, $\mathbb{L}$, $\mathbb{L}^1$, $\mathbb{G}$ and $\mathbb{K}^1$) in $\mathrm{GL}_2(\widetilde{\mathbb{I}}/\mathfrak{a})$ for any $\widetilde{\mathbb{I}}$-ideal $\mathfrak{a}$, we have $\overline{\mathbb{H}}_{\mathfrak{a}} = \overline{\mathcal{T}}'_{\mathfrak{a}} \ltimes \overline{\mathbb{G}}_{\mathfrak{a}}$, $\overline{\mathbb{L}}_{\mathfrak{a}} = \overline{\mathcal{T}}'_{\mathfrak{a}} \ltimes \overline{\mathbb{L}}^1_{\mathfrak{a}}$ and $\overline{\mathbb{K}}_{\mathfrak{a}} = \overline{\mathcal{T}}'_{\mathfrak{a}} \ltimes \overline{\mathbb{K}}^1_{\mathfrak{a}}$. Thus the reduction maps $\mathbb{G} \to \overline{\mathbb{G}}_{\mathfrak{a}}$, $\mathbb{L}^1 \to \overline{\mathbb{L}}^1_{\mathfrak{a}}$ and $\mathbb{K}^1 \to \overline{\mathbb{K}}^1_{\mathfrak{a}}$ given by $g \mapsto (g \bmod \mathfrak{a})$ are all surjective. In particular, by our assumption, $\overline{\mathbb{K}}^1 := \overline{\mathbb{K}}^1_{\mathfrak{m}_{\widetilde{\mathbb{I}}}}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$.

We prove $P \nmid L(\mathbb{I})$ for all prime divisors of Λ, which shows $L(\mathbb{I}) = 1$. Take a prime divisor $\mathfrak{P}$ of $\widetilde{\mathbb{I}}$ above P. Suppose that $\overline{\mathbb{K}}^1_{\mathfrak{P}}$ is a finite group. This is equivalent to assuming $\overline{\mathbb{G}}_{\mathfrak{P}}$ is finite since $\mathbb{K}^1/\mathbb{G} \cong \mathbb{K}/\mathbb{H} \hookrightarrow \mathrm{Im}(\rho_{\mathbb{I}})/\mathbb{H}$ is finite. Thus $\overline{\mathbb{K}}^1_{\mathfrak{P}}$ is a finite group whose image modulo $\mathfrak{m}_{\widetilde{\mathbb{I}}}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. By the classification of finite subgroups of $\mathrm{PGL}_2(K)$ for a characteristic 0 field K, if $p \geqslant 7$ and $\kappa(P)$ has characteristic 0, there is no finite subgroup of $\mathrm{SL}_2(\kappa(\mathfrak{P}))$ whose image in $\mathrm{SL}_2(\mathbb{F})$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. This point is also plain if $p \geqslant 7$ as $\mathrm{SL}_2(\mathbb{F}_p)$ with $p \geqslant 7$ does not have two-dimensional representations over K (see [Sch07, p. 128]). We conclude that $\overline{\mathbb{G}}_{\mathfrak{P}}$ is infinite if $p \geqslant 7$ and $\kappa(P)$ has characteristic 0. If $\kappa(P)$ has characteristic p, $\overline{\mathbb{L}}^1_{\mathfrak{P}}$ is still infinite. To see this, note that $\overline{\mathbb{L}}^1_{\mathfrak{m}_{\widetilde{\mathbb{I}}}}$ contains $\mathcal{U}(\mathbb{F}_p)$; so, $\overline{\mathbb{L}}^1_{\mathfrak{P}}$ contains an element whose reduction modulo $\mathfrak{m}_{\widetilde{\mathbb{I}}/\mathfrak{P}}$ is non-zero unipotent. Such an element under conjugation by $\overline{\mathcal{T}}'_{\mathfrak{P}}$ produces infinitely many elements. Then the open subgroup $\overline{\mathbb{G}}_{\mathfrak{P}}$ of $\overline{\mathbb{L}}^1_{\mathfrak{P}}$ has infinitely many elements. Therefore $\mathcal{M}^0_1(\overline{\mathbb{G}}_{\mathfrak{P}})$ is an infinite Lie algebra.

Let $\widetilde{\mathfrak{s}}_{\mathfrak{P}}$ be the Lie subalgebra of $\mathfrak{sl}_2(\widetilde{\mathbb{I}}/\mathfrak{P})$ generated by $\mathcal{M}^0_1(\overline{\mathbb{G}}_{\mathfrak{P}})$ over $\widetilde{\mathbb{I}}/\mathfrak{P}$. Since $\overline{\mathbb{G}}_{\mathfrak{P}}$ is infinite, $\widetilde{\mathfrak{s}}_{\mathfrak{P}}$ is non-trivial. Since $p \geqslant 5$, the adjoint representation of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\mathfrak{sl}_2(\mathbb{F}_p)$ is absolutely irreducible. Thus the quotient $\widetilde{\mathfrak{s}}_{\mathfrak{P}}/\mathfrak{m}_{\widetilde{\mathbb{I}}} \cdot \widetilde{\mathfrak{s}}_{\mathfrak{P}} = \widetilde{\mathfrak{s}}_{\mathfrak{P}} \otimes_{\widetilde{\mathbb{I}}} \mathbb{F}$ ($\mathbb{F} = \widetilde{\mathbb{I}}/\mathfrak{m}_{\widetilde{\mathbb{I}}}$) is isomorphic to a three-dimensional irreducible subspace in $\mathfrak{sl}_2(\mathbb{F})$ over $\mathbb{F}$ under the adjoint action of $\mathbb{K}^1$. By Nakayama's lemma, $\widetilde{\mathfrak{s}}_{\mathfrak{P}}$ has at least rank 3 over $\widetilde{\mathbb{I}}/\mathfrak{P}$; so, the $\kappa(\mathfrak{P})$-span $\overline{\mathfrak{s}}_{\mathfrak{P}} := \kappa(\mathfrak{P}) \cdot \widetilde{\mathfrak{s}}_{\mathfrak{P}}$ is equal to $\mathfrak{sl}_2(\kappa(\mathfrak{P}))$. By Lemma 8.1, $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ in $\mathrm{SL}_2(\kappa(\mathfrak{P}))$. Hence, by Theorem 2.12(2) and Corollary 3.4, we conclude $P \nmid (L(\mathbb{I}))$. □

Remark 8.3. In the setting of the above theorem, assume $p = 5$. Again by Schur, the unique absolutely irreducible two-dimensional representation over $\overline{\mathbb{Q}}_5$ of $\mathrm{SL}_2(\mathbb{F}_5)$ can be only defined over the integer ring of the field $\mathbb{Q}_5[\sqrt{5}]$. Since we have $\Lambda/P \cong \mathbb{Z}_5[\mu_5]$ for $P = ((t^5 - 1)/T) \subset \Lambda$, we have a subgroup H in $\mathrm{SL}_2(\Lambda/P)$ whose reduction modulo the maximal ideal is isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)$. Therefore $G = \{x \in \mathrm{SL}_2(\Lambda) \mid x \bmod P \in H\}$ has $(G \bmod \mathfrak{m}) = \mathrm{SL}_2(\mathbb{F}_5)$ but the level of G is P.

We now deal with the case where the image of $\overline{\rho}$ does not contain $\mathrm{SL}_2(\mathbb{F}_p)$. We start with the case of dihedral image of $\overline{\rho}$. Let κ be a local field. Write O for the maximal compact subring of κ. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(O)$ be a continuous Galois representation and put $G = \mathrm{Im}(\rho) \cap \Gamma_O(\mathfrak{m}_O)$. We write $\mathfrak{s}$ for the κ-span of the Lie algebra $\mathcal{M}^0_1(G) = \mathcal{M}_1(G) \cap \mathfrak{sl}_2(G)$.

Lemma 8.4. *Let the notation be as above. Suppose either that $\mathfrak{s}$ is a Cartan subalgebra of $\mathfrak{sl}(2)$ or that $\mathrm{Im}(\rho)$ modulo center is a finite dihedral group. If ρ is absolutely irreducible, there exists*

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

a quadratic field $M/\mathbb{Q}$ and a character $\theta : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \overline{\kappa}^\times$ such that $\rho \cong \mathrm{Ind}_M^{\mathbb{Q}} \theta$ and $\theta^c \neq \theta$, where $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ restricted to M is the generator of $\mathrm{Gal}(M/\mathbb{Q})$ and $\theta^c(\sigma) = \theta(c\sigma c^{-1})$.

This follows from Lemma 2.1 if κ has characteristic 0. We give here a different proof.

Proof. In any case, the group $\mathrm{Im}(\rho)$ is in the normalizer of a Cartan subalgebra $\mathfrak{H}$ ($\mathfrak{H} = \mathfrak{s}$ if $\mathfrak{s}$ is a Cartan subalgebra). By extending scalars κ, we may assume that $\mathfrak{H}$ is a split Cartan subalgebra. Then, we can find an open normal subgroup $H \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\rho|_H$ is isomorphic to the direct sum of two abelian characters. Set $\rho_H = \rho|_H$; then, ρ_H is completely reducible. Write $\rho_H = \left(\begin{smallmatrix}\theta & 0\\ 0 & \delta\end{smallmatrix}\right)$. Since ρ extends ρ_H, $g \mapsto \rho_H^h(g) := \rho_H(hgh^{-1}) = \rho(h)\rho_H(g)\rho(h)^{-1}$ is equivalent to ρ_H for all $h \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\{\delta, \theta\}$ by inner conjugation. Indeed,

$$\begin{pmatrix}\theta^h & 0\\ 0 & \delta^h\end{pmatrix} \cong \rho(h)\begin{pmatrix}\theta & 0\\ 0 & \delta\end{pmatrix}\rho(h)^{-1}. \tag{8.1}$$

Let $\Delta \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the stabilizer of δ. Then $M = \overline{\mathbb{Q}}^\Delta$ is at most a quadratic extension of $\mathbb{Q}$. If $M = \mathbb{Q}$ and W is sufficiently large, the two characters extend to $\delta, \theta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{I}^\times$ (e.g. [Hid11a, § 5.1.1] or [Hid00, § 4.3.5]), and $\rho^{ss} = \delta \oplus \theta$, which cannot happen as ρ is absolutely irreducible. Then $[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \Delta] = 2$ and by Frobenius reciprocity, $\rho \cong \mathrm{Ind}_M^{\mathbb{Q}} \delta \cong \mathrm{Ind}_M^{\mathbb{Q}} \theta$ for the quadratic extension $M = \overline{\mathbb{Q}}^\Delta$ of $\mathbb{Q}$. We therefore have $\rho|_\Delta = \theta \oplus \theta^c$, and irreducibility of ρ implies $\theta \neq \theta^c$. □

For a character φ of $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ with an imaginary quadratic field M, we recall its anticyclotomic projection φ^- given by $\sigma \mapsto \varphi(\sigma)\varphi(c\sigma c^{-1})^{-1}$. Let $\mathbb{I}$ be a minimal primitive non-CM component of $\mathbf{h}$ with $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$ for an imaginary quadratic field M in which p splits into $\mathfrak{p}\overline{\mathfrak{p}}$ and a character $\overline{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \overline{\mathbb{F}}_p$ unramified at $\overline{\mathfrak{p}}$. Under the assumption (a) or (b) in Theorem 7.2, $\mathbb{T}^M_{\mathrm{cm}}$ is non-trivial. Pick one such CM component $\mathbb{J}$ of $\mathbb{T}^M_{\mathrm{cm}}$, and write $\mathfrak{C}$ for the prime-to-p conductor of $\Psi_{\mathbb{J}}$. Let $\mathfrak{c}' = \mathfrak{C} \cap \overline{\mathfrak{C}}$, and write $\mathfrak{c}$ for the prime-to-p conductor of $\overline{\psi}^-$ (so, $\mathfrak{c} \mid \mathfrak{c}'$). Assuming $W \supset W(\overline{\mathbb{F}}_p)$, we recall the anticyclotomic Katz measure $L^-(\overline{\psi}^-) \in W[[Z_p^-]]$ as in Theorem 7.2. The natural inclusion $\mathbb{Z}_p^\times \hookrightarrow \mathfrak{O}_{\mathfrak{p}}$ induces $\Gamma \hookrightarrow \Gamma_M \cong \Gamma_M^- \subset Z_p^-$, and hence $W[[Z_p^-]]$ is naturally a Λ_W-algebra for $\Lambda_W = W[[T]] = W[[\Gamma]]$. Since $W[[Z_p^-]]$ is free of finite rank r over Λ_W for the index $r = (Z_p^- : \Gamma)$, we have a regular representation Φ of $W[[Z_p^-]]$ into the $r \times r$ matrix algebra $M_r(\Lambda_W)$, and for $\alpha \in W[[Z_p^-]]$, we define its norm $N_{W[[Z_p^-]]/\Lambda_W}(\alpha) = \det(\Phi(\alpha))$. Define $L^-_{\overline{\psi}} = N_{W[[Z_p^-]]/\Lambda_W}(L^-(\overline{\psi}^-))$. This is the element we meant in Theorem II by the product of anticyclotomic Katz L-functions with a given mod p branch character. We also recall that we defined in (7.1) an element $E_{1,N} \in \mathbb{J}$.

Theorem 8.5. *Let the notation be as above; in particular, let $\mathbb{I}$ be a minimal primitive non-CM component with $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$ for an imaginary quadratic field M as above. Take a large $W \supset W(\overline{\mathbb{F}}_p)$ so that each irreducible component of $\mathrm{Spec}(\mathbb{T})$ is geometrically irreducible. Assume $p \geqslant 5$, and suppose further that $\overline{\psi}^-$ has order > 2, $\overline{\psi}$ ramifies at $\mathfrak{p}$, and one of the following conditions holds:*

(a) *$p \nmid \varphi(N)$ and $C(\overline{\rho}) = N$;*
(b) *$p \nmid \Phi(N)$ for the Euler function Φ of M and $E_{1,N} \notin \mathfrak{m}_{\mathbb{J}}$ for $E_{1,N}$ in (7.1).*

Then for the product $L^-_{\overline{\psi}^-} = N_{W[[Z_p^-]]/\Lambda_W}(L^-(\overline{\psi}^-))$, the global level $L(\mathbb{I})$ of a non-CM component $\mathbb{I}$ of $\mathbb{T}$ is a factor of $(L^-_{\overline{\psi}^-})^2$ in Λ_W. If $L^-_{\overline{\psi}^-}$ is a non unit in Λ_W, for any prime divisor P of $L^-_{\overline{\psi}^-}$, there exists a non-CM component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{T})$ such that $P_\Lambda \mid L(\mathbb{I})$ for $P_\Lambda = P \cap \Lambda$.

The assumption (a) is the one made in Theorem II (3b) in the introduction, and therefore, this theorem proves the assertion (3b) of Theorem II (where cube-freeness of N is assumed but it is not necessary in this residually induced case; see Remark 7.3). An important feature of this theorem is that only (the p-adic L-function part of) the congruence ideal between CM and a given non-CM component $\mathbb{I}$ shows up as the level of $\rho_{\mathbb{I}}$. Therefore congruence between non-CM components and $\mathbb{I}$ does not have direct involvement to the level $L(\mathbb{I})$.

Here are a sketch of the proof and a summary of how we use the listed assumptions in the proof. Since $\overline{\psi}$ ramifies at $\mathfrak{p}$, by Theorem 7.1, $\mathcal{L}_{\mathrm{can}}(\mathbb{I}) \cong \mathbb{I}^2$; so, $\rho_{\mathbb{I}}$ realized on $\mathcal{L}_{\mathrm{can}}(\mathbb{I})$ has values in $\mathrm{GL}_2(\mathbb{I})$. Thus we do not need to take $\widetilde{\mathbb{I}}$, and we work with $\mathbb{I}$ instead of $\widetilde{\mathbb{I}}$. Since $C(\overline{\rho}) \mid N$, by Proposition 5.7, $\mathbb{T}^M_{\mathrm{cm}}$ is non-trivial. The condition that $\overline{\psi}^-$ has order > 2 ramified at p is equivalent to the fact that $\overline{\rho}$ is not isomorphic to $\mathrm{Ind}^{\mathbb{Q}}_{M'} \overline{\psi}'$ for any quadratic fields M' other than M (Proposition 5.2); thus, we have $\mathbb{T}_{\mathrm{cm}} = \mathbb{T}^M_{\mathrm{cm}}$. As seen in Proposition 5.7, we have $\mathbb{T}_{\mathrm{cm}} = \mathbb{T}^M_{\mathrm{cm}} \cong W[[Z_p]]$ for the p-profinite part of the class group $Z = CL_M(\mathfrak{C}p^\infty)$. Note that $W[[Z_p]] \cong W[[Z_p^-]]$ canonically by Lemma 5.6. The assumption (a) or (b) is used to identify $\mathbb{T}_{\mathrm{cm}}$ (or its localization) with (possibly a localization of) the group algebra $W[[Z_p]] \cong W[[Z_p^-]]$ that enables us to identify the congruence power series of $\mathbb{J}$ inside $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ with the class number $h^-(\mathfrak{C})$ and that in $\mathrm{Spec}(\mathbb{T})$ with $h^-(\mathfrak{C})L_p(\Psi_{\mathbb{J}}^-)$ (see the later half of § 7). In other words, the congruence between CM and non-CM components only involves prime factors of $L^-(\overline{\psi}^-)$ (which is basically the product of $L_p(\Psi_{\mathbb{J}}^-)$ over irreducible components $\mathrm{Spec}(\mathbb{J})$ of $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$).

To make this fact more precise, write an irreducible component of $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ as $\mathrm{Spec}(\mathbb{J})$. If Z_p^- is pro-cyclic, $W[[Z_p^-]]$ is an integral domain and hence $\mathbb{J} \cong W[[Z_p]] = \mathbb{T}_{\mathrm{cm}}$. Note that non-pro-cyclicity of Z_p^- implies $p \mid h^-(\mathfrak{C})$ (but not necessarily the converse). Thus the congruence between $\mathbb{T}_{\mathrm{cm}} = \mathbb{J}$ and the non-CM component $\mathbb{I}$ is given simply by the anticyclotomic Katz p-adic L-function $L_p(\Psi_{\mathbb{J}}^-) = L^-(\overline{\psi}^-)$ when Z_p is pro-cyclic. The complete-intersection property of $\mathbb{T}_{\mathrm{cm}} \cong W[[Z_p]]$ proved in Lemma 5.5 will be used to compute the congruence between the non-CM component $\mathbb{I}$ and $\mathbb{T}_{\mathrm{cm}}$ when Z_p is not pro-cyclic. Roughly speaking, by Theorem 7.2, the complete intersection property of $W[[Z_p]] \cong \mathbb{T}_{\mathrm{cm}}$ tells us that the congruence between $\mathbb{T}_{\mathrm{cm}}$ and its complement $\mathbb{T}^\perp_{\mathrm{cm}}$ is just made of the anticyclotomic Katz p-adic L-function, though the congruence between $\mathbb{J}$ and its complement $\mathbb{J}^\perp$ involves $h^-(\mathfrak{C})$ in addition to (the product of) the anticyclotomic Katz p-adic L-function $L^-(\overline{\psi}^-)$. As in Remark 7.3:

(1) minimality of $\mathbb{I}$ implies minimality of $\rho_{\mathbb{J}}$ at primes q in N where $\rho_{\mathbb{J}}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)}$ is reducible;

(2) the condition (b) actually implies (a), and $\mathbb{T}$ is reduced by Lemma 5.4(1);

(3) any CM component $\mathbb{J}$ of $\mathbb{T}^M_{\mathrm{cm}}$ is primitive.

In the computation of congruence modules (in Theorem 7.2) between $\mathbb{J}$ and its complement $\mathbb{J}^\perp$ and between $\mathbb{T}_{\mathrm{cm}}$ and $\mathbb{T}^\perp_{\mathrm{cm}}$ (i.e. determination of $\mathrm{Spec}(\mathbb{J}) \cap \mathrm{Spec}(\mathbb{J}^\perp)$ and $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}) \cap \mathrm{Spec}(\mathbb{T}^\perp_{\mathrm{cm}})$), we needed these properties (see Remark 7.8 for the necessity of these properties). Then by the relation in Corollary 7.6, we computed in Theorem 7.2 the characteristic element of $C := \mathbb{T}_{\mathrm{cm}} \otimes_{\mathbb{T}} \mathbb{T}^\perp_{\mathrm{cm}}$ in $\mathbb{T}_{\mathrm{cm}} = W[[Z_p^-]]$ as the Katz measure without the class number factor. Hence, we are able to prove, by Galois deformation theory, that any (non-CM) component $\mathbb{I}$ in $\mathbb{T}^\perp_{\mathrm{cm}}$ has some points P having ρ_P isomorphic to an induced representation from M (i.e. $P|L(\mathbb{I})$) if and only if P is in $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}) \cap \mathrm{Spec}(\mathbb{T}^\perp_{\mathrm{cm}})$ (i.e. P is a factor of the Katz p-adic L-function $L^-_{\overline{\psi}^-}$).

Now, for simplicity, suppose $\mathbb{I} = \Lambda$. Then $\rho_P = (\rho_{\mathbb{I}} \bmod P)$ is isomorphic to an induced representation $\mathrm{Ind}_M^{\mathbb{Q}} \theta$; thus we have that the adjoint square $\mathrm{Ad}(\rho_P)$ of ρ_P is isomorphic to a reducible representation $(\frac{M/\mathbb{Q}}{}) \oplus \mathrm{Ind}_M^{\mathbb{Q}} \theta^-$ with $\mathrm{Ind}_M^{\mathbb{Q}} \theta^-$ absolutely irreducible. In this sketch, suppose further for simplicity that P is exactly the annihilator $\mathrm{Ann}_{\mathbb{I}_P}$ in $\mathbb{I}_P$ of the $\mathbb{I}_P$-part $C \otimes_{\mathbb{T}} \mathbb{I}_P$ of the congruence module C (in other words, $C \otimes_{\mathbb{T}} \mathbb{I}_P \cong \mathbb{I}_P/P\mathbb{I}_P$). Then we show that the P-localized Lie algebra of $\mathcal{M}_1^0(\mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_{\mathbb{I}}(P^2))$ has three independent generators over $\mathbb{I}_P$; so, $L(\mathbb{I})\mathbb{I}_P \mid P^2\mathbb{I}_P$.

Recall our simplifying assumption $\mathbb{I} = \Lambda$. Writing $V = \Lambda_P^2$ for the space of $\rho_{\mathbb{I}}$ and

$$\mathfrak{sl}(V) = \{x \in \mathrm{End}_\Lambda(V) \mid \mathrm{Tr}(x) = 0\},$$

the Λ_P-span $\mathfrak{s}_P$ of $\mathcal{M}_1^0(G) = \mathcal{M}_1(G) \cap \mathfrak{sl}(V)$ (for $G = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_\Lambda(\mathfrak{m}_\Lambda)$) is a Lie Λ_P-subalgebra of $\mathfrak{sl}(V)$ stable under the adjoint action. Define Galois modules $V_P(m) := (\mathfrak{s}_P \cap P^m\mathfrak{sl}(V))/(\mathfrak{s}_P \cap P^{m+1}\mathfrak{sl}(V))$ (for $m \geqslant 1$) under the adjoint action. Note that $\mathbb{I}_P = \Lambda_P$ is a discrete valuation ring. Choosing a generator ϖ of P and dividing $X \in \mathfrak{s}_P \cap P^m\mathfrak{sl}(V)$ by ϖ^m, this Galois module $V_P(m)$ can also be embedded into $\mathfrak{sl}(V/PV) = \mathfrak{sl}_2(\kappa(P))$ as a Galois module. Note that $\mathfrak{sl}(V/PV) \cong \mathrm{Ad}(\rho_P) \cong (\frac{M/\mathbb{Q}}{}) \oplus \mathrm{Ind}_M^{\mathbb{Q}} \theta^-$ under the adjoint action of the Galois group. Thus, if non-trivial, $\dim_{\kappa(P)} V_P(m)$ is either 1, 2 or 3, and we have three possibilities of the isomorphism class of the Galois module $V_P(1)$ under the adjoint action of $\rho_{\mathbb{I}}$: (i) $\mathrm{Ad}(\rho_P)$, (ii) $(\frac{M/\mathbb{Q}}{})$ or (iii) $\mathrm{Ind}_M^{\mathbb{Q}} \theta^-$. Indeed, by definition, $V_P(1)$ has a Galois equivariant embedding into $\mathfrak{sl}_2(\kappa(P)) = \mathrm{Ad}(\rho_P)$. Since $\mathrm{Ad}(\rho_P) \cong (\frac{M/\mathbb{Q}}{}) \oplus \mathrm{Ind}_M^{\mathbb{Q}} \theta^-$ as Galois modules, we have only three possibilities as above. In case (i), plainly $\mathrm{Ann}_{\Lambda_P} = P\Lambda_P$ and $P\Lambda_P = L(\Lambda)\Lambda_P$, and we are done.

Note that $G := \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_{\mathbb{I}}(\mathfrak{m}_{\mathbb{I}})$ is p-profinite and does not contain any order 2 element (complex conjugation). Therefore, we can take a basis of V so that the image of G in $\mathrm{GL}_2(\mathbb{I}/P)$ is diagonal with respect to this basis. In other words, taking $j = \rho(\sigma)$ for $\sigma \in D_p$ satisfying the condition (1) of Lemma 2.9, the chosen basis is an eigenbasis with respect to $j = \rho(\sigma)$. If we are in case (ii), the image G_{P^2} of G in $\mathrm{GL}_2(\Lambda/P^2)$ is diagonal, which implies that $\rho_{\mathbb{I}} \bmod P^2$ is an induced representation from M. By Galois deformation theory, we conclude $P^2\mathbb{I}_P \supset \mathrm{Ann}_{\mathbb{I}_P} = P\mathbb{I}_P$, a contradiction. In case (iii), $V_P(1)$ has to contain an anti-diagonal element non-trivial modulo P^2 (and hence, nilpotent elements non-trivial modulo P^2). Thus with respect to our chosen basis, taking an a-eigenvector, writing three (distinct) eigenvalues of $\mathrm{Ad}(j)$ as $a, 1, a^{-1}$, we have $X = \left(\begin{smallmatrix} 0 & u \\ 0 & 0 \end{smallmatrix}\right) \in (\mathfrak{s}_P \cap P\mathfrak{sl}(V))$ with $u \not\equiv 0 \bmod P^2$ and taking a^{-1}-eigenvector, $Y = \left(\begin{smallmatrix} 0 & 0 \\ v & 0 \end{smallmatrix}\right) \in (\mathfrak{s}_P \cap P\mathfrak{sl}(V))$ with $v \not\equiv 0 \bmod P^2$. Then $[X, Y]$ produces an $\mathrm{Ad}(j)$-fixed vector in $\mathfrak{s}_P \cap P^2\mathfrak{sl}(V)$ non-trivial modulo P^3. Thus $\mathfrak{s}_P \cap P^2\mathfrak{sl}(V)$ has rank 3 over $\mathbb{I}_P$, and hence $P^2\mathbb{I}_P = L(\mathbb{I})\mathbb{I}_P$, and we are done. If $P^m\mathbb{I}_P = \mathrm{Ann}_{\mathbb{I}_P}$ with $m > 1$, then basically replacing P in the above argument by P^m (P^2 by P^{m+1} and $V_P(1)$ by $V_P(m)$), we get the result. Note that $\mathrm{Spec}(\mathbb{I}/\mathrm{Ann}_{\mathbb{I}}) = \mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}) \cap \mathrm{Spec}(\mathbb{I})$ for the annihilator $\mathrm{Ann}_{\mathbb{I}}$ of C; so, it is the congruence ideal between $\mathrm{Spec}(\mathbb{I})$ and all other CM components.

We have shown locally, in case (i) the congruence ideal is equal to the level ideal $(L(\mathbb{I}))$, and in case (iii), the square of the congruence ideal is equal to the level ideal. Case (ii) does not occur. As suggested by the referee, we note that the cohomological congruence ideal is actually the square of the congruence ideal of the Hecke algebra (as the étale cohomology group of modular curves is free of rank 2 over the Hecke algebra under an appropriate Gorenstein condition). We now give a detailed proof for general $\mathbb{I} \supset \Lambda$.

Proof. As explained above in the sketch, we have $\mathbb{T}_{\mathrm{cm}} = \mathbb{T}_{\mathrm{cm}}^M$ is non-trivial. Since $\mathbb{I}$ is a non-CM component of $\mathbb{T}$, we have $\mathbb{T} \neq \mathbb{T}_{\mathrm{cm}}$. Since $\overline{\rho}$ is absolutely irreducible, under (R), $\mathbb{T}$ is Gorenstein,

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

and hence $\rho_{\mathbb{T}}$ realized on $\mathcal{L}_{\mathrm{can}}(\mathbb{T})$ has values in $\mathrm{GL}_2(\mathbb{T})$; so, $\rho_{\mathbb{I}}$ realized on $\mathcal{L}_{\mathrm{can}}(\mathbb{I})$ has values in $\mathrm{GL}_2(\mathbb{I})$ and $\rho_{\mathbb{I}}|_{D_p} \subset \mathcal{B}(\mathbb{I})$ with (Gal) satisfied (thus ($\mathrm{F}_{\mathrm{can}}$) is satisfied). Let $\mathbb{G} = \mathrm{Im}(\rho_{\mathbb{I}}) \cap \Gamma_{\mathbb{I}}(\mathfrak{m}_{\mathbb{I}})$, and write $\rho_{\mathfrak{P}} = (\rho_{\mathbb{I}} \bmod \mathfrak{P})$ for a prime $\mathfrak{P} \in \mathrm{Spec}(\mathbb{I})$.

Now pick a prime divisor $P \in \mathrm{Spec}(\Lambda)$ and a prime divisor $\mathfrak{P} \in \mathrm{Spec}(\mathbb{I})$ above P. We consider the Lie algebra $\bar{\mathfrak{s}}_{\mathfrak{P}}$ of $\overline{\mathbb{G}}_{\mathfrak{P}} = (\mathbb{G} \bmod \mathfrak{P})$; i.e. we write $\bar{\mathfrak{s}}_{\mathfrak{P}}$ for the $\kappa(\mathfrak{P})$-span of $\mathcal{M}_1^0(\overline{\mathbb{G}}_{\mathfrak{P}})$. There are the following five possibilities:

(O) $\bar{\mathfrak{s}}_{\mathfrak{P}} = 0$;

(C) $\bar{\mathfrak{s}}_{\mathfrak{P}}$ is a Cartan subalgebra $\mathfrak{H}$;

(N) $\bar{\mathfrak{s}}_{\mathfrak{P}}$ is a non-zero nilpotent subalgebra;

(B) $\bar{\mathfrak{s}}_{\mathfrak{P}}$ is a Borel subalgebra;

(F) $\bar{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$.

If we are in case (F) for all $\mathfrak{P}|P$, by Lemma 3.1 combined with Lemma 8.1, $\overline{\mathbb{G}}_{\mathfrak{P}}$ contains an open subgroup of $\mathrm{SL}_2(A_0)$ for all $\mathfrak{P}|P$, and we have $\mathfrak{P}\nmid L(\mathbb{I})$ by Theorem 2.12(2) and Corollary 3.4. If we are in case (N) or (B) for some prime $\mathfrak{P}$, the group $\overline{\mathcal{G}}_{\mathfrak{P}} := \mathrm{Im}(\rho_{\mathfrak{P}})$ normalizes $\bar{\mathfrak{s}}_{\mathfrak{P}}$. Since the normalizer of a (non-trivial) nilpotent or a Borel subalgebra is a Borel subgroup, $\rho_{\mathfrak{P}}$ has values in a Borel subgroup; so, $\rho_{\mathfrak{P}}$ is reducible, which is impossible by the absolute irreducibility of $\overline{\rho}$. Thus cases (B) and (N) do not occur for any $\mathfrak{P}|P$.

In the cases (O) and (C), we first show that $\rho_{\mathfrak{P}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \theta$ for a character $\theta : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to (\mathbb{I}/\mathfrak{P})^\times$. Suppose first that we have some $\mathfrak{P}|P$ in case (O). Then the basic closure of $\overline{\mathbb{G}}_{\mathfrak{P}}$ is contained in the center; so, $\overline{\mathbb{G}}_{\mathfrak{P}} \subset \{\pm 1\}$. Since $p > 2$, we have $\overline{\mathbb{G}}_{\mathfrak{P}} = 1$. Therefore under the notation in the proof of Lemma 8.1, we have $\overline{\mathbb{H}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}} \ltimes \overline{\mathbb{G}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}}$. Since $\mathrm{Im}(\overline{\rho})$ is dihedral modulo center, taking $j \in \mathrm{Im}(\rho_{\mathbb{I}})$ defined just before stating Lemma 8.1, it contains an element j' of order 2 such that $j'jj'^{-1} = \left(\begin{smallmatrix} \zeta' & 0 \\ 0 & \zeta \end{smallmatrix}\right)$ (i.e. conjugation by j' interchanges the two distinct eigenvalues of j). This j' can be lifted to an element (still denoted by j') in $\mathrm{Im}(\rho_{\mathbb{I}})$ keeping the property of interchanging the two distinct eigenvalues of j (e.g. [Bro82, § IV.3] or [Zas99, § IV.7]). Then it interchanges the eigenvalues of elements in $\overline{\mathcal{T}}'_{\mathfrak{P}}$; so, we have $j'\overline{\mathcal{T}}'_{\mathfrak{P}}j'^{-1} \subset \overline{\mathbb{H}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}}$, which implies $\overline{\mathcal{T}}'_{\mathfrak{P}} = 1$. Thus we conclude $\mathfrak{P}|T$ and $\overline{\mathbb{H}}_{\mathfrak{P}} = 1$. Therefore $\mathrm{Im}(\rho_{\mathfrak{P}})$ is isomorphically projected onto $\mathrm{Im}(\overline{\rho})$, and hence we must have $\rho_{\mathfrak{P}} = \mathrm{Ind}_M^{\mathbb{Q}} \theta$ for a character $\theta : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to (\mathbb{I}/\mathfrak{P})^\times$.

Now we suppose that we have some $\mathfrak{P}|P$ in the remaining case (C). Since $\overline{\rho}$ is absolutely irreducible, $\rho_{\mathfrak{P}}$ is absolutely irreducible. Then, by Lemma 8.4, $\rho_{\mathfrak{P}} \cong \mathrm{Ind}_K^{\mathbb{Q}} \theta$ for a quadratic extension $K/\mathbb{Q}$ and a character θ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Since $\rho_{\mathfrak{P}}$ is ordinary and $\overline{\psi}$ ramifies at p, (p) must split in $K/\mathbb{Q}$ as $(p) = \mathfrak{p}\mathfrak{p}^c$. Then we may assume that θ is ramified at $\mathfrak{p}$ and unramified at $\mathfrak{p}^c$. By Proposition 5.2, K must be M, and ramification at $\mathfrak{p}$ forces $\theta \bmod \mathfrak{m}_{\mathbb{I}} = \overline{\psi}$. By (Gal), if $P \neq (T)$ or $\overline{\psi}^-$ is ramified at p, θ is ramified over a decomposition group D_p at p, and the other θ^c is unramified at the decomposition group.

Hereafter we treat the two cases (O) and (C) at the same time writing $\rho_{\mathfrak{P}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \theta$. By primitiveness, $\mathcal{F}_{\mathbb{I}}$ is a family of N-new forms. Thus we have $C(\rho_{\mathfrak{P}}) = N = N(\mathfrak{C})D$ for $\mathfrak{C} = \mathfrak{C}(\Psi_{\mathbb{J}})$ (see Remark 7.3). We may also assume that W and $\mathbb{I}$ have the same residue field $\mathbb{F}$. As before, let $Z = \varprojlim_n Cl_M(\mathfrak{C}\mathfrak{p}^n)$ and Z_p be the maximal p-profinite quotient of Z. By Proposition 5.7(2), there exist a character $\boldsymbol{\theta} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to W[[Z_p]]^\times$ unramified outside $\mathfrak{C}\mathfrak{p}$ and a canonical isomorphism $\mathbb{T}_{\mathrm{cm}} \cong W[[Z_p]]$ such that $\rho_{\mathbb{T}_{\mathrm{cm}}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \boldsymbol{\theta}$. Moreover, identifying $\mathbb{T}_{\mathrm{cm}} = W[[Z_p]]$, $(\mathbb{T}_{\mathrm{cm}}, \boldsymbol{\theta})$ is the

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

universal couple over W among deformations of θ mod $\mathfrak{m}_{\mathbb{I}}$. Thus the character $\boldsymbol{\theta}:\mathrm{Gal}(\overline{\mathbb{Q}}/M)\to\mathbb{T}_{\mathrm{cm}}^{\times}$ satisfies

$$\theta=\boldsymbol{\theta}\quad\mathrm{mod}\ \mathfrak{P}'\quad\text{for a prime } \mathfrak{P}'\in\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}). \tag{8.2}$$

In other words, taking $\iota:\mathbb{T}_{\mathrm{cm}}\to\kappa(\mathfrak{P})$ such that $\iota\circ\boldsymbol{\theta}=\theta$, we have $\mathfrak{P}'=\mathrm{Ker}(\iota)$ for $\mathfrak{P}'$ in (8.2). Since $N=N(\mathfrak{C})D$, the identification $\mathbb{T}_{\mathrm{cm}}=W[[Z_p]]$ gives rise to the algebra homomorphism $\mathbb{T}\to W[[Z_p]]$ described in Lemma 5.6, which was written as Θ there.

We write ρ' for $\rho_{\mathbb{T}_{\mathrm{cm}}}$, $\rho'_{\mathfrak{P}'}$ for ρ' mod $\mathfrak{P}'$. Then we have the identity of Galois representations $\rho_{\mathfrak{P}}\cong\rho'_{\mathfrak{P}'}=\mathrm{Ind}_M^{\mathbb{Q}}\boldsymbol{\theta}_{\mathfrak{P}'}$. This implies

$$\mathrm{Tr}(\rho_{\mathfrak{P}}(\mathrm{Frob}_l))=\mathrm{Tr}(\rho'_{\mathfrak{P}'}(\mathrm{Frob}_l))\quad\text{for all } l \text{ prime to } Np. \tag{8.3}$$

Let $\mathbb{T}'\subset\mathbb{T}$ be the Λ-subalgebra generated by the image of $T(l)$ for all l prime to Np. The identity (8.3) implies $\mathfrak{P}'\cap\mathbb{T}'=\mathfrak{P}\cap\mathbb{T}'$; i.e. the image of $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ and $\mathrm{Spec}(\mathbb{I})$ in $\mathrm{Spec}(\mathbb{T}')$ intersects at $\mathfrak{P}\cap\mathbb{T}'$. We now show that $\mathrm{Spec}(\mathbb{I})$ and $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ intersect at the unique prime divisor $\mathfrak{P}=\mathfrak{P}'$ above $\mathfrak{P}\cap\mathbb{T}'$ in $\mathrm{Spec}(\mathbb{T})$. Since $\overline{\psi}^{-}$ ramifies at p, we may assume that $\overline{\psi}$ is unramified at $\mathfrak{p}^c$. Then $\chi_1|_{\mathbb{Z}_p^{\times}}=\overline{\psi}|_{\mathfrak{O}_{\mathfrak{p}^c}^{\times}}$ (identifying $\mathbb{Z}_p=\mathfrak{O}_{\mathfrak{p}}$), which is non-trivial. As remarked in the sketch, $C(\rho_{\mathfrak{P}})=C(\rho_{\mathfrak{P}'})=C(\overline{\rho})=N$. Since $\overline{\psi}$ is ramified at $\mathfrak{p}$, $\chi_1|_{I_p}$ mod $\mathfrak{m}_W=\overline{\psi}|_{I_p}$ is non-trivial. Thus the assumptions of Lemma 5.4 are met, and we conclude $\mathbb{T}'_{\mathfrak{P}}=\mathbb{T}_{\mathfrak{P}}$. Thus $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$ and $\mathrm{Spec}(\mathbb{I})$ intersect at $\mathfrak{P}'=\mathfrak{P}$ in $\mathrm{Spec}(\mathbb{I})\cap\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$.

By Proposition 5.2(2), that the order of $\overline{\psi}^{-}$ is greater than 2 implies $\mathbb{T}_{\mathrm{cm}}^{M}=\mathbb{T}_{\mathrm{cm}}$. Write

$$\mathrm{Spec}(\mathbb{T})=\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}^{\perp})\cup\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}})$$

for the complementary union of irreducible components $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm}}^{\perp})\subset\mathrm{Spec}(\mathbb{T})$. Note that

$$\mathrm{Spec}(\mathbb{I}_P)\cap\mathrm{Spec}(\mathbb{T}_{\mathrm{cm},P})=\mathrm{Spec}(\mathbb{I}_P\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},P})\subset\mathrm{Spec}(\mathbb{T}_{\mathrm{cm},P}^{\perp}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},P}).$$

By Theorem 7.2, identifying $\mathbb{T}_{\mathrm{cm}}$ with $W[[Z_p^{-}]]$, we have closed immersions

$$\mathrm{Spec}(\mathbb{T}_{\mathrm{cm},\mathfrak{P}}/L^{-}(\overline{\psi}^{-})\mathbb{T}_{\mathrm{cm},\mathfrak{P}})\subset\mathrm{Spec}(\mathbb{T}_{\mathrm{cm},P}^{\perp}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},P})\supset\mathrm{Spec}(\mathbb{I}_{\mathfrak{P}}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},\mathfrak{P}}),$$

and we have, inside $\mathrm{Spec}(\mathbb{T}_{\mathrm{cm},P}^{\perp}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},P})$,

$$\mathrm{Spec}(\mathbb{I}_{\mathfrak{P}}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},\mathfrak{P}})\subset\mathrm{Spec}(\mathbb{T}_{\mathrm{cm},\mathfrak{P}}/L^{-}(\overline{\psi}^{-})\mathbb{T}_{\mathrm{cm},\mathfrak{P}}). \tag{8.4}$$

Let

$$\mathfrak{b}:=\mathrm{Ann}_{\mathbb{T}_{\mathrm{cm},P}}(\mathbb{I}_{\mathfrak{P}}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},P})\subset\mathbb{T}_{\mathrm{cm},P}\quad\text{and}\quad\mathfrak{a}:=\mathrm{Ann}_{\mathbb{I}_{\mathfrak{P}}}(\mathbb{I}_{\mathfrak{P}}\otimes_{\mathbb{T}}\mathbb{T}_{\mathrm{cm},P})\subset\mathbb{I}_{\mathfrak{P}},$$

where $\mathrm{Ann}_A(X)$ is the annihilator in the ring A of an A-module X. Put $\rho_{\mathfrak{b}}=(\rho_{\mathbb{T}_{\mathrm{cm}}}\ \mathrm{mod}\ \mathfrak{b})$ and $\rho_{\mathfrak{a}}=(\rho_{\mathbb{I}}\ \mathrm{mod}\ \mathfrak{a})$. Thus $\mathrm{Tr}(\rho_{\mathfrak{b}})=\mathrm{Tr}(\rho_{\mathfrak{a}})$, which implies $\rho_{\mathfrak{b}}\cong\rho_{\mathfrak{a}}$ (by a result of Carayol–Serre; e.g. [Hid00, Proposition 2.13]). Since the right-hand side $\rho_{\mathfrak{b}}$ is an induced representation from M, the image $\mathrm{Im}(\rho_{\mathfrak{a}})|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)}$ (of the right-hand side) is in the diagonal subgroup of $\mathrm{GL}_2(\mathbb{I}/\mathfrak{a}\mathbb{I})$. Thus $(L(\mathbb{I}))_P\mathbb{I}_{\mathfrak{P}}\subset\mathfrak{a}$. By (8.4), $\mathfrak{a}$ is a factor of $L^{-}_{\overline{\psi}^{-}}\Lambda_{W,P}$. This $\mathfrak{a}$ depends on $\mathfrak{P}$, and $\mathfrak{a}\cap\Lambda$ is a power of P. We fix $\mathfrak{P}|P$ such that $\mathfrak{a}\cap\Lambda$ is the smallest. We would like to show $(\mathfrak{a}\cap\Lambda_P)^2\subset(L(\mathbb{I}))_P$.

Suppose $(L(\mathbb{I}))_P\subsetneq\mathfrak{a}$. Let $\mathfrak{s}_{\mathfrak{P}}=\mathbb{I}_{\mathfrak{P}}\cdot\mathcal{M}_1^0(\mathbb{G})$. We consider the adjoint action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$V:=(\mathfrak{s}_{\mathfrak{P}}\cap\mathfrak{a}\cdot\mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}}))/(\mathfrak{s}_{\mathfrak{P}}\cap\mathfrak{a}'\cdot\mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}}))$$

for $\mathfrak{a}' := \mathfrak{a}\mathfrak{P} \supset (L(\mathbb{I}))_P$. Then the adjoint $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module V is isomorphic to a factor of $\mathrm{Ad}(\rho_{\mathfrak{P}}) \cong (\frac{M/\mathbb{Q}}{}) \oplus \mathrm{Ind}_M^{\mathbb{Q}} \theta^-$. Since $\overline{\psi}^-$ is non-trivial, θ^- with $\theta^- \equiv \psi^- \bmod \mathfrak{m}_{\mathbb{I}}$ is non-trivial, and hence $\mathrm{Ind}_M^{\mathbb{Q}} \theta^-$ is absolutely irreducible. If V contains the two irreducible factors, we have $\dim_{\kappa(\mathfrak{P})} V = 3$ and hence by Nakayama's lemma, we have $(\mathfrak{s}_{\mathfrak{P}} \cap \mathfrak{a} \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}})) = \mathfrak{a} \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}})$; so, $(L(\mathbb{I}))_P = \mathfrak{a}$, a contradiction (against $(L(\mathbb{I}))_P \subsetneq \mathfrak{a}$). In other words, we have $(L(\mathbb{I}))_P \subsetneq \mathfrak{a} \Leftrightarrow V$ does not contain the two irreducible factors.

If V is made up of $(\frac{M/\mathbb{Q}}{})$, the Lie algebra V and hence $\mathfrak{s}_{\mathfrak{P}}/(\mathfrak{s}_{\mathfrak{P}} \cap \mathfrak{a}' \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}}))$ acts trivially on $(\mathbb{I}/\mathfrak{a}')^2$; so, the image of $\mathbb{G}$ in $\mathrm{SL}_2(\mathbb{I}/\mathfrak{a}')$ is in the split diagonal torus. This implies $\rho_{\mathfrak{a}'}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/M)} = \theta' \oplus \theta''$ with $\theta' \cong \overline{\psi} \bmod \mathfrak{m}_{\mathbb{I}}$. By Frobenius' reciprocity law (cf. [Hid11a, § 5.1.1]), we conclude $\rho_{\mathfrak{a}'} \cong \mathrm{Ind}_M^{\mathbb{Q}} \theta'$. This is impossible, as $\mathfrak{a}$ is the minimal $\mathbb{I}_{\mathfrak{P}}$-ideal so that $\rho_{\mathfrak{a}}$ is an induced representation from M.

We deal with the remaining case where V contains only $\mathrm{Ind}_M^{\mathbb{Q}} \theta^-$. We pick again the element $j = \rho(\sigma)$ and j' as specified at the beginning of the proof. As explained before starting the proof, we may assume that $j' = \rho_{\mathbb{I}}(c)$. By the adjoint action, j acts on $\mathfrak{S} := \mathfrak{s}_{\mathfrak{P}} \cap \mathfrak{a} \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}})$ and on V. Thus $V = V[a] \oplus V[1] \oplus V[a^{-1}]$ and $\mathfrak{S} = \mathfrak{S}[a] \oplus \mathfrak{S}[1] \oplus \mathfrak{S}[a^{-1}]$ for the three eigenvalues $a, 1, a^{-1}$ of $\mathrm{Ad}(j)$. Since the Galois action on $V[1]$ factors through $(\frac{M/\mathbb{Q}}{})$, we conclude $V[1] = 0$. We also know that j' interchanges $V[a]$ and $V[a^{-1}]$ (and $\mathfrak{S}[a]$ and $\mathfrak{S}[a^{-1}]$) isomorphically. Thus $V[a] \cong V[a^{-1}] \neq 0$ and $\mathfrak{S}_{\mathfrak{P}}[?]$ surjects down to $V[?]$ for $? = a, 1, a^{-1}$. Then $\mathfrak{S}$ contains matrices $X := \left(\begin{smallmatrix} 0 & u \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{S}[a]$ and $Y := \left(\begin{smallmatrix} 0 & 0 \\ v & 0 \end{smallmatrix}\right) \in \mathfrak{S}[a^{-1}]$ whose images $\overline{X}$ (respectively $\overline{Y}$) in V are non-trivial in $V[a]$ (respectively $V[a^{-1}]$); i.e. $0 \neq \overline{X} \in V[a]$ and $0 \neq \overline{Y} \in V[a^{-1}]$. This X is in $\mathcal{M}[a]$ and Y is in $\mathcal{M}[a^{-1}]$ in the proof of Lemma 2.9. In other words, for the Λ-module $\mathfrak{n} = \{x \in \mathbb{I} \mid \left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right) \in \mathcal{M}(\mathbb{G})\}$ and its opposite $\mathfrak{n}_t$ introduced in the proof of Lemma 2.9, $\mathfrak{a} = \mathbb{I}_{\mathfrak{P}}\mathfrak{n} = \mathbb{I}_{\mathfrak{P}}\mathfrak{n}_t$. Then

$$0 \neq [X, Y] = \begin{pmatrix} uv & 0 \\ 0 & -uv \end{pmatrix} \in (\mathfrak{s}_{\mathfrak{P}} \cap \mathfrak{a}^2 \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}}))/(\mathfrak{s}_{\mathfrak{P}} \cap \mathfrak{a}^2\mathfrak{P} \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}})) =: V'.$$

The Lie algebra V' also has non-trivial image of λX and λY for any generator λ of $\mathfrak{a}$. This shows $\dim_{\kappa(\mathfrak{P})} V' = 3$, and by Nakayama's lemma $\mathfrak{s}_{\mathfrak{P}} \cap \mathfrak{a}^2 \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}}) = \mathfrak{a}^2 \cdot \mathfrak{sl}_2(\mathbb{I}_{\mathfrak{P}})$. Thus $\mathfrak{a}^2 = \mathbb{I}_{\mathfrak{P}}\mathfrak{n}\mathfrak{n}_t$ and $\mathfrak{u}\mathfrak{u}_t \subset (L(\mathbb{I}))$, where as before we put $\mathfrak{u} = \mathfrak{n} \cap \Lambda$ and $\mathfrak{u}_t = \mathfrak{n}_t \cap \Lambda$. If $\mathbb{I} = \Lambda$, $\mathfrak{u} = \mathfrak{n}$ and $\mathfrak{u}_t = \mathfrak{n}_t$, this finishes the proof as we described already.

If $\mathbb{I} \supsetneq \Lambda$, we therefore need to show $\mathbb{I}_{\mathfrak{P}}\mathfrak{u} \cap \Lambda_P = \mathbb{I}_{\mathfrak{P}}\mathfrak{u}_t \cap \Lambda_P = \mathfrak{a} \cap \Lambda_P$. Recall we have chosen $\mathfrak{P}$ so that $\mathfrak{a}_{\mathfrak{P}} \cap \Lambda = \Lambda_{W,P}\mathfrak{n} \cap \Lambda$ (i.e. $\mathfrak{P}$ has been chosen so that $\mathfrak{a}_{\mathfrak{P}} \cap \Lambda$ is the highest power of P). Take $\varepsilon \in \mathbb{I}_P \cap \mathbb{I}_{\mathfrak{P}}^{\times}$ so that $\varepsilon\mathfrak{u}\mathbb{I}_{\mathfrak{P}} \cap \Lambda_P = \mathfrak{a} \cap \Lambda_P$. Conjugating $\mathbb{G}$ by $\alpha = \left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we may assume that $\mathfrak{u}_P = \Lambda_P \cap \mathfrak{n}_P = \mathfrak{a}_P \cap \Lambda_P$. Since $\mathrm{Im}(\rho_{\mathbb{I}})$ surjects down to a dihedral group $H := \mathrm{Im}(\overline{\rho})$, in this case the condition (v) is not satisfied (as $\mathrm{Im}(\overline{\rho})$ does not contain non-trivial unipotent elements); so, we are assuming (s) (which is satisfied if $\psi^-|_{D_p}$ has order $\geqslant 3$). Note that $D := \overline{\rho}(D_p) \cap \mathrm{GL}_2(\mathbb{F}_p)$ is made of diagonal matrices of order prime to p. Taking their Teichmüller lifts, we can lift D isomorphically onto $\widetilde{D} \subset \mathrm{GL}_2(\mathbb{Z}_p)$. By our construction, $\widetilde{D}$ is in the image of D_p. We can also lift H isomorphically onto a dihedral subgroup $\widetilde{H} \subset \mathrm{Im}(\rho_{\mathbb{I}})$ so that $\widetilde{D} \subset \widetilde{H}$ (e.g. [Bro82, Exercise 1 of § IV.3] or [Zas99, § IV.7]). Then, as explained in the proof of Corollary 3.4, $j \in \mathrm{GL}_2(\mathbb{I})$ in condition (1) of Lemma 2.9 is chosen in $\widetilde{D}$. Thus we have $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose restriction to M is the complex conjugation such that $j' = \rho_{\mathbb{I}}(c) \in \widetilde{H}$. Then $j'jj'^{-1} = \left(\begin{smallmatrix} \zeta' & 0 \\ 0 & \zeta \end{smallmatrix}\right)$ if $j = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta' \end{smallmatrix}\right)$; i.e. the conjugation of j' interchanges the two eigenvalues. By Lemma 1.4, we have $\mathcal{T}' = \{\left(\begin{smallmatrix} t^s & 0 \\ 0 & 1 \end{smallmatrix}\right) \mid s \in \mathbb{Z}_p\} \subset \rho_{\mathbb{I}}(D_{\mathfrak{p}}) \subset \mathrm{Im}(\rho_{\mathbb{I}})$, and $j'\mathcal{T}'j'^{-1} = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & t^{-s} \end{smallmatrix}\right) \mid s \in \mathbb{Z}_p\} \subset \rho_{\mathbb{I}}(cD_{\mathfrak{p}}c^{-1})$. We have chosen an eigenbasis of $\widetilde{\mathbb{I}}^2$ of j to write the matrix form of $\rho_{\mathbb{I}}$. Then to have $\mathfrak{c}$ with $\Gamma_{\Lambda}(\mathfrak{c})$ inside $\mathrm{Im}(\rho_{\mathbb{I}})$, we change the basis v of the ζ-eigenspace of j multiplying by an element in $\mathbb{I}$ prime to P. Since

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

$j' = \rho_{\mathbb{I}}(c)$ interchanges the two eigenspaces of j, we choose the basis of the other ζ'-eigenspace to be given by $\rho_{\mathbb{I}}(c)v$. Then this j' and $\widetilde{D}$ generate the dihedral subgroup of $\widetilde{H} \subset \mathrm{GL}_2(\mathbb{Z}_p) \cap \mathrm{Im}(\rho_{\mathbb{I}})$ lifting H isomorphically, and j' is equal to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{GL}_2(\Lambda)$. Hence we may assume $Y = j'Xj'^{-1}$, which implies $(\mathfrak{a} \cap \Lambda_P)^2 \subset (L(\mathbb{I}))_P$.

Note that $\mathrm{Char}_{\Lambda_W}(W[[Z_p^-]]/L^-(\overline{\psi}^-)W[[Z_p^-]])$ is given by $N_{W[[Z_p^-]]/\Lambda_W}(L^-(\overline{\psi}^-)) = L^-_{\overline{\psi}^-}$. Conversely if we start with $P|L^-_{\overline{\psi}^-}$, by Theorem 7.2, the intersection scheme $\mathrm{Spec}(\mathbb{T}^{\perp}_{\mathrm{cm},P} \otimes_{\mathbb{T}} \mathbb{T}_{\mathrm{cm},P})$ is non-empty containing a prime divisor; so, we can find an irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbb{T}^{\perp}_{\mathrm{cm}})$ such that ρ_P is isomorphic to $\mathrm{Ind}_M^{\mathbb{Q}} \lambda$ for a character λ. This implies $P|L(\mathbb{I})$. □

Here is the result in the residually dihedral case not included in the above theorem.

THEOREM 8.6. *If $\overline{\rho}$ is absolutely irreducible with $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$ for a quadratic field M and a character $\overline{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to \overline{\mathbb{F}}_p$ with $\overline{\psi}^-$ having order > 2, then for any non-CM component $\mathbb{I}$ of $\mathbb{T}$, we have the following.*

(1) *If M is real and p splits into $\mathfrak{p}\overline{\mathfrak{p}}$ in M, writing $1 + p^{m+1}\mathbb{Z}_p$ with $m \geqslant 0$ for the kernel of the natural map $\Gamma \to Cl_M(\mathfrak{p}^\infty)$, then $L(\mathbb{I}) \supset (t^{p^m} - 1)^2$.*

(2) *If p does not split in M, then $L(\mathbb{I}) \supset (T^2)$.*

This theorem settles the case (3a) of Theorem II in the introduction. Note also that $\overline{\psi}^-$ having order > 2 implies $|\mathbb{F}| \geqslant 4$.

Proof. Let P be a prime divisor of Λ, and write $\mathfrak{P}$ for any prime divisor of $\mathbb{I}$ above P. Let $\mathfrak{c}$ be the prime-to-p conductor of ψ. By the same argument as in the proof of Theorem 8.5, if $P|L(\mathbb{I})$, we have either $\overline{\mathfrak{s}}_{\mathfrak{P}} = 0$ or $\overline{\mathfrak{s}}_{\mathfrak{P}}$ is a Cartan subalgebra or $\overline{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}(2)$. If $\overline{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}(2)$ for all $\mathfrak{P}|P$, then $P \nmid L(\mathbb{I})$ by Lemma 8.1, Theorem 2.12 and Corollary 3.4 combined. If $\overline{\mathfrak{s}}_{\mathfrak{P}} \neq \mathfrak{sl}(2)$, by the same argument as in the proof of Theorem 8.5, $\rho_{\mathfrak{P}} = \mathrm{Ind}_M^{\mathbb{Q}} \theta$ for a character θ. Then for the prime-to-p conductor $\mathfrak{C}$ of θ, we may assume that $\theta : Z \to \kappa(P)$, where $Z = \varprojlim_n Cl_M(\mathfrak{C}\mathfrak{p}^\infty)$. If M is real, Z is a finite group, and $\theta([\gamma, \mathbb{Q}_p]^{p^m}) = 1$, where we identify the inertia groups $I_{\mathfrak{p}}$ and I_p and $[\gamma, \mathbb{Q}_p] \in I_{\mathfrak{p}}$. This implies $P|(t^{p^m} - 1)$ by (Gal).

If p is non-split, θ has to be unramified at p as θ or θ^c is unramified at p (note, by (s), that $\theta^-|_{D_p}$ has to have order $\geqslant 3$). Then $\theta([\gamma, \mathbb{Q}_p]) = 1$, which implies $P|(T)$ by (Gal). Write Z for the class group $Cl_M(\mathfrak{C})$ of M.

To show $L(\mathbb{I})|(t^{p^m} - 1)^2$ for some $m \geqslant 0$, we deal with the two cases at the same time. Let Z_p be the p-part of Z; so, $Z = Z_p \times Z'$ for Z' of prime-to-p order. Pick a prime $\mathfrak{P}$ of $\mathbb{I}$ for which $\rho_{\mathfrak{P}}$ is an induced representation from M. Let $\mathfrak{a}$ be the minimal ideal of $\mathbb{I}_{\mathfrak{P}}$ such that $\rho_{\mathfrak{a}} = (\rho_{\mathbb{I}} \bmod \mathfrak{a})$ is an induced representation from M. Then $\rho_{\mathfrak{a}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \lambda$ and λ can be identified with a character of Z by class field theory. Thus we have a W-algebra homomorphism $W[Z] \to \mathbb{I}_{\mathfrak{P}}/\mathfrak{a}$ by the universality of the group algebra, and this factors through a local ring of $W[Z]$ isomorphic to $W[Z_p]$. Since $\mathbb{I}$ is generated topologically by $\mathrm{Tr}(\rho_{\mathbb{I}})$ over $Q(W)$ and ψ^- has order > 3, $\mathbb{I}_{\mathfrak{P}}/\mathfrak{a}\mathbb{I}_{\mathfrak{P}}$ is generated by the values of λ. Thus $\mathbb{I}_{\mathfrak{P}}/\mathfrak{a}$ is reduced; so, $\mathfrak{a}$ is square-free, $\mathfrak{a} \cap \Lambda \supset (t^{p^m} - 1)$, and $(\mathfrak{a} \cap \Lambda_P) \supset (L(\mathbb{I}))_P$. Then by the same argument as in the proof of Theorem 8.5, we conclude $(L(\mathbb{I}))_P \supset (\mathfrak{a} \cap \Lambda)^2$. □

Assume that $\overline{\rho}$ is absolutely irreducible and its projective image in $\mathrm{PGL}_2(\mathbb{F})$ is one of the following three type of groups: a tetrahedral group, an octahedral group or an icosahedral group. These groups cannot be a quotient of a Borel subgroup or a unipotent group or a dihedral

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

group, if $\bar{\mathfrak{s}}_{\mathfrak{P}} \neq \mathfrak{sl}(2)$, we have $\bar{\mathfrak{s}}_{\mathfrak{P}} = 0$. Again under the notation of the proof of Lemma 3.1, $\overline{\mathbb{H}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}} \ltimes \overline{\mathbb{G}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}}$ as $\overline{\mathbb{G}}_{\mathfrak{P}} = 1$. Then we have $\overline{\rho}(\sigma)$ whose projective image does not commute with the image of j, and we find $j' \in \mathrm{Im}(\rho_{\mathfrak{P}})$ having the same effect on j projecting down to $\overline{\rho}(\sigma)$. Then $j'\overline{\mathcal{T}}'_{\mathfrak{P}}j'^{-1} = \overline{\mathbb{H}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}}$, which implies $\overline{\mathcal{T}}'_{\mathfrak{P}} = 1$; so, $\mathfrak{P}|T$. Thus we get the following theorem, which settles case (2) of Theorem II in the introduction.

Theorem 8.7. *Assume that $\overline{\rho}$ is absolutely irreducible and its projective image is one of the following three type of groups: a tetrahedral group, an octahedral group or an icosahedral group. Then if* $\mathrm{Spec}(\mathbb{I})$ *is an irreducible component of* $\mathrm{Spec}(\mathbb{T})$, *we have $T|L(\mathbb{I})|T^n$ for sufficiently large $n > 0$.*

It is interesting to determine the minimal integer n depending on $\mathbb{I}$. The following theorem settles the last remaining case (4) of Theorem II.

Theorem 8.8. *Suppose $p \geqslant 5$, $p \nmid \varphi(N)$ and that N is cube-free. Assume that $\overline{\rho}$ is reducible and its semi-simplification is a direct sum of two characters $\overline{\theta}$ and $\overline{\psi}$ with $\overline{\theta}$ ramified at p and $\overline{\psi}$ unramified at p and that $\overline{\theta}/\overline{\psi}$ has order > 2. Let* $\mathrm{Spec}(\mathbb{I})$ *be an irreducible component of* $\mathrm{Spec}(\mathbb{T})$. *Then $L(\mathbb{I})$ is a factor of $L(\overline{\theta}, \overline{\psi})$ given in Definition 4.1(2). Moreover for any prime divisor P of $L(\overline{\theta}, \overline{\psi})$, if $p \nmid \varphi(N)$, there exists an irreducible non-CM component* $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{T})$ *such that $P|L(\mathbb{I})$.*

The strategy of proving this theorem is similar to the one we used for Theorem 8.5, replacing CM components by Eisenstein components in $\mathrm{Spec}(\mathbf{H})$. As we computed the ideal of the intersection $\mathrm{Spec}(\mathcal{C}_{\mathbf{E}_{\mathfrak{m}}}) = \mathrm{Spec}(\mathbf{h}_{\mathfrak{m}}) \cap \mathrm{Spec}(\mathbf{E}_{\mathfrak{m}})$ for $\mathfrak{m} := \mathfrak{m}(\overline{\theta}, \overline{\psi}; M_1, M_2)$ in Corollary 4.3, the argument goes through. Note here $\mathbb{T} = \mathbf{h}_{\mathfrak{m}}$.

Proof. Let the notation be as in the proof of Theorem 8.5. In particular, P is a prime divisor of $\mathrm{Spec}(\Lambda)$ and $\mathfrak{P}$ is a prime divisor of $\mathrm{Spec}(\mathbb{I})$ above P. Again there are the following five possibilities: (O) $\bar{\mathfrak{s}}_{\mathfrak{P}} = 0$; (C) $\bar{\mathfrak{s}}_{\mathfrak{P}}$ is a Cartan subalgebra $\mathfrak{H}$; (N) $\bar{\mathfrak{s}}_{\mathfrak{P}}$ is a nilpotent subalgebra; (B) $\bar{\mathfrak{s}}_{\mathfrak{P}}$ is a Borel subalgebra; (F) $\bar{\mathfrak{s}}_{\mathfrak{P}} = \mathfrak{sl}_2(\kappa(\mathfrak{P}))$.

We can forget about the case (F) for all $\mathfrak{P}|P$ as $P \nmid L(\mathbb{I})$ in case (F). An induced representation $\mathrm{Ind}_M^{\mathbb{Q}} \lambda$ for a quadratic extension $M/\mathbb{Q}$ is reducible only when λ^- is trivial, and if $\lambda^- = \mathbf{1}$, λ extends to a character $\widetilde{\lambda}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and we have $\mathrm{Ind}_M^{\mathbb{Q}} \lambda = \widetilde{\lambda} \oplus \widetilde{\lambda}(\frac{M/\mathbb{Q}}{})$. By the assumption that $\overline{\theta}/\overline{\psi}$ has order $\geqslant 3$, we find that $\rho_{\mathfrak{P}} \cong \mathrm{Ind}_M^{\mathbb{Q}} \lambda$ is impossible (so, the assumption of Lemma 3.5 is satisfied, and we have ($L(\mathbb{I})$) well defined). In particular, any component of $\mathrm{Spec}(\mathbb{T})$ does not have CM. Thus if $\bar{\mathfrak{s}}_{\mathfrak{P}} \neq \mathfrak{sl}(2)$ or $\bar{\mathfrak{s}}_{\mathfrak{P}} \neq 0$, we have $\rho_{\mathfrak{P}} \cong \left(\begin{smallmatrix} \theta_{\mathfrak{P}} & * \\ 0 & \psi_{\mathfrak{P}} \end{smallmatrix}\right)$ with $\theta_{\mathfrak{P}} \bmod \mathfrak{m}_{\mathbb{T}} = \overline{\theta}$ and $\psi_{\mathfrak{P}} \bmod \mathfrak{m}_{\mathbb{T}} = \overline{\psi}$ with $\psi_{\mathfrak{P}}$ unramified at p as $\overline{\theta}$ ramifies at p. If $\bar{\mathfrak{s}}_{\mathfrak{P}} = 0$, again we have $\overline{\mathbb{H}}_{\mathfrak{P}} = \overline{\mathcal{T}}'_{\mathfrak{P}}$, which is normalized by $\mathrm{Im}(\rho_{\mathfrak{P}})$; so, if $\mathfrak{P} \nmid T$, $\rho_{\mathfrak{P}}$ is reducible. If $\mathfrak{P}|T$ and $\bar{\mathfrak{s}}_{\mathfrak{P}} = 0$, we have $\overline{\mathbb{H}}_{\mathfrak{P}} = 1$ and hence, $\mathrm{Im}(\overline{\rho}_{\mathfrak{P}})$ surjects down onto $\mathrm{Im}(\overline{\rho})$ with finite kernel K (the possible error term K is in the diagonal torus, which comes from the difference of $\det(\overline{\mathcal{T}}'_{\mathfrak{P}})$ and the p-profinite part of $\mathrm{Im}(\det(\rho_{\mathfrak{P}}))$). This implies $\rho_{\mathfrak{P}}$ is reducible. Thus $\mathfrak{P}$ is an Eisenstein ideal.

We now specify the Λ-adic Eisenstein component with which $\mathrm{Spec}(\mathbb{I})$ intersects at $\mathfrak{P}$. Write

$$\rho_{\mathfrak{P}}^{ss} = \begin{pmatrix} \theta_{\mathfrak{P}} & 0 \\ 0 & \psi_{\mathfrak{P}} \end{pmatrix}.$$

The prime-to-p conductor of $\rho_{\mathfrak{P}}^{ss}$ is the product $\mathfrak{C}(\theta_{\mathfrak{P}})\mathfrak{C}(\psi_{\mathfrak{P}})$ of the prime-to-p conductors $\mathfrak{C}(\theta_{\mathfrak{P}})$ and $\mathfrak{C}(\psi_{\mathfrak{P}})$. Thus we have $\mathfrak{C}(\theta_{\mathfrak{P}})\mathfrak{C}(\psi_{\mathfrak{P}})|N$. By (Gal), we may assume that $\psi_{\mathfrak{P}}$ is unramified at p. Thus $\psi_{\mathfrak{P}}$ only (possibly) ramifies at prime factors of N prime to p. By class field theory, the image of the inertia group I_l at l in the abelianization of the decomposition group D_l at l is isomorphic to the almost l-profinite group $\mathbb{Z}_l^\times$. Thus $\psi_{\mathfrak{P}}|_{I_l}$ with values in an almost p-profinite subgroup of $\kappa(\mathfrak{P})^\times$ has to be of finite order. Then by global class field theory, $\psi_{\mathfrak{P}}$ is of finite order. If $\kappa(\mathfrak{P})$ has characteristic p, $\psi_{\mathfrak{P}}$ has values in $\overline{\mathbb{F}}_p^\times$ (so, $\psi_{\mathfrak{P}} = \overline{\psi}$), and we have a unique Teichmüller lift $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to W^\times$ of $\psi_{\mathfrak{P}} = \overline{\psi}$. If $\kappa(\mathfrak{P})$ has characteristic 0, we put $\psi = \psi_{\mathfrak{P}}$. We may assume that ψ has values in $W^\times$, extending scalars if necessary. Now we consider the strict ray class group $Cl_{\mathbb{Q}}(Np^n)$ and $Y = \varprojlim_n Cl_{\mathbb{Q}}(Np^n) \cong \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. By class field theory, for the maximal ray class field $\mathbb{Q}[\mu_{Np^\infty}]/\mathbb{Q}$ modulo Np^∞, we have a canonical isomorphism $\mathrm{Gal}(\mathbb{Q}[\mu_{Np^\infty}]/\mathbb{Q}) \cong Y$. We identify these two groups. Write Y_p for the Sylow p-profinite subgroup of Y; so, $Y = Y^{(p)} \times Y_p$ canonically for the finite group $Y^{(p)}$ of order prime to p. We consider the group algebra $W[[Y_p]]$ and for $u \in Y$, we write $[u_p]$ for the group element in $Y_p \subset W[[Y_p]]^\times$ represented by the projection of u in Y_p. By the same deformation argument proving Proposition 5.7(2) (and used in the proof of Theorem 8.5), for the Teichmüller lift $\theta_0 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to W^\times$ of $\overline{\theta} = \theta_{\mathfrak{P}} \bmod \mathfrak{m}_{\mathbb{I}}$, if $p \nmid \varphi(N)$, $(W[[Y_p]], \boldsymbol{\theta})$ for $\boldsymbol{\theta}([u, \mathbb{Q}_p]) = \theta_0(u)[u_p] \in W[[Y_p]]$ for $u \in Y$ is the universal couple among all deformations

$$(A, \epsilon : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to A^\times)$$

of $(\mathbb{F}, \theta_0 \bmod \mathfrak{m}_W)$ with prime-to-p conductor $\mathfrak{C}(\epsilon)|N$.

Let Y_t be the maximal torsion subgroup of Y_p. We may assume that any character: $Y_t \times Y^{(p)} \to \overline{\mathbb{Q}}_p^\times$ actually has values in $W^\times$ by extending scalars if necessary. The maximal torsion-free quotient of Y_p is canonically isomorphic to Γ, and we have a non-canonical decomposition $Y = Y_t \times \Gamma$ with the p-group Y_t. We identify $W[[\Gamma]]$ with $W[[T]]$ by $\gamma \mapsto t = 1+T$. Since $W[[Y_p]] = W[Y_t][[\Gamma]]$, geometrically irreducible components of $\mathrm{Spec}(W[[Y_p]])$ are indexed by characters $\theta : Y_t \to W^\times$ so that the component is given by the W-algebra projection $\theta_* : W[[Y_p]] \twoheadrightarrow W[[T]]$ sending $y \in Y_t$ to $\theta(y)$ and γ to t. We call this component the θ-component. Take θ such that $\theta_* \circ \boldsymbol{\theta} \bmod \mathfrak{P} = \theta_{\mathfrak{P}}$ in $\mathbb{I}$. By (Gal), we have $\theta_* \circ \boldsymbol{\theta}(\mathrm{Frob}_l) = \theta(\mathrm{Frob}_l)\langle l \rangle$ for all primes l outside Np. Since $\theta_{\mathfrak{P}}$ gives rise to a point $\mathfrak{P}'$ of an irreducible component $\mathrm{Spec}(W[[T]])$ of the universal deformation space $\mathrm{Spec}(W[[Y_p]])$ so that $\theta_{\mathfrak{P}} \equiv \theta_* \circ \boldsymbol{\theta} \bmod \mathfrak{P}'$ (with $\mathfrak{P}' = \mathfrak{P} \cap W[[T]]$). Consider the Λ-adic Eisenstein series $E(\theta, \psi)$. By our construction, $\rho_{\mathfrak{P}}$ is isomorphic to $\psi \oplus (\theta_* \circ \boldsymbol{\theta}) \bmod \mathfrak{P}'$. Then in a way similar to the CM case, we can find a possibly 'old' Eisenstein component $\mathbb{I}'$ with Galois representation $\psi \oplus (\theta_* \circ \boldsymbol{\theta})$ which intersects with $\mathbb{I}$ at P. Indeed, again by $l|C := \mathfrak{C}(\psi_{\mathfrak{P}})\mathfrak{C}(\theta_{\mathfrak{P}}) \Leftrightarrow l|N$, a mismatch of $\dim H_0(I_l, \rho_{\mathfrak{P}})$ and $\dim H_0(I_l, \rho_{\mathbb{I}})$ could occur only when $l|(N/C)$ and $l|\mathfrak{C}(\xi)$ but $l \nmid \mathfrak{C}(\eta)$ for $\{\xi, \eta\} = \{\psi_{\mathfrak{P}}, \theta_{\mathfrak{P}}\}$. Writing $\Xi(\eta)$ for the set of primes $l|(N/C)$ with the above divisibility/non-divisibility property, we consider the imprimitive characters ψ' (respectively θ') induced by ψ (respectively θ) modulo $M_1 := \mathfrak{C}(\psi) \prod_{l \in \Xi(\psi)} l$ (respectively $M_2 := p \cdot \mathfrak{C}(\theta) \prod_{l \in \Xi(\theta)} l$). The Eisenstein series $E(\theta', \psi')$ has congruence modulo P with the $\mathbb{I}$-adic form. Therefore $\mathbb{I}/(L(\mathbb{I}))\mathbb{I}$ is a surjective image of the Λ-submodule $\mathcal{C}_{\mathbf{E}_\mathfrak{m}} \otimes_{\mathbb{T}} \mathbb{I}$ of the Eisenstein congruence module $\mathcal{C}_{\mathbf{E}_\mathfrak{m}}$ (for $\mathfrak{m} = \mathfrak{m}(\overline{\theta}, \overline{\psi}; M_1, M_2)$) defined just above Corollary 4.3. Therefore $(L(\mathbb{I}))_P \subset (L(\overline{\theta}, \overline{\psi}))_P$. Let $\mathfrak{a}_{\mathfrak{P}} = \mathrm{Ann}_{\mathbb{I}_{\mathfrak{P}}}(\mathcal{C}_{\mathbf{E}_\mathfrak{m}} \otimes_{\mathbb{T}} \mathbb{I})$. Then $\mathfrak{a}_{\mathfrak{P}}$ is the minimal ideal so that $\rho_{\mathfrak{P}}$ is isomorphic to representation into $\mathcal{B}(\mathbb{I}_{\mathfrak{P}}/\mathfrak{a})$ and is a factor of $L(\overline{\theta}, \overline{\psi})$. If $P|(p)$, we know by [Hid13a, Theorem 6.2], $\rho_{\mathfrak{P}}$ is irreducible if $p \nmid \varphi(N)$; so, there is no reducible prime $\mathfrak{P}|(p)$. Thus we may assume that $P \nmid (p)$. Then by Corollary 3.6, $\mathfrak{c}_P = \bigcap_{\mathfrak{P}|P} \mathfrak{a}_{\mathfrak{P}} \cap \Lambda_{W,P}$; so, $\mathfrak{c}_P | L(\overline{\theta}, \overline{\psi})$.

The existence of $\mathbb{I}$ with $\mathfrak{P}|L(\mathbb{I})$ for $P|L(\overline{\theta}, \overline{\psi})$ follows from the definition of $\mathcal{C}_{\mathbf{E}}$. Indeed, there exist $(\theta, \psi; M_1, M_2)$ with $P|A(T; \theta.\psi)$ and at least one component $\mathrm{Spec}(\mathbb{I})$ containing $P \in \mathrm{Spec}(\mathcal{C}_{\mathbf{E}_\mathfrak{m}})$ for this choice of $(\theta, \psi; M_1, M_2)$. As already remarked, any component of $\mathrm{Spec}(\mathbb{T})$ is not of CM type. □

Here is a summarizing remark.

Remark 8.9. The proof of Theorems 8.5 and 8.8 is separated into two parts. The first part is to prove that the congruence ideal between a non-CM component and abelian components (i.e. either Eisenstein or CM components) is (essentially) equal to the level ideal. This is the principal work done in this paper. The second part is to identify the level as a factor of an appropriate p-adic L-function by the help of a proven main conjecture and Galois deformation theory.

9. Mixed cases

Pick a minimal primitive irreducible component $\mathrm{Spec}(\mathbb{I})$ of $\mathrm{Spec}(\mathbf{h})$. Let $\mathrm{Spec}(\mathbb{T})$ be the connected component of $\mathrm{Spec}(\mathbf{h})$ containing $\mathrm{Spec}(\mathbb{I})$. We consider an $\widetilde{\mathbb{I}}$-lattice $\mathcal{L}$ in $Q(\mathbb{I})^2$ stable under $\rho_{\mathbb{I}}$. Take its reflexive closure $\widetilde{\mathcal{L}}$, which remains stable under $\rho_{\mathbb{I}}$. For any $0 \neq a \in \widetilde{\mathbb{I}}$, the multiple $a\widetilde{\mathcal{L}}$ remains $\widetilde{\mathbb{I}}$-reflexive. By [Bou98, VII.4.2 Proposition 7], the set of associated primes of $\widetilde{\mathcal{L}}/a\widetilde{\mathcal{L}}$ is made of prime divisors. Thus, if $\widetilde{\mathbb{I}}/a\widetilde{\mathbb{I}} = W$, $\widetilde{\mathcal{L}}/a\widetilde{\mathcal{L}}$ has to be a free W-module, since W is a discrete valuation ring. Then we must have $\mathrm{rank}_W \widetilde{\mathcal{L}}/a\widetilde{\mathcal{L}} = 2$, which implies that, by Nakayama's lemma, $\widetilde{\mathcal{L}}$ is free of rank 2 over $\widetilde{\mathbb{I}}$. Thus if $\widetilde{\mathbb{I}}$ is a unique factorization domain, the condition (F) in the introduction holds.

By resolution of singularity (see [Lip78]), we have a complete regular local ring $\mathbb{I}^{sm} \subset Q(\mathbb{I})$ containing $\mathbb{I}$. The non-flat locus of π in $\mathrm{Spec}(\mathbb{I})$ is at most of codimension 2 (so, its support is the unique closed point $\mathfrak{m}$ of $\mathrm{Spec}(\mathbb{I})$). Writing E for the set of prime divisors of $\mathbb{I}^{sm}$ above the maximal ideal of $\mathbb{I}$ (those of exceptional divisors over the singular point $\mathfrak{m}_{\mathbb{I}} \in \mathrm{Spec}(\mathbb{I})$), the set of prime divisors of $\mathbb{I}$ is in bijection to prime divisors of $\mathbb{I}^{sm}$ outside E as $\mathrm{Spec}(\mathbb{I})\backslash\{\mathfrak{m}_{\mathbb{I}}\} \cong \mathrm{Spec}(\mathbb{I}^{sm})\backslash E$. Since $\mathbb{I}^{sm}$ is regular, it is a unique factorization domain (see [Mat86, Theorem 20.3]). Thus by the above argument, extending scalars W so that $\mathrm{Spec}(\mathbb{I}^{sm})(W) \neq \emptyset$, the reflexive $\mathbb{I}^{sm}$-closure L of $\mathbb{I}^{sm}\cdot\mathcal{L}_{\mathrm{can}}(\mathbb{I}) \subset Q(\mathbb{I})^2$ is free of rank 2 over $\mathbb{I}^{sm}$ and is stable under $\rho_{\mathbb{I}}$. We write $\rho_{\mathbb{I}^{sm}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{I}^{sm})$ for the Galois representation realized on L. Though for simplicity, we assume the condition ($\mathrm{F}_{\mathrm{can}}$) in this section, the divisibility conjecture we make should hold for $\mathbb{I}^{sm}$ ignoring primes in E taking $\rho_{\mathbb{I}^{sm}}$ in place of $\rho_{\mathbb{I}}$ without assuming ($\mathrm{F}_{\mathrm{can}}$).

Throughout this section we assume (R) and ($\mathrm{F}_{\mathrm{can}}$) in addition to $p \geqslant 5$ and that N is cube-free. Then by Theorem I, we have the conductor $\mathfrak{c}$ of $\mathrm{Im}(\rho_{\mathbb{I}}) \cap \mathrm{SL}_2(\Lambda)$. Here $\mathrm{Im}(\rho_{\mathbb{I}})$ is taken in $\mathrm{GL}_2(Q(\mathbb{I}))$. In order to determine the global level exactly, we need to know the characteristic power series of the congruence module between the CM part and the non-CM part and also the Eisenstein and non Eisenstein parts of $\mathrm{Spec}(\mathbb{T})$. A key ingredient of solving this question is Gorenstein-ness of each part (cf. Theorem 7.2). If different CM components or/and Eisenstein components are mixed, it is difficult to prove Gorenstein-ness of the CM/Eisenstein part. Writing $\overline{\rho}$ for $\rho_{\mathfrak{m}_{\mathbb{T}}}$, let us describe this problem in more detail. By Proposition 5.2, if $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\varphi} \cong \mathrm{Ind}_K^{\mathbb{Q}} \overline{\phi}$ for two distinct bimaginary quadratic fields, for the unique real quadratic field K', there exists a mod p character $\overline{\phi}'$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K')$ such that $\overline{\rho} \cong \mathrm{Ind}_{K'}^{\mathbb{Q}} \overline{\phi}'$. We separate our argument into the following five mixed cases which cover all possible cases (p-splitting imaginary quadratic fields involved) by Proposition 5.2:

- (EIS) $\overline{\rho} = \theta \oplus \psi$ with both $\overline{\theta}$ and $\overline{\psi}$ unramified at p with $\overline{\psi}/\overline{\theta}$ has order > 2;
- (UCM) absolutely irreducible $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\psi}$ for an imaginary quadratic field M with $\overline{\psi}$ unramified at p and $\overline{\psi}^-$ has order > 2;

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

(SCM) absolutely irreducible $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\varphi} \cong \mathrm{Ind}_K^{\mathbb{Q}} \overline{\phi} \cong \mathrm{Ind}_{K'}^{\mathbb{Q}} \overline{\phi}'$ for two p-splitting distinct imaginary quadratic fields M and K; so, $\varphi^- = (\frac{MK/M}{})$, $\phi^- = (\frac{MK/K}{})$ and $\phi'^- = (\frac{MK/K'}{})$;

(HCM) absolutely irreducible $\overline{\rho} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\varphi} \cong \mathrm{Ind}_K^{\mathbb{Q}} \overline{\phi} \cong \mathrm{Ind}_{K'}^{\mathbb{Q}} \overline{\phi}'$ for an imaginary quadratic field M in which p splits and an imaginary quadratic field K in which p is not split; so, $\varphi^- = (\frac{MK/M}{})$, $\phi^- = (\frac{MK/K}{})$ and $\phi'^- = (\frac{MK/K'}{})$;

(ECM) $\overline{\rho} = \overline{\theta} \oplus \overline{\psi} \cong \mathrm{Ind}_M^{\mathbb{Q}} \overline{\varphi}$ for a quadratic field M; so, $\overline{\psi}/\overline{\theta} = (\frac{M/\mathbb{Q}}{})$.

The five cases are disjoint, and M in case (ECM) is imaginary as $\overline{\psi}/\overline{\theta}$ is an odd character. Except for the case (ECM), we have well-defined $L(\mathbb{I})$ (see § 3). The difficulty of determining all possible cases of $\bar{\mathfrak{s}}_{\mathfrak{P}} \neq \mathfrak{sl}_2$ in these cases comes from the fact that some primes P with $\bar{\mathfrak{s}}_{\mathfrak{P}} \neq \mathfrak{sl}_2$ could be a prime of congruence between components of $U(p)$-deprived Hecke algebra $\mathbf{h}^{(p)} \subset \mathbf{h}$ generated by $T(l)$ ($l \nmid Np$) and $U(q)$ for $q \neq p$ over Λ. In order to determine exact level $L(\mathbb{I})$, we need to show that the local component $\mathbb{T}^{(p)}$ of $\mathbf{h}^{(p)}$ involved is Gorenstein up to finite error (which is not known and perhaps not expected in general either).

The Katz measure μ on $\mathfrak{Z}$ actually depends on the choice of p-adic CM type of the imaginary quadratic field M (i.e. a choice of $(M, \mathfrak{p})$ and $(M, \overline{\mathfrak{p}})$). Our choice is $(M, \mathfrak{p})$ for $\mathfrak{p}$ corresponding to $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. If we change $(M, \mathfrak{p})$ to $(M, \overline{\mathfrak{p}})$, we get another measure, μ^*. The two measures are related by a functional equation (e.g. [Hid10, Introduction]). We write $(L^-_{\psi^-})^*$ for the product of the Katz p-adic L-function with modulo p branch character ψ^- with respect to $(M, \overline{\mathfrak{p}})$. We may conjecture the following outcome in the above cases.

CONJECTURE 9.1. For the non-CM component $\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathbb{T})$ and a positive integer $m \gg 0$:

- in case (EIS), $L(\mathbb{I})$ is a factor of $L(\overline{\theta}, \overline{\psi}) \cdot L(\overline{\psi}, \overline{\theta})$;
- in case (UCM), $L(\mathbb{I})$ is a factor of $(L^-_{\overline{\psi}^-} \cdot (L^-_{\overline{\psi}^- \circ c})^*)^2$;
- in case (SCM), $L(\mathbb{I})$ is a factor of $(L^-_{\overline{\varphi}^-} \cdot L^-_{\overline{\phi}^-} \cdot (L^-_{\overline{\varphi}^- \circ c})^* \cdot (L^-_{\overline{\phi}^- \circ c})^* (t^{p^m} - 1))^2$;
- in case (HCM), $L(\mathbb{I})$ is a factor of

$$\begin{cases} (L^-_{\overline{\varphi}^-})^2 \cdot (t^{p^m} - 1)^2 & \text{if } \overline{\varphi}^- \text{ is ramified at } p, \\ (L^-_{\overline{\varphi}^-} \cdot (L^-_{\overline{\varphi}^- \circ c})^* \cdot (t^{p^m} - 1))^2 & \text{if } \overline{\varphi}^- \text{ is unramified at } p \end{cases}$$

  for a sufficiently large integer $m > 0$;
- in case (ECM), further suppose that $\overline{\theta\psi}$ has prime-to-p conductor N. For prime divisor $P \in \mathrm{Spec}(\Lambda)$ not under the intersection of a CM and an Eisenstein component, we can define local conductor $\mathfrak{c}_P$ as in § 3. For P under the intersection of a CM and an Eisenstein component, in the isomorphism class of $\rho_{\widetilde{\mathbb{I}}}$ realized on $\mathcal{L}_{\mathrm{can}}(\widetilde{\mathbb{I}}_P)$ over $\widetilde{\mathbb{I}}_P$, we can find ρ with maximal possible local conductor $\mathfrak{c}_P$. Then we have $(L(\mathbb{I})) = \Lambda \cap \bigcap_P \mathfrak{c}_P$ is a factor of $L(\overline{\theta}, \overline{\psi}) \cdot L(\overline{\theta}, \overline{\psi}) \cdot (L^-_{\overline{\varphi}^-} \cdot (L^-_{\overline{\varphi}^- \circ c})^*)^2$.

To explain our reasoning supporting this conjecture, we pick case (SCM). Then $\mathrm{Spec}(\mathbb{T})$ could contain two CM components $\mathrm{Spec}(\mathbb{T}^K_{\mathrm{cm}})$ and $\mathrm{Spec}(\mathbb{T}^M_{\mathrm{cm}})$. After inverting T, by Corollary 5.3, the connected component S of $\mathrm{Spec}(\mathbb{T}[1/T])$ containing $\mathrm{Spec}(\mathbb{I}[1/T])$ can have non-trivial intersection with $\mathrm{Spec}(\mathbb{T}^M_{\mathrm{cm}})$ for one choice M. There is a possible contribution from a non-CM component whose specialization at some $P|(t^{p^m} - 1)$ is an induced representation $\mathrm{Ind}_{K'}^{\mathbb{Q}} \phi'$ for the real quadratic field $K' \subset KM$. Then our argument proving Theorem 8.5 relative to an irreducible component $\mathbb{J}$ of $\mathbb{T}^M_{\mathrm{cm}}$ should go through after inverting $(t^{p^m} - 1)$ for a sufficiently large m. Thus, outside an exceptional divisor (containing $(t^{p^m} - 1)$ and the zero divisor of $E_{1,N}$ for M and

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

for K), the conjecture follows. The real challenge would be the analysis at primes inside the exceptional divisor. All other cases should be similar in the sense that the conjecture is provable outside an exceptional divisor.

10. Prime-to-p conductor of p-adic Galois representation

We summarize facts on ramification at a prime $q \neq p$ of p-adic Galois representations we have used. Let R be a p-profinite local ring. Let $M \subset \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}$ with integer ring $\mathfrak{O}$, and put $\widehat{\mathfrak{O}}^{(p)} = \prod_{l \neq p}(\mathfrak{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l)$. For any continuous character $\psi : M^\times \backslash M_{\mathbb{A}}^\times \to R^\times$ unramified outside Np, the restriction $\psi : (\widehat{\mathfrak{O}}^{(p)})^\times \to R^\times$ has to be a finite order character, as ψ is ramified only at finitely many primes and $R^\times$ is an almost p-profinite group. Thus we have an integral ideal $\mathfrak{C}(\psi)$ maximal among ideals $\mathfrak{a}$ prime to p with $(1 + \mathfrak{a}\widehat{\mathfrak{O}}^{(p)}) \cap (\widehat{\mathfrak{O}}^{(p)})^\times \subset \mathrm{Ker}(\psi)$. We call $\mathfrak{C}(\psi)$ the *prime-to-p conductor* of ψ. By local class field theory, a continuous character: $\mathrm{Gal}(\overline{\mathbb{Q}}/M) \to R^\times$ can be viewed as an idele character ψ, and hence the definition of $\mathfrak{C}(\psi)$ applies also to Galois characters. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting non-trivially on M leaving it stable, we define $\psi^\sigma : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to R^\times$ by $\psi^\sigma(\tau) = \psi(\sigma\tau\sigma^{-1})$. The idele character corresponding to the Galois character ψ^σ is given by composing ψ with the action of σ on $M_{\mathbb{A}}^\times$. For a rational prime $q \neq p$, the q-primary part $\mathfrak{C}_q(\psi)$ of $\mathfrak{C}(\psi)$ is called the q-conductor of ψ. Obviously, $\mathfrak{C}_q(\psi)$ only depends on ψ restricted to the inertia group at q, and therefore, $\mathfrak{C}_q(\psi)$ is well defined for any finite order character ψ of the inertia group. If $M = \mathbb{Q}$, we often identify the ideal $\mathfrak{C}_q(\psi) = (q^e)$ with the positive integer q^e.

Recall the exact sequence $1 \to I_q^w \to I_q \to I_q^t \to 0$ of the wild inertia group I_q^w and the tame inertia group $I_q^t \cong \widehat{\mathbb{Z}}^{(q)}$ which is an abelian group (e.g. [Hid00, § 3.2.5]).

LEMMA 10.1. *Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to \mathrm{GL}_2(R)$ be a continuous representation for a reduced p-profinite noetherian local ring R. Put $\rho_P = (\rho \bmod P)$ for $P \in \mathrm{Spec}(R)$. Suppose $q \neq p$.*

(1) *Unless $\rho_{\mathfrak{p}}|_{I_q}$ is reducible indecomposable for some minimal prime $\mathfrak{p}$ of R, $\rho|_{I_q}$ has finite image.*

(2) *If there exists a prime ideal P_0 of the p-profinite ring R such that ρ_{P_0} is absolutely irreducible over I_q^w, then for all prime ideals P of R, $\rho_P = (\rho \bmod P)$ is absolutely irreducible over I_q^w.*

(3) *Suppose that R is an integral domain. If $\rho|_{I_q^w}$ is reducible and ρ is absolutely irreducible, then $\rho \cong \mathrm{Ind}_K^{\mathbb{Q}_q} \xi$ for a character ξ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ of a quadratic extension $K/\mathbb{Q}_q$.*

(4) *If R is an integral domain and $\rho|_{I_q}$ is reducible indecomposable, we have $\rho \cong \left(\begin{smallmatrix}\mathcal{N}\eta & * \\ 0 & \eta\end{smallmatrix}\right)$ with $\eta|_{I_q}$ having finite order, where $\mathcal{N}$ is the unramified cyclotomic character acting on μ_{p^∞}.*

Proof. We first prove (1). Since $R \hookrightarrow \bigoplus_{\mathfrak{p}} R/\mathfrak{p}$ for finitely many minimal ideals $\mathfrak{p}$, replacing R by $R/\mathfrak{p}$, we may assume that R is an integral domain. Since $\rho|_{I_q^w}$ has finite image (factoring through $\mathrm{GL}_2(R/\mathfrak{m}_R)$) and $I_q = I_q^t \ltimes I_q^w$ by restricting ρ to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ for a finite extension $K/\mathbb{Q}_q$, we may assume that $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/K)}$ is reducible to prove (1). Let $I_K^w = I_q^w \cap \mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ and I_K^t be the image of $I_K = I_q \cap \mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ in I_q^t. Then $1 \to I_K^w \to I_K \to I_K^t \to 1$ is exact. Since $\rho(I_K^w)$ cannot contain a non-trivial unipotent element as $q \neq p$, $\rho|_{I_K^w} = \eta \oplus \xi$ for two finite order characters factoring through $(R/\mathfrak{m}_R)^\times$. Since I_K^t is cyclic, by [Hid00, Corollary 4.37], either $\rho_M := \rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q/M)} \cong \widetilde{\xi} \oplus \widetilde{\eta}$ for extensions $\widetilde{\xi}$ and $\widetilde{\eta}$ of ξ and η to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/M)$ for an extension M/K with $[M : K] \leqslant 2$ or $\rho(I_K)$ contains a non-trivial unipotent element of p-power order, which

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

is excluded by our assumption; thus $\rho_M \cong \widetilde{\xi} \oplus \widetilde{\eta}$. Replacing M by its finite extension, we may assume that $\widetilde{\xi}$ and $\widetilde{\eta}$ factor through I_M^t on which an element $\phi \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/M)$ surjecting down to the Frobenius element over M acts by $\phi\sigma\phi^{-1} = \sigma^Q$ for a q-power Q. Defining the inner conjugate ξ^ϕ by $\xi^\phi(\sigma) = \xi(\phi\sigma\phi^{-1})$, we have $\widetilde{\eta}^\phi = \widetilde{\eta}^Q = \widetilde{\eta}$. This implies $\widetilde{\eta}$ is of finite order; so, $\rho|_{I_q}$ has finite image. This proves (1).

By p-profiniteness of R, the residue field $R/\mathfrak{m}_R$ is finite for the maximal ideal $\mathfrak{m}_R$ of R. Since $\Gamma_R(\mathfrak{m}_R)$ is p-profinite, $q \neq p$ implies that $\rho|_{I_q^w}$ factors through $\mathrm{GL}_2(R/\mathfrak{m}_R)$. If $\rho_0|_{I_q^w}$ is absolutely irreducible, then $\overline{\rho}|_{I_q^w}$ is absolutely irreducible for $\overline{\rho} = \rho \bmod \mathfrak{m}_R$. Then we have $\rho_P|_{I_q^w}$ is absolutely irreducible for all $P \in \mathrm{Spec}(R)$. This proves (2).

We prove (4). Write $\rho|_{I_q} \cong \left(\begin{smallmatrix} \xi & u \\ 0 & \eta \end{smallmatrix}\right)$. Then $\rho^\phi|_{I_q} \cong \left(\begin{smallmatrix} \xi^\phi & u^\phi \\ 0 & \eta^\phi \end{smallmatrix}\right) \cong \rho|_{I_q}$ for a Frobenius $\phi \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. By indecomposability, we have $\eta^\phi = \eta^q = \eta$ over I_q; so, $\eta|_{I_q}$ is of finite order, and $u^\phi = qu$, which shows $\eta/\xi = \mathcal{N}$ for the cyclotomic character $\mathcal{N}$ giving the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ on μ_{p^∞}; so, $\mathcal{N}$ is unramified, and we get the desired result.

To prove (3), assume reducibility of $\rho|_{I_q^w}$. Since $q \neq p$, $\rho|_{I_q^w} \cong \xi \oplus \eta$. Then we have

$$\rho(\sigma) \begin{pmatrix} \xi & 0 \\ 0 & \eta \end{pmatrix} \rho(\sigma)^{-1} = \rho^\sigma \cong \begin{pmatrix} \xi^\sigma & 0 \\ 0 & \eta^\sigma \end{pmatrix}$$

for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. If $\xi^\sigma = \xi$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, absolutely irreducible ρ commutes with $\rho(I_q^w)$; so, we conclude $\xi = \eta$. We call this case Z. If $\xi^\sigma \cong \eta \neq \xi$, then its stabilizer is $\mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ for a quadratic extension $K/\mathbb{Q}_q$. We call this case D.

In case D, by [Ser77, Proposition 24 in § 8.1] (whose proof does not require $p \neq 0$ in R as long as $\rho|_{I_q^w}$ is semi-simple), $\rho \cong \mathrm{Ind}_K^{\mathbb{Q}} \widetilde{\xi}$ for a character $\widetilde{\xi}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ extending ξ as asserted.

Suppose that we are in case Z. Then $\rho(I_q^w)$ is in the center of $\rho(I_q)$. Since I_q^t is abelian and $\rho(I_q) = \rho(I_q^w) \rtimes \rho(I_q^t)$, $\rho(I_q)$ is an abelian group. Thus $\rho|_{I_q}$ is reducible. By (4), we have $\rho|_{I_q} = \xi \oplus \eta$. Then $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ acts on ξ and η by inner conjugation. If the stabilizer of ξ is a proper subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, we find a quadratic extension $K/\mathbb{Q}_q$ such that ρ is an induced representation as asserted. If the stabilizer is the entire group, $\xi = \eta$ and $\rho(I_q)$ is in the center of $\mathrm{Im}(\rho)$. Since $\mathrm{Im}(\rho) = \rho(I_q) \rtimes \langle \rho(\phi) \rangle$ for an element ϕ giving the Frobenius automorphism of the maximal unramified extension of $\mathbb{Q}_q$, $\mathrm{Im}(\rho)$ is abelian, contradicting the absolute irreducibility of ρ. This finishes the proof of (3). □

Suppose that R is an integral domain. We recall the conductor $C_q(\rho)$ of a two-dimensional Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to \mathrm{GL}_2(R)$ for a prime $q \neq p$ (e.g. [Hid11a, Theorem 5.1.9]). It only depends on the restriction of ρ to the inertia group $I_q \subset \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Regarding ρ having values in $\mathrm{GL}_2(Q(R))$ for the quotient field $Q(R)$ of R, we define $C_q(\rho) = q^e$ as follows. Let $\mathbb{Q}_q^{ur}$ be the maximal unramified extension of $\mathbb{Q}_q$ and K with integer ring V be the splitting field of $\rho|_{I_q}$. We put

$$I_i = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}_q^{ur}) \mid \sigma(x) \equiv x \bmod \mathfrak{m}_V^{i+1}\}.$$

Then we define

$$e = \sum_{i=0}^{\infty} \frac{1}{[I_0 : I_i]} (2 - \dim_{Q(R)} H^0(I_i, \rho)).$$

If $P_1 \supset P_2$ are two primes of R, $\dim_{\kappa(P_1)} H^0(I_i, \rho_{P_1}) \geqslant \dim_{\kappa(P_2)} H^0(I_i, \rho_{P_2})$; so, $C_q(\rho_{P_1}) \leqslant C_q(\rho_{P_2})$ for $\rho_{P_j} = \rho \bmod P_j$. If R is not an integral domain, we define

$$C_q(\rho) = \mathrm{Sup}_{P \in \mathrm{Spec}(R)} C_q(\rho_P).$$

Here are some explicit identifications of $C_q(\rho)$ (given in [Hid11a, Theorem 5.1.9]) when R is an integral domain. This covers all cases used in the proof of Theorem 8.5 (as $\overline{\rho}$ is an induced representation in Theorem 8.5). If $\rho|_{I_q}$ is isomorphic to a representation $\left(\begin{smallmatrix}\eta & * \\ 0 & \eta\end{smallmatrix}\right)$ over $Q(R)$, we have

$$C_q(\rho) = \begin{cases} q & \text{if } \eta \text{ is unramified and } \rho \text{ is indecomposable,} \\ \mathfrak{C}_q(\eta)^2 & \text{if } \eta \text{ is ramified.} \end{cases}$$

If $\rho_P \cong \alpha \oplus \beta$ for two characters $\alpha, \beta : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to R^\times$, the characters $\alpha|_{I_q}$ and $\beta|_{I_q}$ are of finite order. We then have $C_q(\rho) = \mathfrak{C}_q(\alpha)\mathfrak{C}_q(\beta)$. If ρ is absolutely irreducible and it has the form $\rho \cong \mathrm{Ind}_H^{I_q} \xi$ for an open subgroup H of I_q of index 2, writing (q^e) for the discriminant of the quadratic extension $\overline{\mathbb{Q}}_q^H/\overline{\mathbb{Q}}_q^{I_q}$, we have $C_q(\rho) = q^{e+f}$, where (q^f) is the norm relative to $\overline{\mathbb{Q}}_q^H/\overline{\mathbb{Q}}_q^{I_q}$ of the conductor $\mathfrak{C}_q(\xi)$ of ξ.

For an automorphic representation π generated by a holomorphic Hecke eigenform f, we have its p-adic Galois representation $\rho_f = \rho_\pi$ (e.g. [Hid11a, § 4.2]). Then $C_q(\rho_f)$ coincides with the q-part of the conductor $C_q(\pi)$ of π in the sense of [Gel75, Theorem 4.24] (see also [Car86] for $C_q(\rho_f) = C_q(\pi)$).

Lemma 10.2. *Suppose that R is a reduced p-profinite local ring. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to \mathrm{GL}_2(R)$ be a continuous representation. Then:*

(1) *for any prime ideal P of R containing a minimal prime $\mathfrak{p}$, we have $C_q(\rho_P) \leqslant C_q(\rho)$;*

(2) *suppose that R is an integral domain in which $p \neq 0$. Then unless $\rho|_{I_q}$ is reducible indecomposable, for any point $P \in \mathrm{Spec}(R[1/p])$, $C_q(\rho_P)$ is independent of P, in particular, $C_q(\rho_P) = C_q(\rho)$;*

(3) *suppose that $\mathrm{Spec}(R) = \mathrm{Spec}(I) \cup \mathrm{Spec}(J)$ for two irreducible components $\mathrm{Spec}(I)$ and $\mathrm{Spec}(J)$. If $\mathrm{Spec}(I[1/p]) \cap \mathrm{Spec}(J[1/p])$ contain a prime P_0 and $\rho_{\mathfrak{p}}|_{I_q}$ is not reducible indecomposable for the two minimal prime ideals $\mathfrak{p}$ of R, $C_q(\rho_P)$ is independent of $P \in \mathrm{Spec}(R[1/p])$, in particular, $C_q(\rho_P) = C_q(\rho)$;*

(4) *if P is a prime ideal of R with $\kappa(P)$ having characteristic 0 and $\rho_{\mathfrak{p}}|_{I_q}$ is not reducible indecomposable for each minimal prime ideal $\mathfrak{p}$ of R_P, then $C_q(\rho_{P'}) = C_q(\rho_P)$ for any prime ideal P' of the localization R_P.*

Proof. The first assertion follows directly from the definition, and the third is the special case of the second. For assertions (2) and (3), we note that $\rho|_{I_q}$ has finite image under the assumption. If R is an integral domain and $p \notin P$ for $P \in \mathrm{Spec}(R)$, $1 + PR = R \cap (1 + PR_P)$ is a torsion-free group; so, $\rho_P(I_q) \cong \rho(I_q)$. In particular, we have, for any subgroup $I \subset I_q$, $\dim_{Q(R)} H^0(I, \rho) = \dim_{\kappa(P)} H^0(I, \rho_P)$, which implies $C_q(\rho) = C_q(\rho_P)$, proving (2).

As for (3), writing $I = R/\mathfrak{p}$ and $J = R/\mathfrak{q}$, by (2), $C_q(\rho_P)$ is constant for all $P \in \mathrm{Spec}(I[1/p])$ and $C_q(\rho_Q)$ is independent of $Q \in \mathrm{Spec}(J[1/p])$. We have $C_q(\rho_P) = C_q(\rho_{\mathfrak{p}}) = C_q(\rho_{P_0}) = C_q(\rho_{\mathfrak{q}}) = C_q(\rho_Q)$.

Assertion (4) follows from (3). Note that $R_P[1/p] = R_P$ as $\kappa(P)$ has characteristic 0. For any two irreducible components $\mathrm{Spec}(I) = \mathrm{Spec}(R_P/\mathfrak{p})$ and $\mathrm{Spec}(J) = \mathrm{Spec}(R_P/\mathfrak{q})$ of $\mathrm{Spec}(R_P)$, we have $P \in \mathrm{Spec}(I) \cap \mathrm{Spec}(J)$; so, $C_q(\rho_{\mathfrak{p}}) = C_q(\rho_{\mathfrak{q}}) = C_q(\rho_P)$. For any P', taking a minimal prime ideal $\mathfrak{q}$ contained in P', we get $C_q(\rho_{P'}) = C_q(\rho_{\mathfrak{q}}) = C_q(\rho_P)$. This finishes the proof. □

We call a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ minimal if $C_q(\rho \otimes \chi) \geqslant C_q(\rho)$ for any finite order character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$.

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

Lemma 10.3. *Let R be a p-profinite noetherian integral domain and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \to \mathrm{GL}_2(R)$ be a semi-simple representation. Let $\overline{\rho} = (\rho \bmod \mathfrak{m}_R)$.*

(1) If $\overline{\rho}|_{I_q} \cong \overline{\xi} \oplus \overline{\eta}$ for two characters $\overline{\xi}$ and $\overline{\eta}$ of I_q, then $\rho|_{I_q} \cong \xi \oplus \eta$ for two characters ξ and η. If further ρ is minimal and one of ξ and η extends to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, one of ξ and η is unramified, and $\overline{\rho}$ is minimal.

(2) Suppose that $\overline{\rho} \cong \overline{\xi} \oplus \overline{\eta}$ for two characters $\overline{\xi}$ and $\overline{\eta}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. If ρ is absolutely irreducible, $q \equiv 1 \bmod p$. If further ρ is minimal, $\overline{\rho}$ and $\overline{\xi}$ are unramified at q (so, $\overline{\rho}$ is minimal), and $\overline{\xi}/\overline{\eta}$ has order 2.

(3) Suppose that $\overline{\rho} \cong \overline{\xi} \oplus \overline{\eta}$ for two characters $\overline{\xi}$ and $\overline{\eta}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. If ρ is reducible minimal isomorphic to $\xi \oplus \eta$, one of ξ and η is unramified, and $\overline{\rho}$ is minimal. If $\overline{\rho}$ is unramified but ρ is ramified, we again have $q \equiv 1 \bmod p$.

(4) Assume that $p \neq 0$ in R. Suppose that either $\overline{\rho} \cong \overline{\eta} \oplus \overline{\xi}$ or $\overline{\rho} \cong \mathrm{Ind}_K^{\mathbb{Q}_q} \overline{\xi}$ for a quadratic extension $K/\mathbb{Q}_q$. If $C_q(\overline{\rho}) < C_q(\rho)$ and ρ is minimal, we have $q^j \equiv 1 \bmod p$, where $j = 1$ if $\overline{\rho} \cong \overline{\eta} \oplus \overline{\xi}$ or K is ramified and $j = 2$ if K is unramified.

Proof. We first prove assertion (1). If $\rho|_{I_q}$ is absolutely irreducible, by Lemma 10.1(3), we have either (i) $\rho|_{I_q^w}$ is absolutely irreducible or (ii) $\rho \cong \mathrm{Ind}_K^{\mathbb{Q}_q} \xi$ for a character ξ and a ramified quadratic extension $K/\mathbb{Q}_q$. Case (i) does not occur as $\rho|_{I_q^w}$ factors through $\overline{\rho}$. Suppose that we are in case (ii) and that $\rho|_{I_q}$ is absolutely irreducible. Then we have $\xi^{1-\sigma} \equiv 1 \bmod \mathfrak{m}_R$ for $\sigma \in I_q$ non-trivial over K, as $\overline{\rho}|_{I_q}$ is reducible. Then by local class field theory, $\xi^{1-\sigma}$ can be regarded as a character of $O^\times$ for the integer ring O of K. By irreducibility of $\rho|_{I_q}$, $\xi^{1-\sigma} \neq 1$ with $\xi^{1-\sigma} \equiv 1 \bmod \mathfrak{m}_R$. Thus $\xi^{1-\sigma}$ has p-power order. Since $O^\times$ is a q-profinite group times $\mathbb{F}_q^\times$ (as K is ramified over $\mathbb{Q}_q$), $\xi^{1-\sigma}$ factors through $\mathbb{F}_q^\times$. Any character of $O^\times$ factoring through $\mathbb{F}_q^\times$ is σ-invariant; so, $\xi^{1-\sigma}|_{I_q} = 1$. Thus $\mathrm{Ind}_K^{\mathbb{Q}} \xi|_{I_q}$ is reducible, a contradiction. Thus $\rho|_{I_q} \cong \xi \oplus \eta$. If one of ξ and η extends to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, the two characters extend to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ as $\det(\rho)$ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Then we must have $\rho = \xi \oplus \eta$ for suitable choice of extensions. By the minimality, one of η and ξ is unramified; so, one of $\overline{\xi}$ and $\overline{\eta}$ is unramified. This implies that $\overline{\rho}$ is minimal as well. This finishes the proof of (1).

We now prove (2). By (1), $\rho|_{I_q} \cong \xi \oplus \eta$ with $\overline{\xi} = \xi \bmod \mathfrak{m}_R$. Since ρ is absolutely irreducible, by Lemma 10.1(3), we have $\rho \cong \mathrm{Ind}_K^{\mathbb{Q}_q} \xi$ for a character ξ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ extending the character ξ of $I_q \cap \mathrm{Gal}(\overline{\mathbb{Q}}_q/K)$ for a quadratic extension $K/\mathbb{Q}_q$. If $K/\mathbb{Q}_q$ is ramified, $\xi^\sigma = \xi$ for $\sigma \in I_q$ non-trivial on K; so, ρ is reducible, a contradiction. Thus $K/\mathbb{Q}_q$ is unramified. Take $\phi \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ giving rise to q-th power Frobenius modulo q. Then ϕ is non-trivial on K, we have $\xi^{1-\phi} \equiv 1 \bmod \mathfrak{m}_R$ and $\overline{\xi}/\overline{\eta} = (\frac{K/\mathbb{Q}_q}{})$ as $\overline{\rho} \cong \overline{\xi} \oplus \overline{\eta}$. Thus $\xi^{1-\phi}$ is a p-power order character. Note that $\xi|_{I_q}$ has finite order. Write $\xi|_{I_q} = \xi_p \xi^{(p)}$ so that ξ_p has p-power order and $\xi^{(p)}$ has order prime to p. Then $\xi_p^{1-\phi} = \xi^{1-\phi}$ and $(\xi^{(p)})^{1-\phi} = 1$, since $\xi^{1-\phi}$ has p-power order. Thus $\xi^{(p)}$ extends to a finite order character Ξ of $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. Then $\rho \otimes \Xi^{-1}$ has less conductor than ρ. Since $\rho \otimes \Xi^{-1}$ is absolutely irreducible, it is ramified; so, ξ_p is non-trivial. Since ϕ acts on I_q^t by the cyclotomic character (e.g. [Hid00, p. 123]), we have $\xi_p^{\phi-1} = \xi_p^{q-1} = 1$ which implies $q \equiv 1 \bmod p$. By minimality of ρ, we conclude $\Xi|_{I_q} = \xi^{(p)} = 1$, and $\xi|_{I_q}$ has order p-power. Thus $\overline{\xi}|_{I_q} = 1$ and hence, $\overline{\rho} = 1 \oplus (\frac{K/\mathbb{Q}_q}{})$, which is unramified, and $\overline{\xi}/\overline{\eta} = (\frac{K/\mathbb{Q}_q}{})$ has order 2. This finishes the proof of (2).

We prove (3). If ρ is reducible, by semi-simplicity of ρ, we have $\rho \cong \xi \oplus \eta$. By minimality of ρ, one of ξ and η is unramified, and hence $\overline{\rho}$ is minimal. If further $\overline{\rho}$ is unramified while ρ

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press

is ramified, one of the characters ξ and η non-trivial on I_q become trivial modulo $\mathfrak{m}_R$; so, $q \equiv 1 \bmod p$.

To see (4), we note that under $p \nmid (q-1)$ and minimality of ρ, ρ is absolutely irreducible if and only if $\overline{\rho}$ is absolutely irreducible by (2). If $\rho \cong \eta \oplus \xi$ and $\overline{\rho} = \overline{\xi} \oplus \overline{\eta}$ with $\overline{\eta} = (\eta \bmod \mathfrak{m}_R)$, for the Teichmüller lift $\widetilde{\xi}$ of $\overline{\xi}$ and $\widetilde{\eta}$ of $\overline{\eta}$, $C_q(\rho) > C_q(\overline{\rho})$ implies that one of $\xi\widetilde{\xi}^{-1}$ and $\eta\widetilde{\eta}^{-1}$, say $\xi\widetilde{\xi}^{-1}$, is non-trivial over I_q^t of p-power order. Then $1 = (\xi\widetilde{\xi}^{-1})^{1-\phi} = (\xi\widetilde{\xi}^{-1})^{1-q}$ implies $q \equiv 1 \bmod p$. Now suppose that $\rho \cong \mathrm{Ind}_K^{\mathbb{Q}_q} \xi$ is absolutely irreducible. Then for $\overline{\xi} = (\xi \bmod \mathfrak{m}_R)$, $\overline{\xi}^{1-\sigma} \neq 1$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ non-trivial on the quadratic extension K. If K is ramified, again $C_q(\rho) > C_q(\overline{\rho})$ implies $1 = (\xi\widetilde{\xi}^{-1})^{1-\phi} = (\xi\widetilde{\xi}^{-1})^{1-q}$ as we can choose the Frobenius ϕ inducing identity on K. If K is unramified, by the same argument, $q^2 \equiv 1 \bmod p$ as the Frobenius over K acts on I_q^t by $\sigma \mapsto \sigma^{q^2}$.

By Lemma 10.1(3), the remaining case is when $\rho|_{I_q^w}$ is irreducible but ρ is not induced. Since $\rho|_{I_q^w}$ factors through $\overline{\rho}$ which is induced, $\rho(I_q^w)$ is a dihedral group (as $\rho|_{I_q^w}$ is irreducible). Since 2 is a factor of the order of the dihedral group $\rho(I_q^w)$, we conclude $q = 2$. Since $\rho(I_q^w)$ is dihedral, $\rho|_{I_2^w} \cong \mathrm{Ind}_I^{I_2^w} \xi$ for an index 2 subgroup I of I_2^w. By [Wei74], the image G of $\mathrm{Im}(\rho)$ in $\mathrm{PGL}_2(R)$ is isomorphic either to S_4 or A_4. We have an isomorphism $S_4/V \cong S_3$ for the unique $(2,2)$-subgroup V. Let L be the extension of $\mathbb{Q}_2$ such that $\mathrm{Gal}(L/\mathbb{Q}_q) \cong G$ by ρ. Then L has subfield M with $\mathrm{Gal}(L/M) = V$. By [Kut80, § 5.1], we have $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_2/M)} \cong \mathrm{Ind}_{L'}^M \xi$ for any of three quadratic extensions L' of M in L. Since $p \neq 2$, $V \cap G$ has to inject into $\overline{G}$. Thus $\overline{G}$ has to be isomorphic to S_4 or A_4, a contradiction, since $\overline{G}$ is dihedral. Therefore, this case cannot happen, hence we get (4). □

For a global representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R)$, assuming that ρ only ramifies at finitely many places (so, $C_q(\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q)/\mathbb{Q}_q)}) = 1$ for almost all $q \neq p$), we define its prime-to-p conductor by $C(\rho) = \prod_{q \neq p} C_q(\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_q)/\mathbb{Q}_q)})$. All Galois representations we studied in this paper ramify only at finitely many primes; so, it has a well-defined conductor. A global Galois representation ρ as above is called minimal if $C(\rho)$ is minimal among $C(\rho \otimes \xi)$ for all finite order Galois characters ξ.

Lemma 10.4. *Let R be a p-profinite integral domain and $\Psi : \mathrm{Gal}(\overline{\mathbb{Q}}/M) \to R^\times$ be a character with prime-to-p conductor $\mathfrak{C}$ for an imaginary quadratic field M. If $\mathrm{Ind}_M^{\mathbb{Q}} \Psi$ is minimal at primes q split in M, we have $\mathfrak{F}_c = \mathfrak{O}$ for the decomposition $\mathfrak{C} = \mathfrak{F}\mathfrak{F}_c\mathfrak{I}$ in Definition 6.1.*

Proof. If $\mathfrak{F}_c \neq \mathfrak{O}$, we have a rational prime q such that $(q) \mid \mathfrak{F}\mathfrak{F}_c$. Since $\mathfrak{F} + \mathfrak{F}_c = \mathfrak{O}$ and $\mathfrak{F} \subset \mathfrak{F}_c^c$, we can split $(q) = \mathfrak{Q}\mathfrak{Q}^c$ in M so that $\mathfrak{Q}|\mathfrak{F}$. Then identifying I_q with $I_{\mathfrak{Q}^c}$, we may regard $\Psi|_{I_{\mathfrak{Q}^c}}$ as a character of I_q. Since the image of I_q in $\mathrm{Gal}(\mathbb{Q}_q^{ab}/\mathbb{Q}_q)$ for the maximal abelian extension $\mathbb{Q}_q^{ab}/\mathbb{Q}_q$ is isomorphic to $\mathrm{Gal}(\mathbb{Q}_q[\mu_{q^\infty}]/\mathbb{Q}_q) \cong \mathbb{Z}_q^\times$, we have a global Galois character $\xi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to R^\times$ unramified outside q and $\xi|_{I_q} = \Psi|_{I_q}$. Then we have, for q-primary parts,

$$C_q((\mathrm{Ind}_M^{\mathbb{Q}} \Psi) \otimes \xi^{-1}) \supset \mathfrak{F}_q \supsetneq (\mathfrak{F}\mathfrak{F}_c)_q = C_q(\mathrm{Ind}_M^{\mathbb{Q}} \Psi)$$

contradicting minimality of $\mathrm{Ind}_M^{\mathbb{Q}} \Psi$. □

Acknowledgement

The author is partially supported by the NSF grants DMS 0753991 and DMS 0854949.

References

Bou98 N. Bourbaki, *Algèbre commutative* (Hermann, Paris, 1961–1998).

Bro82 K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87 (Springer, New York, 1982).

Car86 H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Éc. Norm. Supér. (4) **19** (1986), 409–468.

Car94 H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local compact*, Contemp. Math. **165** (1994), 213–237.

Fis02 A. Fischman, *On the image of Λ-adic Galois representations*, Ann. Inst. Fourier (Grenoble) **52** (2002), 351–378.

Gel75 S. S. Gelbart, *Automorphic forms on adele groups*, Annals of Mathematics Studies, vol. 83 (Princeton University Press, Princeton, NJ, 1975).

GV04 E. Ghate and V. Vatsal, *On the local behaviour of ordinary $\mathbb{I}$-adic representations*, Ann. Inst. Fourier (Grenoble) **54** (2004), 2143–2162.

Hid86a H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. Éc. Norm. Supér. (4) **19** (1986), 231–273.

Hid86b H. Hida, *Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. **85** (1986), 545–613.

Hid86c H. Hida, *Hecke algebras for GL_1 and GL_2, Sém. de Théorie des Nombres, Paris 1984–85*, Progr. Math. **63** (1986), 131–163.

Hid88 H. Hida, *Modules of congruence of Hecke algebras and L-functions associated with cusp forms*, Amer. J. Math. **110** (1988), 323–382.

Hid93 H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts, vol. 26 (Cambridge University Press, Cambridge, 1993).

Hid00 H. Hida, *Modular forms and galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 69 (Cambridge University Press, Cambridge, 2000).

Hid09 H. Hida, *Quadratic exercises in Iwasawa theory*, Int. Math. Res. Notices IMRN **2009** (2009), 912–952; doi:10.1093/imrn/rnn151.

Hid10 H. Hida, *The Iwasawa μ-invariant of p-adic Hecke L-functions*, Ann. of Math. (2) **172** (2010), 41–137.

Hid11a H. Hida, *Geometric modular forms and elliptic curves*, second edition (World Scientific Publishing Co., Singapore, 2011).

Hid11b H. Hida, *Hecke fields of analytic families of modular forms*, J. Amer. Math. Soc. **24** (2011), 51–80.

Hid11c H. Hida, *Constancy of adjoint $\mathcal{L}$-invariant*, J. Number Theory **131** (2011), 1331–1346.

Hid13a H. Hida, *Image of Λ-adic Galois representations modulo p*, Invent. Math. **194** (2013), 1–40.

Hid13b H. Hida, *Local indecomposability of Tate modules of non-CM abelian varieties with real multiplication*, J. Amer. Math. Soc. **26** (2013), 853–877.

HT93 H. Hida and J. Tilouine, *Anticyclotomic Katz p-adic L-functions and congruence modules*, Ann. Sci. Éc. Norm. Supér. (4) **26** (1993), 189–259.

HT94 H. Hida and J. Tilouine, *On the anticyclotomic main conjecture for CM fields*, Invent. Math. **117** (1994), 89–147.

Kat78 N. M. Katz, *p-adic L-functions for CM fields*, Invent. Math. **49** (1978), 199–297.

Kut80 P. Kutzko, *The Langlands conjecture for Gl_2 of a local field*, Ann. of Math. (2) **112** (1980), 381–412.

Lip78 J. Lipman, *Desingularization of two-dimensional schemes*, Ann. of Math. (2) **107** (1978), 151–207.

Mat86 H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8 (Cambridge University Press, New York, 1986).

Maz89 B. Mazur, *Deforming Galois representations*, in *Galois group over* $\mathbb{Q}$, Mathematical Sciences Research Institute Publications 16 (Springer, Berlin, 1989), 385–437.

MT90 B. Mazur and J. Tilouine, *Représentations galoisiennes, différentielles de Kähler et 'conjectures principales'*, Publ. Math. Inst. Hautes Études Sci. **71** (1990), 65–103.

MW86 B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Math. **59** (1986), 231–264.

Miy89 T. Miyake, *Modular forms*, Springer Monographs in Mathematics (Springer, 1989).

Mom81 F. Momose, *On the l-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 89–109.

Oht99 M. Ohta, *Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves*, Compositio Math. **115** (1999), 241–301.

Oht00 M. Ohta, *Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. II*, Math. Ann. **318** (2000), 557–583.

Oht03 M. Ohta, *Congruence modules related to Eisenstein series*, Ann. Sci. Éc. Norm. Supér. (4) **36** (2003), 225–269.

Pin93 R. Pink, *Classification of pro-p subgroups of* SL_2 *over a p-adic ring, where p is an odd prime*, Compositio Math. **88** (1993), 251–264.

Rib75 K. A. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275.

Rib76 K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162.

Rib85 K. A. Ribet, *On l-adic representations attached to modular forms. II*, Glasg. Math. J. **27** (1985), 185–194.

Rub88 K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **93** (1988), 701–713.

Sch07 I. Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **29** (1907), 85–137.

Ser77 J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42 (Springer, 1977).

Shi71 G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Iwanami-Shoten and Princeton University Press, 1971).

SW99 C. M. Skinner and A. J. Wiles, *Residually reducible representations and modular forms*, Publ. Math. Inst. Hautes Études Sci. **89** (1999), 5–126.

Til89 J. Tilouine, *Sur la conjecture principale anticyclotomique*, Duke Math. J. **59** (1989), 629–673.

Vig89 M.-F. Vignéras, *Représentations modulaires de* $\mathrm{GL}(2,F)$ *en caractéristique* l, F *corps p-adique,* $p \neq l$, Compositio Math. **72** (1989), 33–66.

Wei74 A. Weil, *Exercices dyadiques*, Invent. Math. **27** (1974), 1–22; Œuvres III, [1974e]).

Zas99 H. Zassenhaus, *The theory of groups* (Courier Dover, 1999).

Zha12 B. Zhao, *Local indecomposability of Hilbert modular Galois representations*, Ann. Inst. Fourier (Grenoble) to appear; arXiv:1204.4007v1 [math.NT].

Haruzo Hida hida@math.ucla.edu
Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, USA

https://doi.org/10.1112/S0010437X14007684 Published online by Cambridge University Press