BOLLETTINO
UNIONE MATEMATICA ITALIANA

Miriam Ciavarella

Eisenstein ideal and reducible λ-adic Representations Unramified Outside a Finite Number of Primes.

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **9-B** (2006), n.3, p. 711–721.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2006_8_9B_3_711_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2006.

Bollettino U. M. I.
(8) **9**-B (2006), 711-721

Eisenstein Ideal and Reducible λ-adic Representations Unramified Outside a Finite Number of Primes.

Miriam Ciavarella

Sunto. – *L'argomento di questo articolo è lo studio di particolari rappresentazioni λ-adiche bidimensionali di* $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$*; fissati* $p_1, \ldots, p_n$ *primi distinti, considereremo rappresentazioni* $\rho : G \to GL_2(A)$*, date dalla matrice* $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *che sono non ramificate fuori* $p_1, \ldots, p_n, \infty$ *e dalla caratteristica residua di* λ*, che sono prodotto di m rappresentazioni su estensioni finite dell'anello dei vettori di Witt del campo residuo e che sono riducibili modulo* λ*. In analogia con la teoria delle rappresentazioni modulari, introdurremo l'analogo dell'algebra di Hecke di Mazur* $\boldsymbol{T}$*, con un ideale* I *di* $\boldsymbol{T}$ *che chiameremo ideale di Eisenstein.*
Seguendo la strategia di Ribet e Papier [3]*, sotto le ipotesi:*

- $p_i \not\equiv 1 \bmod \ell$*, per ogni* $i = 1, \ldots, n$*,*
- *la semisemplificazione di* $\overline{\rho}$ *è descritta da due caratteri* α*,* β *che sono distinti se ristretti a* $\boldsymbol{Z}_\ell^\times$*,*

otterremo i seguenti risultati:

Proposizione 0.1 – *L'ideale di Eisenstein* I *è uguale a* BC*, dove* B *è il* $\boldsymbol{T}$*-sottomodulo di* A *generato da tutti i* $b(g)$ *con* $g \in G$ *e analogamente* C *è definito usando i* $c(g)$*. Inoltre,* I *è l'deale di* $\boldsymbol{T}$ *generato dalle quantitá* $a(h) - 1$ *per* $h \in \mathrm{Gal}(K/\boldsymbol{Q}^{\mathrm{ab}} \cap K)$*.*

Proposizione 0.2 – *Supponiamo che la congettura di Vandiver sia vera per* ℓ *e che* I *sia non-zero. Allora, a meno di sostituire* ρ *con un coniugato, la rappresentazione* ρ *assume valori in* $GL_2(\boldsymbol{T})$ *e la sua matrice dei coefficienti soddisfa:*

$$a \equiv \varphi, \quad d \equiv \psi, \quad c \equiv 0 \pmod{I}$$

dove $\varphi \equiv \alpha \bmod \mathcal{M}$ *e* $\psi \equiv \beta \bmod \mathcal{M}$*, per* $\mathcal{M} = \boldsymbol{T} \cap (\lambda)$*.*

In particolare esiste uno e uno solo omomorfismo di anelli suriettivo dall'anello di deformazione universale $\mathcal{R}(\overline{\rho})$ *in* $\boldsymbol{T}$*, che induce l'isomorfismo identitá sui campi residui.*

Summary. – *The object of this note is to study certain 2-dimensional λ-adic representations of* $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$*; fixed* $p_1, \ldots, p_n$ *distinct primes, we will consider representations* $\rho : G \to GL_2(A)$*, given by the matrix* $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *which are unramified outside* $p_1, \ldots, p_n, \infty$ *and the residue characteristic of* λ*, which are a product*

of m representations over finite extensions of the ring of Witt vectors of the residue field and which are reducible modulo λ. In analogy with the theory of the modular representations, we will introduce the analogue of Mazur's Hecke algebra $\boldsymbol{T}$, together with an ideal I of $\boldsymbol{T}$ which we will call the Eisenstein ideal.
Following the Ribet and Papier's method [3], *under the hypotheses:*

- $p_i \not\equiv 1 \bmod \ell$, *for any* $i = 1, ..., n$,
- *the semisimplification of* $\overline{\rho}$ *is described by two characters* α, β *which are distinct if restricted to* $\boldsymbol{Z}_\ell^\times$,

we obtain the following results:

PROPOSITION 0.3 – *The Eisenstein ideal I is equal to BC, where B is the $\boldsymbol{T}$-submodule of A generated by all $b(g)$ with $g \in G$ and similary C is defined using the $c(g)$'s. Moreover, I is the ideal of $\boldsymbol{T}$ generated by the quantities $a(h) - 1$ for $h \in \mathrm{Gal}(K/\boldsymbol{Q}^{\mathrm{ab}} \cap K)$.*

PROPOSITION 0.4 – *Suppose that Vandiver's conjecture is true for ℓ and that I is non-zero. Then, after replacement of ρ by a conjugate, the representation ρ takes values in $GL_2(\boldsymbol{T})$ and its matrix coefficients satisfy:*

$$a \equiv \varphi, \quad d \equiv \psi, \quad c \equiv 0 \pmod{I}$$

where $\varphi \equiv \alpha \bmod \mathcal{M}$ and $\psi \equiv \beta \bmod \mathcal{M}$, for $\mathcal{M} = \boldsymbol{T} \cap (\lambda)$.

In particular there is one and only one surjective ring homomorphism from the universal deformation ring $\mathcal{R}(\overline{\rho})$ to $\boldsymbol{T}$, inducing the identity isomorphism on residue fields.

1. – Introduction.

Recent studies about the deformation theory of Galois representations compare an universal deformation ring $\mathcal{R}$ with an Hecke algebra $\boldsymbol{T}$; the most important example is the Wiles and Taylor-Wiles Theorem, which establishes an isomorphism between $\mathcal{R}$ and $\boldsymbol{T}$ in some special cases.

The object of this note is to generalize a result of Kennet A. Ribet and E. Papier [3], establishing a surjective homomorphism from an universal deformation ring $\mathcal{R}$ to an Hecke algebra $\boldsymbol{T}$ generated by traces.

Let $\ell, p_1, ..., p_n$ be (n+1) odd primes. Let $\overline{\boldsymbol{Q}}$ be an algebraic closure for $\boldsymbol{Q}$ and let $K_\ell \subset \overline{\boldsymbol{Q}}$ be the largest extension of $\boldsymbol{Q}$ which is unramified away from ℓ and infinity and let, for $i = 1, ..., n$, $K_{p_i} \subset \overline{\boldsymbol{Q}}$ be the largest extension of $\boldsymbol{Q}$ which is unramified away from p_i and infinity; we consider the compositum field $K = K_\ell K_{p_1} ... K_{p_n}$. Let $G = \mathrm{Gal}(K/\boldsymbol{Q})$. Let k be a finite field extension of $\mathbf{F}_\ell$, let $W(k)$ be the ring of Witt vectors of k, and for $i = 1, .., m$ let $\mathcal{O}_i$ be a finite extension of $W(k)$ with residue field equal to k and maximal ideal equal to (λ_i). For $j = 1, .., m$ let $\rho_j : G \to GL_2(\mathcal{O}_j)$ be a continuous 2-dimensional λ_j-adic representation of $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$, unramified outside $\ell, p_1, ..., p_n, \infty$, such that $\overline{\rho}_j = \overline{\rho}_{j'}$ for

$j, j' = 1, ..., m$. We shall consider the situation in which $\overline{\rho}_j$ is reducible. Let A be the fiber product of the $\mathcal{O}_j$'s

$$A = \left\{ (x_j) \in \prod_j \mathcal{O}_j : \overline{x}_j = \overline{x}_{j'} \text{ for all } j, j' \right\}$$

where $\overline{x}_j$ denotes the image of x_j in k. So A is local and the product of the ρ_j provides a continuous 2-dimensional λ-adic representation

$$\rho : G \to GL_2(A)$$

unramified outside $\ell, p_1, ..., p_n, \infty$ such that $\overline{\rho} = \overline{\rho}_j : G \to GL_2(k)$; so ρ is reducible modulo the maximal ideal (λ) of A, where $\lambda = (\lambda_1, ..., \lambda_m)$ of A. We shall write $\overline{\rho}^{ss}$ for the semisimplification of $\overline{\rho}$, which does not depend on the particular integer model for ρ. So $\overline{\rho}^{ss}$ is described by two characters

$$\alpha, \beta : G \to k^{\times}.$$

As our general hypothesis, we will suppose that α and β are distinct if restricted to $\boldsymbol{Z}_{\ell}^{\times}$.

For any $g \in G$, we will write $\mathrm{tr}(g)$ and $\det(g)$ instead of $\mathrm{tr}(\rho(g))$ and $\det(\rho(g))$ respectively.

2. – Hecke algebra.

Our Hecke algebra $\boldsymbol{T}$ will be the $W(k)$-subalgebra of A generated by the quantities $\mathrm{tr}(\rho(g))$ with $g \in G$. So $\boldsymbol{T}$ is a local $\boldsymbol{Z}_{\ell}$-algebra with maximal ideal $\mathcal{M} = \boldsymbol{T} \cap (\lambda)$, with residue field $\boldsymbol{T}/\mathcal{M} \cong k$, finitely generated, without nihilpotent elements but possibly with zero divisors.

As a $W(k)$-module (therefore as a $\boldsymbol{Z}_{\ell}$-module) $\boldsymbol{T}$ is free of finite rank; it is therefore complete and separated with respect to its (ℓ)-adic topology. Therefore the (ℓ)-adic topology on $\boldsymbol{T}$ coincides with the $\mathcal{M}$-adic topology on $\boldsymbol{T}$. In fact from the inclusion $\ell\boldsymbol{T} \subseteq \mathcal{M}$, we deduce $\ell^n\boldsymbol{T} \subseteq \mathcal{M}^n$ for all n. Conversely we consider the noetherian finite local ring $\boldsymbol{T}/\ell\boldsymbol{T}$ (it is finite because $\boldsymbol{T}$ is finitely generated on $\boldsymbol{Z}_{\ell}$). Let $\overline{\mathcal{M}}$ be the maximal ideal of $\boldsymbol{T}/\ell\boldsymbol{T}$. So $\overline{\mathcal{M}}$ is a vector $\mathbf{F}_{\ell}$-subspace $\overline{\mathcal{M}} \subseteq \boldsymbol{T}/\ell\boldsymbol{T}$ and, since $\boldsymbol{T}/\ell\boldsymbol{T}$ is finite, $\exists k$ such that $\overline{\mathcal{M}}^k = 0$ in $\boldsymbol{T}/\ell\boldsymbol{T}$, so $\mathcal{M}^k \subseteq \ell\boldsymbol{T}$.

We therefore have $\boldsymbol{T} \xrightarrow{\sim} \lim_{\leftarrow_i} \boldsymbol{T}/\mathcal{M}^i$, which allows applications of Hensel's lemma [1] in $\boldsymbol{T}$. We shall write tr and det for the trace and the determinant of ρ. Because ℓ is odd, the identity

$$2 \cdot \det(g) = \mathrm{tr}(g)^2 - \mathrm{tr}(g^2)$$

shows that the values of det are contained in $\boldsymbol{T}$.

3. – Eisenstein ideal.

We shall define the Eisenstein ideal I of $\boldsymbol{T}$.

Since α e β are characters, they factor through the abelianization G^{ab} of G, and by the global class field theory $G^{ab} \cong \boldsymbol{Z}_\ell^\times \times \boldsymbol{Z}_{p_1}^\times \times \cdots \times \boldsymbol{Z}_{p_n}^\times$. So we can write

$$\alpha, \beta : \boldsymbol{Z}_\ell^\times \times \boldsymbol{Z}_{p_1}^\times \times \cdots \times \boldsymbol{Z}_{p_n}^\times \to k^\times.$$

Let g_0 be an element of G such that its restriction to $\boldsymbol{Z}_\ell^\times$ is a topological generator of $\boldsymbol{Z}_\ell^\times$. We can write $\alpha = \alpha_\ell \alpha_{p_1} \cdots \alpha_{p_n}$ and $\beta = \beta_\ell \beta_{p_1} \cdots \beta_{p_n}$ where

$$\alpha_\ell, \beta_\ell : \boldsymbol{Z}_\ell^\times \to k^\times$$

$$\alpha_{p_i}, \beta_{p_i} : \boldsymbol{Z}_{p_i}^\times \to k^\times \quad \text{for} \quad \text{all} \quad i = 1, ..., n.$$

Because $\alpha(g_0) \neq \beta(g_0)$, the quadratic polynomial

$$X^2 - \mathrm{tr}(g_0)X + \det(g_0)$$

has distinct roots modulo $\mathcal{M}$. By Hensel's lemma, it splits over $\boldsymbol{T}$. Let r, s be its roots, ordered so that we have

$$r \equiv \alpha(g_0) \bmod \mathcal{M}$$

$$s \equiv \beta(g_0) \bmod \mathcal{M}.$$

We want to lift α and β to two $\boldsymbol{T}^\times$-valued characters, such that at g_0 they assume the values r, s respectively. We will suppose $p_i \not\equiv 1 \bmod \ell$ for $i = 1, ..., n$.

LEMMA 3.1. – *There exist unique characters $\varphi_\ell, \psi_\ell : \boldsymbol{Z}_\ell^\times \to \boldsymbol{T}^\times$ satisfying*

$$\varphi_\ell(g_0) = r, \quad \psi_\ell(g_0) = s.$$

The product of these characters is $\det|_{\boldsymbol{Z}_\ell^\times}$.

PROOF. – Any character $\theta : \boldsymbol{Z}_\ell^\times \to \boldsymbol{T}^\times$ is determined by its value on the generator g_0 of $\boldsymbol{Z}_\ell^\times$. We have an exact sequence

$$1 \to 1 + \mathcal{M} \to \boldsymbol{T}^\times \to k^\times \to 1$$

which splits, because $1 + \mathcal{M}$ is a pro-ℓ-group and $|k^\times|$ is prime to ℓ. Therefore we can write $\boldsymbol{T}^\times = k^\times \times (1 + \mathcal{M})$.

Since $1 + \mathcal{M}$ is a pro-ℓ group, for each t in $1 + \mathcal{M}$ there is a homomorphism $\boldsymbol{Z}_\ell \to 1 + \mathcal{M}$ sending g_0 in t. We define $\varphi'_\ell : \boldsymbol{Z}_\ell^\times \to 1 + \mathcal{M}$ as the homomorphism such that $\varphi'_\ell(g_0)$ is the image of r in $1 + \mathcal{M}$ and we put $\varphi_\ell = \alpha \cdot \varphi'_\ell$. ■

For $i = 1, ..., n$ let $\varphi_{p_i} : \boldsymbol{Z}_{p_i}^\times \to \boldsymbol{T}^\times$ the Teichmüller lift of α_{p_i} and $\psi_{p_i} : \boldsymbol{Z}_{p_i}^\times \to \boldsymbol{T}^\times$ the Teichmüller lift of β_{p_i}. We now let

$$\varphi = \varphi_\ell \cdot \varphi_{p_1} \cdots \varphi_{p_n} : \boldsymbol{Z}_\ell^\times \times \boldsymbol{Z}_{p_1}^\times \times \cdots \times \boldsymbol{Z}_{p_n}^\times \to \boldsymbol{T}^\times$$

$$\psi = \psi_\ell \cdot \psi_{p_1} \cdots \psi_{p_n} : \boldsymbol{Z}_\ell^\times \times \boldsymbol{Z}_{p_1}^\times \times \cdots \times \boldsymbol{Z}_{p_n}^\times \to \boldsymbol{T}^\times.$$

So

$$\varphi \equiv \alpha \mod \mathcal{M}$$

and

$$\psi \equiv \beta \mod \mathcal{M}.$$

Because of our assumption $p_i \not\equiv 1 \bmod \ell$, the only lift of a character $\boldsymbol{Z}_{p_i}^\times \to k^\times$ to $\boldsymbol{T}^\times$ is the Teichmüller lift. Therefore the character φ (resp. ψ) is the unique lift of α (resp. β) over $\boldsymbol{T}^\times$ such that $\varphi(g_0) = r$ (resp. $\psi(g_0) = s$). Moreover $\varphi\psi = \det$.

We define $\eta : G \to \boldsymbol{T}$ to be the function $\mathrm{tr} - \varphi - \psi$ and define the Eisenstein ideal I to be the ideal of $\boldsymbol{T}$ generated by all the quantities $\eta(g)$, for $g \in G$. The congruences

$$\mathrm{tr} \equiv \alpha + \beta \equiv \varphi + \psi \mod \mathcal{M}$$

show that I is contained in $\mathcal{M}$. It is easily seen that the ideal I is intrinsic, although the characters φ and ψ depend on g_0. More precisely, we have the following result:

PROPOSITION 3.1. – *Let γ and δ be characters $G \to \boldsymbol{T}^\times$, and let J be an ideal of $\boldsymbol{T}$. Suppose that we have the congruence*

$$\mathrm{tr} \equiv \gamma + \delta \mod J.$$

Then $I \subseteq J$. Moreover, after permuting γ and δ if necessary, we have $\gamma \equiv \varphi \mod J$ and $\delta \equiv \psi \mod J$.

PROOF. – We may assume that J is a proper ideal of $\boldsymbol{T}$, so that J is contained in $\mathcal{M}$. Since $\mathrm{tr} \equiv \gamma + \delta \mod J$ and $2 \cdot \det(g) = \mathrm{tr}(g)^2 - \mathrm{tr}(g^2)$ for all $g \in G$, we have the congruence:

$$\gamma\delta \equiv \det \mod J.$$

Since γ and δ are characters, they factor through G^{ab}. We put, for $i = 1, ..., n$

$$\gamma_{p_i} = \gamma\mid_{\boldsymbol{Z}_{p_i}^\times}, \quad \gamma_\ell = \gamma\mid_{\boldsymbol{Z}_\ell^\times}, \quad \delta_{p_i} = \delta\mid_{\boldsymbol{Z}_{p_i}^\times}, \quad \delta_\ell = \delta\mid_{\boldsymbol{Z}_\ell^\times}.$$

We observe that:

$$\gamma(g_0)\delta(g_0) \equiv \det(g_0) \equiv rs \mod J$$

$$\gamma(g_0) + \delta(g_0) \equiv r + s \mod J.$$

So, after permuting γ and δ if necessary, we have, by Hensel's lemma:

$$\gamma(g_o) \equiv r \mod J, \qquad \delta(g_0) \equiv s \mod J$$

and we obtain

$$\gamma_\ell \equiv \varphi\mid_{\boldsymbol{Z}_\ell^\times} \mod J, \qquad \delta_\ell \equiv \psi\mid_{\boldsymbol{Z}_\ell^\times} \mod J.$$

For $i = 1, ..., n$ let g_i be an element of G such that its restriction to $\boldsymbol{Z}_{p_i}^{\times}$ is a topological generator of $\boldsymbol{Z}_{p_i}^{\times}$. We have that:

$$\mathrm{tr}(g_i) \equiv \gamma(g_i) + \delta(g_i) \mod J$$

$$\det(g_i) \equiv \gamma(g_i)\delta(g_i) \mod J$$

but

$$\mathrm{tr}(g_i) \equiv \varphi(g_i) + \psi(g_i) \mod \mathcal{M}$$

$$\det(g_i) \equiv \varphi(g_i)\psi(g_i) \mod \mathcal{M}.$$

So

$$\gamma_{p_i} + \delta_{p_i} \equiv \varphi_{p_i} + \psi_{p_i} \mod \mathcal{M}$$

$$\gamma_{p_i}\delta_{p_i} \equiv \varphi_{p_i}\psi_{p_i} \mod \mathcal{M}.$$

Then, after permuting γ_{p_i} and δ_{p_i} if necessary, we have:

$$\gamma_{p_i} \equiv \varphi_{p_i} \mod \mathcal{M}$$

$$\delta_{p_i} \equiv \psi_{p_i} \mod \mathcal{M}.$$

Then γ_{p_i} (resp. δ_{p_i}) is a lift of α_{p_i} (res. β_{p_i}) to $\boldsymbol{T}^{\times}$. Since $p_i \not\equiv 1 \mathrm{mod}\ \ell$, γ_{p_i} (resp. δ_{p_i}) is the Teichmüller lift of α_{p_i} (res. β_{p_i}), so $\gamma_{p_i} = \varphi_{p_i}$ (resp. $\delta_{p_i} = \psi_{p_i}$), in particular:

$$\gamma\ |_{\boldsymbol{Z}_{p_i}^{\times}} = \gamma_{p_i} \equiv \varphi_{p_i} \mod J$$

$$\delta\ |_{\boldsymbol{Z}_{p_i}^{\times}} = \delta_{p_i} \equiv \psi_{p_i} \mod J,$$

from which we obtein the congruences:

$$\gamma \equiv \varphi \mod J$$

$$\delta \equiv \psi \mod J.$$

Now:

$$\eta(g) = \mathrm{tr}(g) - \varphi(g) - \psi(g) \equiv \mathrm{tr}(g) - \gamma(g) - \delta(g) \equiv 0 \mod J$$

for all $g \in G$, so $\eta(g) \in J$ for all $g \in G$ and this implies that $I \subseteq J$. ∎

4. – Some consequences for $\overline{\rho}$.

Now we study the representation $\rho : G \to GL_2(A)$. The residual representation of ρ is given by the matrix:

$$\overline{\rho} = \begin{pmatrix} \alpha & * \\ 0 & \beta \end{pmatrix}$$

in others words, if $a, b, c, d : G \to A$ denote the matrix coefficients of ρ (so that $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$), we have

$$a \equiv \alpha, \quad d \equiv \beta, \quad c \equiv 0 \mod (\lambda).$$

Recall that r, s are the eigenvalues of $\rho(g_0)$. Since r, s are distinct, $\rho(g_0)$ is similar to a diagonal matrix, so it is possible to find a conjugate of ρ over $GL_2(A)$ such that:

$$\overline{\rho} = \begin{pmatrix} \alpha & * \\ 0 & \beta \end{pmatrix}$$

and

$$\rho(g_0) = \begin{pmatrix} r & 0 \\ 0 & s \end{pmatrix}.$$

Now, for $i = 1, ..., n$ let g_i an element of G such that its restriction to $\boldsymbol{Z}_{p_i}^{\times}$ is a topological generator and that $\rho(g_i)$ commutes whit $\rho(g_0)$, then $\rho(g_i)$ is diagonal.

PROPOSITION 4.1. – *For all $g \in G$, we have $a(g), d(g) \in \boldsymbol{T}$. For all pairs $g, g' \in G$, we have $b(g)c(g') \in \boldsymbol{T}$.*

PROOF. – The first assertion follows from the fact that $\mathrm{tr}(g)$ and $\mathrm{tr}(gg_0)$ belong to $\boldsymbol{T}$ and that $r - s$ is an unit of $\boldsymbol{T}$.

The second one is a consequence of the equation

$$b(g)c(g') = a(gg') - a(g)a(g'). \tag{1}$$

■

We now let $H = \mathrm{Gal}(K/\boldsymbol{Q}(\mu_{\ell^\infty}\mu_{p_1^\infty} \cdots \mu_{p_n^\infty})) = \mathrm{Gal}(K/(\boldsymbol{Q}^{ab} \cap K))$. Let B be the $\boldsymbol{T}$-submodule of A generated by all $b(g)$ with $g \in G$. Since the function b vanishes on the closure of the subgroup of G generated by $g_0, g_1, ..., g_n$, we have that B is already generated by the $b(h)$'s with $h \in H$. Similarly, we define C using the $c(g)$'s. We denote by BC the $\boldsymbol{T}$-submodule of A generated by all products $\beta \cdot \gamma$ with $\beta \in B$ and $\gamma \in C$. Then BC is generated by all products $b(g)c(g')$, so that, by (1), it is in fact an ideal of $\boldsymbol{T}$.

PROPOSITION 4.2. – *We have $I = BC$. Moreover, I is the ideal of $\boldsymbol{T}$ generated by the quantities $a(h) - 1$ for $h \in H$, or alternatively the ideal of $\boldsymbol{T}$ generated by the $d(h) - 1$ for $h \in H$.*

PROOF. – Because of the symmetry between a and d, we prove only the first assertion. Let us temporarily denote by J the ideal of $\boldsymbol{T}$ generated by the $a(h) - 1$. We will prove that

$$BC \subseteq J \subseteq I \subseteq BC.$$

1. We prove that $I \subseteq BC$.

We introduce the function "$a \mod BC$" obtained by composing the coefficient function a with the canonical map $\boldsymbol{T} \to \boldsymbol{T}/BC$. Call this function $\overline{a}$. Using (1), we see that $\overline{a}$ is a character $G \to (\boldsymbol{T}/BC)^{\times}$ and so it factors through G^{ab}. Since

$$a(g_0) = \varphi(g_0),$$

we have that

$$\overline{a} \,|_{\boldsymbol{Z}_\ell^\times} \equiv \varphi \,|_{\boldsymbol{Z}_\ell^\times} \mod BC.$$

Because $a \in \boldsymbol{T}$, we have that $a \equiv \varphi \mod \mathcal{M}$ and since for $i = 1, ..., n$ $\varphi \,|_{\boldsymbol{Z}_{p_i}^\times}$ is the Teichmüller lift of a, we have

$$a \,|_{\boldsymbol{Z}_{p_i}^\times} \equiv \varphi \,|_{\boldsymbol{Z}_{p_i}^\times} \mod BC.$$

Then also

$$\overline{a} \,|_{\boldsymbol{Z}_{p_i}^\times} \equiv \varphi \,|_{\boldsymbol{Z}_{p_i}^\times} \mod BC$$

so

$$\overline{a} \equiv \varphi \mod BC$$

and then

$$a \equiv \varphi \mod BC.$$

Similarly we get

$$d \equiv \psi \mod BC.$$

Adding these congruences, we find that

$$\eta(g) = a(g) + d(g) - \varphi(g) - \psi(g) \equiv 0 \mod BC$$

so $\eta(g) \in BC$ for all $g \in G$ and so $I \subseteq BC$.

2. Now we prove that $J \subseteq I$.

For all $h \in H$ we have that $\varphi(h) = \psi(h) = 1$; therefore

$$[a(h) - 1] + [d(h) - 1] = \eta(h) \in I.$$

Similarly

$$r(a(h) - 1) + s(d(h) - 1) = \eta(hg_0) \in I.$$

Because $r - s$ is an unit of $\boldsymbol{T}$, we get

$$a(h) - 1, d(h) - 1 \in I;$$

therefore $J \subseteq I$.

3. Now we prove that $BC \subseteq J$.

For all $h, h' \in H$ we have

$$b(h)c(h') = a(hh') - a(h)a(h') \equiv 0 \mod J.$$

This gives the inclusion $BC \subseteq J$. ■

Let L_α, L_β be finite extensions of $\boldsymbol{Q}$ such that $\ker(\alpha) = \mathrm{Gal}(K/L_\alpha)$ and $\ker(\beta) = \mathrm{Gal}(K/L_\beta)$. Let L be the compositum field of L_α, L_β.

PROPOSITION 4.3. – *Let $g \in \mathrm{Gal}(K/L)$. We have that $\varphi(g), \psi(g) \equiv 1 \mod \mathcal{M}$. Further, we have*

$$\eta(g) \equiv b(g)c(g) \mod (I\mathcal{M}).$$

PROOF. – Since $\varphi \equiv \alpha \mod \mathcal{M}$ and $\psi \equiv \beta \mod \mathcal{M}$, the first assertion is clear.
Now $\varphi\psi = ad - bc$, so

$$b(g)c(g) - \eta(g) = (d(g) - \psi(g))(\varphi(g) - 1) + (a(g) - \varphi(g))(\psi(g) - 1) + (a(g) - \varphi(g))(d(g) - \psi(g)) \equiv 0 \mod (I\mathcal{M}).$$

■

Let $\overline{\rho} = \begin{pmatrix} \alpha & \overline{b} \\ 0 & \beta \end{pmatrix}$ where $\alpha, \beta, \overline{b} : \mathrm{Gal}(K/\boldsymbol{Q}) \to k^\times$.

Since $K_{p_1} \cap \ldots \cap K_{p_n} \cap K_\ell = \boldsymbol{Q}$, we have that $\mathrm{Gal}(K/\boldsymbol{Q}) = \mathrm{Gal}(K_{p_1}/\boldsymbol{Q}) \times \ldots \times \mathrm{Gal}(K_{p_n}/\boldsymbol{Q}) \times \mathrm{Gal}(K_\ell/\boldsymbol{Q})$. We call $\mathrm{Gal}(K_{p_1}/\boldsymbol{Q}) \times \ldots \times \mathrm{Gal}(K_{p_n}/\boldsymbol{Q}) = G_p$ and $\mathrm{Gal}(K_\ell/\boldsymbol{Q}) = G_\ell$.

Let M be the union of all finite abelian extensions of $\boldsymbol{Q}(\mu_\ell)$ in K_ℓ which have ℓ-power degree. The Galois group $X = \mathrm{Gal}(M/\boldsymbol{Q}(\mu_\ell))$ is a $\boldsymbol{Z}_\ell$-module on which $\Delta = \mathrm{Gal}(\boldsymbol{Q}(\mu_\ell)/\boldsymbol{Q})$ acts by conjugation. In other words, X is a module over the group ring $\boldsymbol{Z}_\ell[\Delta]$. The $\boldsymbol{Z}_\ell$-module X is the direct sum of the eigenspaces

$$X(\varepsilon) = \{x \in X \mid \delta \cdot x = \varepsilon(\delta) \cdot x \ \{\text{for all } \delta \in \Delta\}$$

ε running over the group of $\boldsymbol{Z}_\ell^\times$-valued characters of Δ.

Let $\chi : G_\ell \to \boldsymbol{Z}_\ell^\times$ be the ℓ-adic cyclotomic character, and let $\omega : G_\ell \to \mathbf{F}_\ell^\times$ be the reduction of χ modulo ℓ. Then $\alpha\,|_{G_\ell} = \omega^t$ and $\beta\,|_{G_\ell} = \omega^q$ for $t, q \in \boldsymbol{Z}/(\ell-1)\boldsymbol{Z}$.

THEOREM 4.1. – *Suppose that each of the two eigenspaces $X(\omega^{t-q})$ and $X(\omega^{q-t})$ is cyclic. Then there exist a $g \in \mathrm{Gal}(K_\ell/\boldsymbol{Q}(\mu_\ell))$ for which*

$$B = \boldsymbol{T} \cdot b(g), \quad C = \boldsymbol{T} \cdot c(g), \quad I = \boldsymbol{T} \cdot \eta(g).$$

PROOF. – Let we define the function $\overline{b}$: we compose the function $b : G_\ell \to B$ with the projection $B \to B/\mathcal{M}B$ and we restrict it to the subgroup $\mathrm{Gal}(K_\ell/\boldsymbol{Q}(\mu_\ell))$ of G_ℓ. By the Proposition 4.3 we have that for all $g \in \mathrm{Gal}(K/L)$

$$a(g) \equiv 1 \mod \mathcal{M}$$
$$d(g) \equiv 1 \mod \mathcal{M}$$

then

$$a(g), d(g) \equiv 1 \bmod \mathcal{M} \quad \text{for all } g \in \mathrm{Gal}(K_\ell/L \cap K_\ell).$$

Because $L \cap K_\ell \subseteq \boldsymbol{Q}(\mu_\ell)$, we have that $\mathrm{Gal}(K_\ell/\boldsymbol{Q}(\mu_\ell)) \subseteq \mathrm{Gal}(K_\ell/L \cap K_\ell)$ and so $\overline{b}$ is a homomorphism.

Now $B/\mathcal{M}B$ is an abelian ℓ-group, so $\overline{b}$ must factor through X. A matrix calculation shows that

$$\overline{b}(\sigma\tau\sigma^{-1}) = \omega^{t-q}(\sigma) \cdot \overline{b}(\tau)$$

for $\sigma \in G_\ell$, $\tau \in \mathrm{Gal}(K_\ell/\boldsymbol{Q}(\mu_\ell))$; thus $\overline{b}$ factors through the cyclic quotient $X(\omega^{t-q})$ of X.

Therefore, if g is any element of $\mathrm{Gal}(K_\ell/\boldsymbol{Q}(\mu_\ell))$ whose image in $X(\omega^{t-q})$ generates $X(\omega^{t-q})$, then the image of $\overline{b}$ is the cyclic group generated by $\overline{b}(g)$. Thus $B/\mathcal{M}B$ is generated as a $\boldsymbol{T}$-module by $\overline{b}(g)$. By Nakayama's lemma, B is generated as a $\boldsymbol{T}$-module by $b(g)$.

Analogously, if g maps to a generator of $X(\omega^{q-t})$, then $C = \boldsymbol{T} \cdot c(g)$. Taking a g which maps to generators of both $X(\omega^{t-q})$ and $X(\omega^{q-t})$, we find that B is generated by $b(g)$ and C by $c(g)$. Hence $I = BC$ is generated by $b(g)c(g)$; by Nakayama's lemma, together with the Proposition 4.3, $I = \boldsymbol{T} \cdot \eta(g)$. ■

We recall the well know Vandiver conjecture for $\boldsymbol{Q}(\mu_\ell)$. It is true (at least) for all $\ell \leq 125.000$ [5], and no counterexample is known.

Vandiver conjecture. The prime number ℓ is prime to the class number of the maximal real subfield of $\boldsymbol{Q}(\mu_\ell)$.

COROLLARY 4.1. – *Suppose that Vandiver's conjecture is true for ℓ and that I is non-zero. Then, after replacement of ρ by a conjugate $N\rho N^{-1}$, (with $N \in GL_2(A)$), the representation ρ takes values in $GL_2(\boldsymbol{T})$ and its matrix coefficients satisfy:*

$$a \equiv \varphi, \quad d \equiv \psi, \quad c \equiv 0 \pmod{I}.$$

PROOF. – We consider $b(g)$ and $c(g)$ with g as above. Then $b(g) \neq 0$, since $I = (b(g)c(g))$ is non-zero. Taking $N = \begin{pmatrix} b(g)^{-1} & 0 \\ 0 & 1 \end{pmatrix}$, we obtain a conjugate of ρ with the required properties. ■

Let $\overline{V}$ be the finite-dimensional k-representation space of $\overline{\rho}$. Since it's always possible to find an integer model for ρ such that $\overline{\rho}$ is reducible but not semisimple, the natural mapping

$$k \to End_{k[G]}(\overline{V})$$

is an isomorphism. For the deformation theory of Galois representations [4],there exist an universal coefficient-ring $\mathcal{R}(\overline{\rho}) = \mathcal{R}$ with residue field k and an universal deformation

$$\rho^{univ} : G \to GL_2(\mathcal{R})$$

of $\overline{\rho}$ to $\mathcal{R}$. In particular, this means that there is one and only one homomorphism

$$\pi : \mathcal{R} \to \boldsymbol{T}$$

inducing the identity isomorphism on residue fields.

PROPOSITION 4.4. – *The homomorphism π is surjective.*

PROOF. – We observe that since $\boldsymbol{T}$ is generated by the traces of ρ, π if $x \in \boldsymbol{T}$ then $x = \mathrm{tr}(\rho(g))$ for some $g \in G$. So, since $\rho(g) = \pi(\rho^{univ}(g))$, we have $x = \mathrm{tr}(\rho(g)) = \mathrm{tr}(\pi(\rho^{univ}(g))) = \pi(\mathrm{tr}(\rho^{univ}(g)))$. ■

REFERENCES

[1] M. F. ATIYAH - I. G. MACDONALD, *Introduction to Commutative Algebra*, University of Oxford, Addison-Wesley Publishing Company, 1969.

[2] H. CARAYOL, *Formes modulaires et representations galoisiennes valeurs dans un anneau local complet, Contemporary Mathematics*, Volume 165, Amer. Math. Soc., Providence, RI, 1994, 213-237.

[3] A. RIBET KENNETH - E. PAPIER, *Eisenstein ideals and λ-adic representations*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **28** 1981, no. 3 (1982), 651-665.

[4] B. MAZUR, *An introduction to the deformation theory of Galois representation.* In Modular Forms and Fermat's Last Theorem, G. Cornell, J. H. Silverman, G. Stevens, Eds. Springer, 43-311.

[5] S. WAGSTAFF, *The irregular prime to 125.000*, Math. Comp., **32** (1978), 583-591.

[6] A. WILES, *Modular elliptic curves and Fermat last Theorem*, Ann. of Math., **141** (1995), 443-551.

Dipartimento di Matematica, Università di Torino,
Via Carlo Alberto 10, 10123 Torino
e-mail: ciavarella@dm.unito.it

Pervenuta in Redazione
il 20 gennaio 2005