ANNALES

DE

L'INSTITUT FOURIER

Adriaan HERREMANS

A combinatorial interpretation of Serre's conjecture on modular Galois representations

Tome 53, nº 5 (2003), p. 1287-1321.

<http://aif.cedram.org/item?id=AIF_2003__53_5_1287_0>

Ann. Inst. Fourier, Grenoble
53, 5 (2003), 1287–1321

A COMBINATORIAL INTERPRETATION OF SERRE'S CONJECTURE ON MODULAR GALOIS REPRESENTATIONS

by Adriaan HERREMANS*

Introduction.

In 1987, Jean-Pierre Serre stated a conjecture on modular representations of degree 2 of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. He considers a continuous representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$, where V is a 2-dimensional vector space over a finite field F of characteristic p. This representation is assumed to be absolutely irreducible and odd (i.e., $\det\rho(c) = -1$ if c denotes the complex conjugation). Serre then conjectures that there exists an integer $N \geqslant 1$ prime to p, an integer $k \geqslant 2$, a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times$ and a cuspform $f = \sum_{n=1}^{\infty} a_n q^n$ of level N, weight k and character ε with coefficients in F, which is an eigenvector of all Hecke operators T_l for all primes $l \not| pN$, such that ρ is unramified outside pN and

$$(1) \qquad \begin{cases} \mathrm{Tr}\ \rho(\mathrm{Frob}_l) = a_l \\ \det\ \rho(\mathrm{Frob}_l) = \varepsilon(l) l^{k-1} \end{cases} \text{for all prime numbers } l \not| pN$$

where Frob_l is an arithmetic Frobenius element at l. Furthermore, Serre defines for the representation ρ a conductor N, a weight k and a character

* The author is a postdoc researcher of the Research Fund of Flanders – Belgium (F.W.O. Vlaanderen), visiting the university of Orsay in the European program "Improving Human Potential and the Socio-Economical Knowledge Base".
Keywords: Modular forms – Modular symbols – 2-dim. irreducible Galois representations – Shimura cohomology.
Math. classification: 11F11 – 11F30 – 11F67 – 11F80.

ε, and in a strong form of his conjecture, requires that f as above should exist of type (N, k, ε). All details can be found in [14].

Our goal in this paper is to present a combinatorial conjecture equivalent to Serre's conjecture in his strong modified form (see §4.2). The idea is to replace modular forms by their counterparts in the theory of modular symbols. In order to state this new conjecture, we look at the free $\mathbb{Z}$-module of finite rank

$$\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$$

for $N \geqslant 1$ and $k \geqslant 2$, where C_N is the set of pairs (u, v) of elements in $\mathbb{Z}/N\mathbb{Z}$ such that $\mathbb{Z}u + \mathbb{Z}v = \mathbb{Z}/N\mathbb{Z}$, and $\mathbb{Z}[X,Y]_{k-2}$ is the group of homogeneous polynomials in two variables X and Y of degree $k-2$ with coefficients in $\mathbb{Z}$. We describe a right action of matrices in $SL_2(\mathbb{Z})$ on this module (see §5.1) and define $L_k(N)$ to be the quotient of $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ by the subgroup generated by the elements $x + x\|[\sigma]$ and $x + x\|[\tau] + x\|[\tau^2]$ for $x \in \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$, where $\sigma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$. On this space we define explicit Hecke operators T_l and diamond operators R_d (see §5.2).

Our conjecture can be stated as follows:

MAIN CONJECTURE 1. — *Let $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$ be a continuous absolutely irreducible odd representation in a 2-dimensional vector space V over a finite field F of characteristic p. Let N, k, ε be the conductor, the weight and the character attached to ρ by Serre (see [14, §1, §2]). Then there exists a non zero $\mathbb{Z}$-linear map*

$$\mu : L_k(N) \to F$$

satisfying the following conditions:

1. *For each prime l not dividing pN, we have*

$$\mu \circ T_l = a_l \mu \tag{2}$$

   where $a_l = \mathrm{Tr}\ \rho(\mathrm{Frob}_l)$.

2. *For each integer d prime to N, we have*

$$\mu \circ R_d = \varepsilon(d)\mu. \tag{3}$$

The main theorem of this paper is then:

MAIN THEOREM 1. — *The main conjecture (stated as above) is equivalent to the strong conjecture of Serre (in his strong modified form, see §4.2).*

The theorems of this paper were mainly obtained in my Ph.D.thesis, where the main theorem was proved for $k \leqslant p+2$. Most of the ideas took shape throughout discussions with Joseph Oesterlé, to whom I would like to present my deepest gratitude. The existence of this paper owes a lot to him. Furthermore, I would like to thank Jan Denef for his support during the Ph.D.work.

1. Preliminaries.

1.1. Modular forms.

Denote by $\mathcal{H}$ the complex upper half plane. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2^+(\mathbb{R})$ and $z \in \mathcal{H}$, we put $j(\gamma, z) := cz + d$. For a holomorphic function f on $\mathcal{H}$, an integer k and $\gamma \in GL_2^+(\mathbb{R})$ we denote

$$f|[\gamma]_k(z) := f(\gamma z) j(\gamma, z)^{-k} \det\gamma^{k-1}.$$

We define

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a, d \equiv 1 \bmod N,\ c \equiv 0 \bmod N \right\}$$

and denote $\mathcal{F}_k(\Gamma_1(N))$ (resp. $\mathcal{M}_k(\Gamma_1(N))$, $\mathcal{S}_k(\Gamma_1(N))$) the space of modular functions (resp. modular forms, modular cuspforms) over $\mathbb{C}$ of weight k with respect to $\Gamma_1(N)$. The integer N is called the level of the modular function.

Let Δ_n (resp. Δ'_n) be the subset of $M_2(\mathbb{Z})$ consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc = n$, $a - 1 \equiv c \equiv 0 \bmod N$ (resp. $ad - bc = n$, $d - 1 \equiv c \equiv 0 \bmod N$). For every $n \geqslant 1$ we define Hecke operators T_n and T'_n on modular functions by the formulas:

$$\begin{array}{rccc} T_n: & \mathcal{F}_k(\Gamma_1(N)) & \rightarrow & \mathcal{F}_k(\Gamma_1(N)) \\ & f & \mapsto & \sum\limits_{\alpha \in \Gamma_1(N) \backslash \Delta_n} f|[\alpha]_k \end{array}$$

and similar for T'_n where we replace Δ_n by Δ'_n. If a modular form $f = \sum a_n q^n$ is an eigenvector of the Hecke operators T_n, we have that $T_n f = a_n f$. It it known that $W_N \circ T_n = T'_n \circ W_N$ (see e.g. [4, §4] or [16, p. 86-87]) where W_N is the Atkin-Lehner involution and that both T_n and T'_n stabilize the space of modular forms and modular cuspforms.

For d prime to N, we define a diamond operator R_d by

$$\begin{array}{cccc} R_d: & \mathcal{F}_k(\Gamma_1(N)) & \rightarrow & \mathcal{F}_k(\Gamma_1(N)) \\ & f & \mapsto & f|[\sigma_d]_k \end{array}$$

where $\sigma_d \in SL_2(\mathbb{Z})$ is a matrix congruent to $\left(\begin{smallmatrix} \bar{d}^{-1} & * \\ 0 & \bar{d} \end{smallmatrix}\right) \bmod N$ with $\bar{d} \in (\mathbb{Z}/N\mathbb{Z})^\times$ the class of d. Let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ be a Dirichlet character. We say that $f \in \mathcal{F}_k(\Gamma_1(N))$ belongs to $\mathcal{F}_k(N, \varepsilon)$ if $R_d f = \varepsilon(d) f$ for every d prime to N (analogous we define $\mathcal{M}_k(N, \varepsilon)$ and $\mathcal{S}_k(N, \varepsilon)$). We define $R'_d = R_{\bar{d}^{-1}}$ and we have that $W_N \circ R_d = R'_d \circ W_N$ (see e.g. [4, §4]).

1.2. The Shimura isomorphism.

The standard representation of $GL_2(\mathbb{C})$ on $\mathbb{C}^2$ is the representation given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} au + bv \\ cu + dv \end{pmatrix}.$$

We deduce from this representation, for each $k \geqslant 0$, a representation of $GL_2(\mathbb{C})$ on the k^{th} tensor power $\mathrm{T}^k_{\mathbb{C}}(\mathbb{C}^2)$ of $\mathbb{C}^2$. We shall denote by V_k the subspace $\mathrm{TS}^k_{\mathbb{C}}(\mathbb{C}^2)$ of $\mathrm{T}^k_{\mathbb{C}}(\mathbb{C}^2)$ consisting of the symmetric tensors. It is stable under $GL_2(\mathbb{C})$. The representation of $GL_2(\mathbb{C})$ on V_k is characterized by the relation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}^{\otimes k} = \begin{pmatrix} au + bv \\ cu + dv \end{pmatrix}^{\otimes k}. \tag{4}$$

From the natural non degenerated pairing on $\mathbb{C}^2$

$$< \begin{pmatrix} u \\ v \end{pmatrix}, \begin{pmatrix} u' \\ v' \end{pmatrix} >= \det \begin{pmatrix} u & u' \\ v & v' \end{pmatrix}$$

we deduce a non degenerated pairing on V_k characterised by

$$< \begin{pmatrix} u \\ v \end{pmatrix}^{\otimes k}, \begin{pmatrix} u' \\ v' \end{pmatrix}^{\otimes k} >= (uv' - vu')^k.$$

Remark that we have $<\gamma x, y> = < x, \tilde{\gamma} y>$ for $x, y \in V_k$ and $\gamma \in GL_2(\mathbb{C})$, where $\tilde{\gamma} = \gamma^{-1}\det(\gamma)$ (called 'the main involution' by Shimura, see [16, p. 72]).

The *Shimura cohomology group* is now defined, for $k \geqslant 2$, by $\mathcal{H}_k(\Gamma_1(N)) := H^1(\Gamma_1(N), V_{k-2})$.

We shall denote by

$$sh : \mathcal{F}_k(\Gamma_1(N)) \to \mathcal{H}_k(\Gamma_1(N))$$

the $\mathbb{C}$-linear map

$$f \mapsto \text{cohomology class of } \left(\gamma \mapsto \int_{z_0}^{\gamma z_0} f(z) \begin{pmatrix} z \\ 1 \end{pmatrix}^{\otimes k-2} dz \right)$$

with $z_0 \in \mathcal{H}$ (see [16, chap. 8]). One can prove that the map is well-defined and that this definition does not depend on the choice of $z_0 \in \mathcal{H}$.

We define a Hecke operator

$$T'_n : \mathcal{H}_k(\Gamma_1(N)) \to \mathcal{H}_k(\Gamma_1(N))$$

in the following way: if u is a 1-cocycle in $Z^1(\Gamma_1(N), V_{k-2})$ we choose a map $u_\Delta : \Delta'_n \to V_{k-2}$ such that

$$u_\Delta(\gamma\alpha) = \gamma u_\Delta(\alpha) + u(\gamma) \tag{5}$$

for $\gamma \in \Gamma_1(N)$ and $\alpha \in \Delta'_n$. Such a map always exists. Let $\gamma' \in \Gamma_1(N)$. By (5), the map $\alpha \mapsto u_\Delta(\alpha\gamma') - u_\Delta(\alpha)$ is $\Gamma_1(N)$-linear on the left, hence $\tilde{\alpha}(u_\Delta(\alpha\gamma') - u_\Delta(\alpha))$ depends only on $\Gamma_1(N)\alpha$, and we define

$$u'(\gamma') = \sum_{\alpha \in \Gamma_1(N)\backslash\Delta'_n} \tilde{\alpha}(u_\Delta(\alpha\gamma') - u_\Delta(\alpha)). \tag{6}$$

One proves that the class of u' only depends on the class of u and is independent of the choice u_Δ. We define therefore T'_n(class of u) = class of u'. We remark that we use the notation T'_n just to draw the attention that this operator is defined with respect to Δ'_n.

Denote by $\overline{\mathcal{S}_k(\Gamma_1(N))}$ the complex vector space of antiholomorphic cuspforms. As an immediate consequence of the Shimura isomorphism we can state

Theorem 2 (Shimura isomorphism).

$$(sh, \overline{sh}) : \mathcal{M}_k(\Gamma_1(N)) \times \overline{\mathcal{S}_k(\Gamma_1(N))} \to \mathcal{H}_k(\Gamma_1(N))$$

is an isomorphism of complex vector spaces, where $\overline{sh}$ *is defined by* $\overline{sh}(\bar{f}) = \overline{sh(f)}$.

In fact Shimura proves in [16, Thm. 8.4] that there exists an isomorphism between modular cuspforms and the cuspidal subgroup of the Shimura cohomology group defined over the real numbers. The theorem stated above follows essentially from extending scalars and the observation that $\mathcal{M}_k(\Gamma_1(N))/\mathcal{S}_k(\Gamma_1(N))$ is isomorphic to the quotient of the Shimura cohomology group by its cuspidal subgroup.

Furthermore, it is known that the Shimura isomorphism is compatible with Hecke and diamond operators (see [16, Thm. 8.5]), i.e.,

Theorem 3. — *For every* $n \geqslant 1$ *and every* $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ *we have that*

$$sh \circ T_n' = T_n' \circ sh, \quad sh \circ R_d' = R_d' \circ sh.$$

2. Combinatorial description of the Shimura cohomology groups.

2.1. Shapiro's Lemma and the cohomology of an $SL_2(\mathbb{Z})$-module.

We first give an explicit formula which describes Shapiro's Lemma:

Lemma 1 (Shapiro's Lemma). — *Let* G *be a group and* H *be a subgroup of finite index. Let* Q *be a left* H*–module. Let* P *be the coinduced module* $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], Q)$. *Then* G *acts on* P *by* $(g'u)(g) = u(gg')$ *and we have*

$$H^1(H, Q) \cong H^1(G, P)$$

canonically.

We first define a map $H^1(G, P) \to H^1(H, Q)$. Let $v : G \to P$ be a 1-cocycle in $Z^1(G, P)$. Define $u(h) := v(h)(e)$ for $h \in H$. It is easy to see that this is a 1-cocycle and that the map is well-defined.

We now define a map $H^1(H,Q) \to H^1(G,P)$. Let $u : H \to Q$ be a 1-cocycle in $Z^1(H,Q)$. Take a map $\underline{u} : G \to Q$ such that

$$\underline{u}(hg) = h\underline{u}(g) + u(h) \quad \text{for } h \in H, g \in G$$

(such a map $\underline{u}$ always exists). We then define $v : G \to P$ by

$$v(g)(g') = \underline{u}(g'g) - \underline{u}(g').$$

One checks that this is a 1-cocycle, that the map is well-defined and that the cohomology class of v is independent of the choice of $\underline{u}$.

Furthermore, it is straightforward that the composition of this two maps gives the identity.

Remark. — If Q is a left G–module, we have that $P \cong \mathbb{Z}[H\backslash G] \otimes_{\mathbb{Z}} Q$, where G acts on $\mathbb{Z}[H\backslash G] \otimes_{\mathbb{Z}} Q$ as $g'(Hg \otimes q) = Hgg'^{-1} \otimes g'q$. The isomorphism works as follows: to an element $u \in P$ we associate $\sum_{g \in H\backslash G} Hg \otimes g^{-1}u(g)$ in $\mathbb{Z}[H\backslash G] \otimes_{\mathbb{Z}} Q$. The inverse isomorphism associates to an element $Hg \otimes q \in \mathbb{Z}[H\backslash G] \otimes_{\mathbb{Z}} Q$, the map $u \in P$ defined by

$$u(g') = \begin{cases} 0, & \text{if } g' \notin Hg \\ g'q, & \text{if } g' \in Hg. \end{cases}$$

These isomorphisms are compatible with the actions of G.

Assume now that M is an $SL_2(\mathbb{Z})$–module where multiplication by 2 and 3 are invertible. Denote M^+ for the submodule of M fixed by $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and M^- the submodule of M on which $-I$ acts as -1. Following ideas in [12, §1.7, Prop. 9], we obtain the following, where σ and τ denote the matrices $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.

PROPOSITION 1. — *Denote $M^{+\sigma}$ for the submodule of elements of M^+ which are invariant under σ, and define in a similar way $M^{+\tau}$, then we have that*

$$H^1(SL_2(\mathbb{Z}), M) \cong M^+/(M^{+\sigma} + M^{+\tau}).$$

Proof. — We first remark that $M = M^+ \oplus M^-$ and $H^1(SL_2(\mathbb{Z}), M^-) = 0$. Indeed, if $u \in Z^1(SL_2(\mathbb{Z}), M^-)$ is a 1-cocycle, we have $u(-I.g) = (-I).u(g) + u(-I) = g.u(-I) + u(g)$ and therefore $2u(g) = -(g-1)u(-I)$. Because multiplication by 2 is invertible in M^-, u is a coboundary. Since

$H^1(SL_2(\mathbb{Z}),M) = H^1(SL_2(\mathbb{Z}),M^+) \oplus H^1(SL_2(\mathbb{Z}),M^-)$, it suffices to describe $H^1(SL_2(\mathbb{Z}),M^+)$.

If $\phi \in Z^1(SL_2(\mathbb{Z}),M^+)$ is a 1-cocycle, we have $\phi(-g) = (-I).\phi(g) + \phi(-I)$, hence $\phi(-I) = 0$ (by taking $g = -I$) and $\phi(-g) = \phi(g)$. In other words, ϕ defines by passing to the quotient, a 1-cocycle in $Z^1(PSL_2(\mathbb{Z}),M^+)$.

Since $PSL_2(\mathbb{Z})$ is the free product of the groups of order 2 and 3 generated by the images of σ and τ respectively, we have an isomorphism

$$\begin{array}{ccc} Z^1(SL_2(\mathbb{Z}),M^+) & \longrightarrow & \ker(1+\sigma) \times \ker(1+\tau+\tau^2) \\ \phi & \longmapsto & (\phi(\sigma),\phi(\tau)) \end{array}$$

where $\ker(1+\sigma)$ denotes the kernel of multiplication by $(1+\sigma)$ in M^+. Furthermore we have $\ker(1+\sigma) = (\sigma-1)M^+$ and $\ker(1+\tau+\tau^2) = (\tau-1)M^+$ since multiplication by 2 and 3 are invertible, and we remark that $(\sigma-1)M^+ \cong M^+/M^{+\sigma}$ and $(\tau-1)M^+ \cong M^+/M^{+\tau}$ (by $(\sigma-1)m_1 \mapsto m_1 + M^{+\sigma}$ and $(\tau-1)m_2 \mapsto m_2 + M^{+\tau}$). So we get an isomorphism of groups $\Lambda : Z^1(SL_2(\mathbb{Z}),M) \to M^+/M^{+\sigma} \times M^+/M^{+\tau}$.

The image under Λ of a 1-coboundary $g \mapsto gm - m$ is the image of m by the diagonal map $M^+ \to M^+/M^{+\sigma} \times M^+/M^{+\tau}$. We end the proof by the fact that

$$\begin{array}{ccc} M^+/M^{+\sigma} \times M^+/M^{+\tau} & \longrightarrow & M^+/(M^{+\sigma} + M^{+\tau}) \\ (m_1 + M^{+\sigma}, m_2 + M^{+\tau}) & \longmapsto & m_2 - m_1 + M^{+\sigma} + M^{+\tau} \end{array}$$

defines by passing to the quotient an isomorphism $H^1(SL_2(\mathbb{Z}),M) \to M^+/(M^{+\sigma} + M^{+\tau})$ (see e.g. [12, §1.7]). □

2.2. Application to the Shimura cohomology.

We can apply the last paragraph to the group $G = SL_2(\mathbb{Z})$, subgroup $H = \Gamma_1(N)$ and the G-module $Q = V_{k-2}$ where k is an integer $\geqslant 2$. Since $\mathcal{H}_k(\Gamma_1(N)) = H^1(\Gamma_1(N), V_{k-2})$ we obtain as a direct consequence of Shapiro's lemma and the remark, canonical isomorphisms

$$\begin{aligned} \mathcal{H}_k(\Gamma_1(N)) &\cong H^1(SL_2(\mathbb{Z}), \mathrm{Hom}_{\mathbb{Z}[\Gamma_1(N)]}(\mathbb{Z}[SL_2(\mathbb{Z})], V_{k-2})), \\ &\cong H^1(SL_2(\mathbb{Z}), \mathbb{Z}[\Gamma_1(N)\backslash SL_2(\mathbb{Z})] \otimes_{\mathbb{Z}} V_{k-2}). \end{aligned}$$

Then we apply Proposition 1 in order to conclude that

$$\mathcal{H}_k(\Gamma_1(N)) \cong M^+/(M^{+\sigma} + M^{+\tau}) \tag{7}$$

where $M = \mathbb{Z}[\Gamma_1(N)\backslash SL_2(\mathbb{Z})] \otimes_{\mathbb{Z}} V_{k-2}$.

Combining all explicit isomorphisms above, we get the following description when $\mathcal{H}_k(\Gamma_1(N))$ is identified with $M^+/(M^{+\sigma} + M^{+\tau})$ by the isomorphism (7): the Shimura map $\mathcal{F}_k(\Gamma_1(N)) \to \mathcal{H}_k(\Gamma_1(N))$ is identified with the map

$$\begin{array}{ccc} \mathcal{F}_k(\Gamma_1(N)) & \to & M^+/(M^{+\sigma} + M^{+\tau}) \\ f & \mapsto & \text{class of } \sum\limits_{g\in\Gamma_1(N)\backslash SL_2(\mathbb{Z})} \Gamma_1(N)g \otimes \int_\rho^i f|[g]_k(z) \begin{pmatrix} z \\ 1 \end{pmatrix}^{\otimes k-2} dz. \end{array}$$

Example. — In order to give the reader a better idea of the role of the modular symbols, we describe shortly the case $k = 2$. In this case, we identify M^+ with $\mathbb{C}[\Gamma_1(N)\backslash PSL_2(\mathbb{Z})]$ in the following way: to an element $\Gamma_1(N)(\pm g)$ of $\Gamma_1(N)\backslash PSL_2(\mathbb{Z})$, we associate the single element $\Gamma_1(N)g = \Gamma_1(N)(-g)$ of $\Gamma_1(N)\backslash SL_2(\mathbb{Z})$ if $N \leqslant 2$ $(-I \in \Gamma_1(N))$, the sum of the two elements $\Gamma_1(N)g$ and $\Gamma_1(N)(-g)$ if $N > 2$ $(-I \notin \Gamma_1(N))$. With this identification we have (see [7, Prop. 6.4.1]):

PROPOSITION 2. — *The composition of the surjection $M^+ \to M^+/(M^{+\sigma} + M^{+\tau})$, of the isomorphism $M^+/(M^{+\sigma} + M^{+\tau}) \to \mathcal{H}_2(\Gamma_1(N))$ (see formula 7) and of the canonical isomorphism $\mathcal{H}_2(\Gamma_1(N)) \to H_1(X_1(N), cusps; \mathbb{C})$ where $X_1(N)$ is the modular curve with regard to $\Gamma_1(N)$ (see e.g. [7, §3.2]) associates to an element $\Gamma_1(N)(\pm g)$ of $\Gamma_1(N)\backslash PSL_2(\mathbb{Z})$ the modular symbol $\{g0, g\infty\}$.*

2.3. Hecke operators.

The linear map $T'_n : \mathcal{H}(\Gamma_1(N)) \to \mathcal{H}_k(\Gamma_1(N))$ gets identified through the isomorphism (7) with a linear map

$$T'_n : M^+/(M^{+\sigma} + M^{+\tau}) \to M^+/(M^{+\sigma} + M^{+\tau})$$

where $M = \mathbb{Z}[\Gamma_1(N)\backslash SL_2(\mathbb{Z})] \otimes_{\mathbb{Z}} V_{k-2}$.

Assume that $\sum n_A A$ is an element of $\mathbb{Z}[GL_2^+(\mathbb{Q})]$ with the following property: for each $\beta \in SL_2(\mathbb{Z})\Delta'_n$, we have

$$\sum_{A\in\beta SL_2(\mathbb{Z})} n_A([A0]-[A\infty]) = [0]-[\infty] \quad \text{in } \mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]. \tag{8}$$

We associate to this element the linear map

$$\begin{array}{rcccl} \phi: & M & \to & M & \\ & \Gamma_1(N)g'\otimes x & \mapsto & \sum\limits_A n_A \sum\limits_{\substack{\Gamma_1(N)g\in\Gamma_1(N)\backslash SL_2(\mathbb{Z})\\ g'A\in\Delta'_n g}} & \Gamma_1(N)g\otimes\tilde{A}x \end{array} \tag{9}$$

where $g' \in SL_2(\mathbb{Z})$, $x \in V_{k-2}$ and $\tilde{A} = \det(A)A^{-1}$. We have clearly $\phi(M^+) \subset M^+$. One can prove the following proposition.

PROPOSITION 3.— *The map $M^+ \to M^+$ induced by ϕ defines, by passing to the quotient, the map $T'_n : M^+/(M^{+\sigma}+M^{+\tau}) \to M^+/(M^{+\sigma}+M^{+\tau})$.*

However, this is not easy and takes several pages of comparing the Hecke operators on the appropriate spaces (in fact we study this operators trough a 'dual' Shimura isomorphism following ideas in [9] and [17]). Note that the action of Hecke operators given on M is of a total different nature than the (usual) action on modular functions and Shimura cohomology groups. All details can be found in [7, chap. 7].

We have a similar description of the diamond operators, which is easier to prove.

PROPOSITION 4.— *The map $M^+ \to M^+$ induced by*

$$\phi : \Gamma_1(N)g\otimes x \mapsto \Gamma_1(N)\sigma_d g\otimes x$$

defines, by passing to the quotient, the map $R'_d : M^+/(M^{+\sigma}+M^{+\tau}) \to M^+/(M^{+\sigma}+M^{+\tau})$.

Remark.— All the results in Sections 1 and 2 can be stated and proved (see [7]) in the more general setting of any subgroup $\Gamma \subset SL_2(\mathbb{Z})$ of finite index (instead of $\Gamma_1(N)$) and the setting of correspondences defined as double cosets (instead of the concrete Hecke or diamond operators).

3. Some algebra.

In this section we state two theorems in abstract algebra, which are used later on in a concrete setting.

THEOREM 4. — *Let K be a field, A be a K–algebra, M and N be two A–modules, of finite dimension over K. Let L be an extension of K. If the $A_{(L)}$-modules $M_{(L)}$ and $N_{(L)}$ are isomorphic, then M and N are isomorphic as A–modules.*

Proof. — See [10, p. 45 and p. 51]. □

THEOREM 5. — *Let R be a Dedekind domain, K be its fraction field, $\mathcal{P}$ be a maximal ideal of R, A be an R-algebra, V be a finite dimensional vector space over K on which A acts R-linearly, M and M' be two R-lattices of V stable under A. Then the $A/\mathcal{P}A$-modules $M/\mathcal{P}M$ and $M'/\mathcal{P}M'$ have isomorphic semi-simplifications.*

Proof. — Let $R_{\mathcal{P}}$ denote the localization of R at $\mathcal{P}$. Then $M_{\mathcal{P}}$ and $M'_{\mathcal{P}}$ are two $R_{\mathcal{P}}$-lattices of V stable under $A_{\mathcal{P}}$ and $A_{\mathcal{P}}/\mathcal{P}A_{\mathcal{P}}$, $M_{\mathcal{P}}/\mathcal{P}M_{\mathcal{P}}$, $M'_{\mathcal{P}}/\mathcal{P}M'_{\mathcal{P}}$ are canonically isomorphic to $A/\mathcal{P}A$, $M/\mathcal{P}M$, $M'/\mathcal{P}M'$. Therefore, by replacing R by $R_{\mathcal{P}}$, we may assume that R is a discrete valuation ring and in particular a principal domain.

We recall that an $A/\mathcal{P}A$-module N of finite dimension over $R/\mathcal{P}R$ has a Jordan–Hölder filtration

$$N = N_0 \supset N_1 \supset \ldots \supset N_n = 0$$

(where N_i/N_{i+1} is a simple $A/\mathcal{P}A$-module for every $0 \leqslant i < n$) and that $\bigoplus_{i=0}^{n-1}(N_i/N_{i+1})$ is called a *semi-simplification* of N.

We separate the proof in different cases.

3.0.1. Case 1: $\mathcal{P}M \subset M' \subset M$.

In this case we have the following two exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & M'/\mathcal{P}M & \to & M/\mathcal{P}M & \to & M/M' & \to & 0 \\ 0 & \to & \mathcal{P}M/\mathcal{P}M' & \to & M'/\mathcal{P}M' & \to & M'/\mathcal{P}M & \to & 0. \end{array}$$

This gives

$$(M/\mathcal{P}M)^{ss} \cong (M'/\mathcal{P}M)^{ss} \oplus (M/M')^{ss} \text{ and}$$

$$(M'/\mathcal{P}M')^{ss} \cong (M'/\mathcal{P}M)^{ss} \oplus (\mathcal{P}M/\mathcal{P}M')^{ss}.$$

Since R is a principal domain, we have obviously $M/M' \cong \mathcal{P}M/\mathcal{P}M'$ and hence the theorem.

3.0.2. Case 2: $M' \subset M$.

Then there exists an $n \in \mathbb{N}$ such that $\mathcal{P}^n M \subset M'$. We have

$$M' \subset M' + \mathcal{P}^{n-1}M \subset M' + \mathcal{P}^{n-2}M \subset \ldots \subset M' + \mathcal{P}M \subset M.$$

Remark that for every $0 \leqslant i \leqslant n-1$, we have

$$\mathcal{P}(M' + \mathcal{P}^i M) \subset M' + \mathcal{P}^{i+1}M \subset M' + \mathcal{P}^i M,$$

and so we can conclude by using n times the arguments of case 1.

3.0.3. Case 3: General case.

Starting with two arbitrary R-lattices, we apply the conclusions of case 2 for $M \cap N \subset M$ and $M \cap N \subset N$. Comparing the two results yields the proof of the theorem. □

Corollary 1 (Using the notation of Theorem 5). — *Assume A to be commutative. Let $\chi : A \to R/\mathcal{P}$ be a homomorphism of R-algebras. If there exists a non zero $x \in M/\mathcal{P}M$ such that $ax = \chi(a)x$ for all $a \in A$, there exists a non zero $y \in M'/\mathcal{P}M'$ such that $ay = \chi(a)y$ for all $a \in A$.*

Proof. — We deduce this lemma from Theorem 5 and the following observation.

Let B be a commutative ring and N be a B-module of finite length. Let $\mathcal{M}$ be a maximal ideal of B. Then the following two statements are equivalent:

1. N contains a submodule isomorphic to $B/\mathcal{M}$.

2. $B/\mathcal{M}$ is isomorphic to some quotient of a Jordan-Hölder filtration of N.

Indeed, $1 \Rightarrow 2$ is obvious. Since N is of finite length, it is a direct sum of submodules, each of which is annihilated by a power of a maximal ideal. Under assumption 2, the summand corresponding to the maximal ideal $\mathcal{M}$ is different from 0, and it obviously contains a submodule isomorphic to $B/\mathcal{M}$.

If we apply this general observation to $B = A$, $\mathcal{M}$ the kernel of χ and N either $M/\mathcal{P}M$ or $M'/\mathcal{P}M'$, we conclude the proof of the corollary by the fact that the semi-simplifications of $M/\mathcal{P}M$ or $M'/\mathcal{P}M'$ are isomorphic. □

4. Serre's conjecture.

4.1. Modular forms with coefficients in F.

Let $N \geqslant 1$ and $k \geqslant 0$ be integers, and $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow F^{\times}$ be a Dirichlet character with values in the finite field F. There are different ways to define the notion of a cuspform of level N, weight k and character ε with *coefficients in F*. We first give the definition used by Serre in [14], under the assumption that $\varepsilon(-1) = (-1)^k$ and that k is even when $p = 2$. (These assumptions are satisfied when N, k, ε are the invariants attached to ρ as in [14, §1, §2]).

Let $\bar{\mathbb{Z}}$ denote the ring of algebraic integers in $\mathbb{C}$. Choose a maximal ideal in $\bar{\mathbb{Z}}$ containing p. Its residue field is an algebraic closure of $\mathbb{F}_p$ that we denote by $\bar{\mathbb{F}}_p$. We denote by $z \mapsto \tilde{z}$ the reduction homomorphism $\bar{\mathbb{Z}} \longrightarrow \bar{\mathbb{F}}_p$ and we choose an embedding $F \longrightarrow \bar{\mathbb{F}}_p$, so that ε can be considered as a character with values in $\bar{\mathbb{F}}_p^{\times}$.

Denote by $\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \bar{\mathbb{Z}}$ the Teichmüller lift of ε, i.e., the unique character which takes values in the roots of unity of order prime to p such that $\tilde{\varepsilon_0} = \varepsilon$. We have that $\varepsilon_0(-1) = (-1)^k$.

Serre defines a modular cuspform with coefficients in F (see [14, §3.1]), of level N, weight k and character ε as a formal power series

$$f = \sum_{n=1}^{\infty} a_n q^n, \quad \text{with } a_n \in F$$

such that there exists an element $f_0 \in \mathcal{S}_k(N, \varepsilon_0)$ of the form

$$f_0 = \sum_{n=1}^{\infty} A_n q^n, \quad \text{with } A_n \in \bar{\mathbb{Z}}$$

with $\tilde{f_0} = f$, i.e. $\tilde{A}_n = a_n$ for all n. Let us denote $\mathcal{S}_k(N, \varepsilon)_F$ for the space of such cuspforms.

We have that $\mathcal{S}_k(N, \varepsilon)_F$ does not depend on the choice of the maximal ideal of $\bar{\mathbb{Z}}$ containing p and of the embedding $F \longrightarrow \bar{\mathbb{F}}_p$: this follows from the fact that $\sigma(f_0) \in \mathcal{S}_k(N, \sigma \circ \varepsilon_0)$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$ (see [3, Prop. 2.7]). The dimension of $\mathcal{S}_k(N,\varepsilon)_F$ over F is equal to the dimension of $\mathcal{S}_k(N,\varepsilon_0)$ over $\mathbb{C}$. We can define on the space $\mathcal{S}_k(N,\varepsilon)_F$ an action of Hecke and diamond operators by $T(f) = \widetilde{Tf_0}$ (here T denotes either T_n or R_d). This definition again is independent of the choice of the maximal ideal in $\bar{\mathbb{Z}}$ and of the embedding $F \to \bar{\mathbb{F}}_p$, since $T(\sigma f) = \sigma(Tf)$ for $\sigma \in \mathrm{Aut}(\mathbb{C})$ for such a correspondence; it is also independent of the choice of the lift f_0. The Hecke and diamond operators commute amongst each other, and we have $R_d f = \varepsilon(d) f$ for d prime to N. We shall say that f is normalized if $a_1 = 1$; if f is normalized and f is an eigenvector of T_n, we have $T_n f = a_n f$.

Another way of defining a modular function with coefficients in F is to use Katz' definition (see e.g. [3, §2]). One can define on the space of Katz modular functions $\mathcal{F}_k(N)_F^{\mathrm{Katz}}$ Hecke operators T_n (for $n \geqslant 1$) and diamond operators R_d (for d prime to N) (see [3]). We will denote $\mathcal{F}_k(N,\varepsilon)_F^{\mathrm{Katz}}$ (resp. $\mathcal{M}_k(N,\varepsilon)_F^{\mathrm{Katz}}$, $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}}$) for the space of Katz modular function (resp. Katz modular forms, Katz modular cuspforms) of level N, weight k, character ε with coefficients in F.

A third way is to define modular cuspforms with coefficients in F, of level N, weight k, as a formal power series

$$f = \sum_{n=1}^{\infty} a_n q^n \text{ with } a_n \in F$$

such that there exists an element $f_0 \in \mathcal{S}_k(\Gamma_1(N))$ of the form

$$f_0 = \sum_{n=1}^{\infty} A_n q^n \text{ with } A_n \in \bar{\mathbb{Z}}$$

with $\tilde{f_0} = f$, i.e., $\widetilde{A_n} = a_n$ for all n. We denote $\mathcal{S}_k(\Gamma_1(N))_F$ for the space of such cuspforms. As in the first definition of Serre, $\mathcal{S}_k(\Gamma_1(N))_F$ does not depend on the choice of the maximal ideal of $\bar{\mathbb{Z}}$ containing p nor on the embedding $F \to \bar{\mathbb{F}}_p$, and the Hecke and diamond correspondences act on it. We define $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$ to be the subspace of $\mathcal{S}_k(\Gamma_1(N))_F$ on which the diamond operator R_d acts by $\varepsilon(d)$ for each d prime to N.

Let now F be a finite field of characteristic p not dividing N and $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times$ be a character. We then have the inclusions

$$\mathcal{S}_k(N,\varepsilon)_F \subset \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}} \subset \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}} \tag{10}$$

and in some cases this inclusions can be strict. They are compatible with the actions of Hecke and diamond operators.

4.2. The various settings of Serre's conjecture.

If $f = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}}$ is normalized and f is an eigenvector of the Hecke operators T_l, for l prime not dividing pN (with associated eigenvalue a_l), Deligne ([3, Thm. 6.7]) proved that there exists a semisimple continuous representation

$$\rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F)$$

characterized (up to conjugation) by the following:

$$\left\{\begin{array}{l}\mathrm{Tr}\rho_f(\mathrm{Frob}_l) = a_l, \\ \det\rho_f(\mathrm{Frob}_l) = \varepsilon(l)l^{k-1}\end{array}\right. \text{ for all prime numbers } l \not| pN. \tag{11}$$

By Frob_l we mean an arithmetic Frobenius element at l.

The weak conjecture of Serre ([14, 3.2.3]) can be stated as

Conjecture 2 (Serre's weak conjecture). — *Let $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$ be a continuous homomorphism, where V is a 2-dimensional vector space over F. If ρ is absolutely irreducible and odd, then there exists a normalized modular cuspform f with coefficients in F (of some level, some weight and some character) which is an eigenvector of all Hecke operators T_l for l prime not dividing pN, and such that $\rho_f \cong \rho$.*

Serre associates a triple (N, k, ε) to ρ and in a first version of his strong version, Serre predicted that this modular cuspform f should belong to $\mathcal{S}_k(N,\varepsilon)_F$ (see [14, 3.2.4]). He realized soon afterwards that his definition of a modular form with coefficients in F was slightly too restrictive, and he suggested to replace $\mathcal{S}_k(N,\varepsilon)_F$ by $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}}$ or $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$. In the literature, the conjecture of Serre is usually studied in the Katz setting, we are going to look at the modified setting (i.e. the case $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$). Nevertheless we have the following theorem:

Theorem 6. — *The strong conjecture of Serre in the setting of Katz modular forms is equivalent to the conjecture in the modified setting.*

Proof. — The equivalence of the conjectures follows from the following facts: in these conjectures, the weight k attached to ρ by Serre is $\geqslant 2$.

But it is known that for $k \geqslant 2$, we have $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}} = \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$ except in the case where $N = 1$ and $p = 2$ or 3 (see [6, Lemma 1.9]; this observation will return several times in the proof of the main theorem: see §9.1). And for $p = 2$ or 3, absolutely irreducible odd representations $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F)$ with conductor 1 do not exist (see [15, p. 229, 3(i)] and [15, p. 710, note 229.2]). □

Remark. — Edixhoven defines another weight k' to ρ (see [5]). We always have $k' \leqslant k$ (and $k' = k$ in most cases). His refinement of the strong conjecture of Serre is that the modular form can be found in $\mathcal{S}_{k'}(N,\varepsilon)_F^{\mathrm{Katz}}$. This refinement implies the conjecture of Serre in the Katz setting. For $p \neq 2$, it is even known (but difficult to prove) that this refinement is equivalent to the Katz setting of Serre's conjecture and even to the weak version of Serre's conjecture (see [6, Thm. 1.12]).

5. The $\mathbb{Z}$-module $L_k(N)$.

5.1. Isomorphism with $\mathcal{H}_k(\Gamma_1(N))$.

We denote by M the module $\mathbb{Z}[\Gamma_1(N)\backslash SL_2(\mathbb{Z})] \otimes_{\mathbb{Z}} V_{k-2}$. Recall from the introduction that C_N is the set of pairs (u,v) of elements in $\mathbb{Z}/N\mathbb{Z}$ such that $\mathbb{Z}u+\mathbb{Z}v = \mathbb{Z}/N\mathbb{Z}$. Then there is a canonical bijection $\Gamma_1(N)\backslash SL_2(\mathbb{Z}) \to C_N$: it maps $\Gamma_1(N)g$ to the reduction mod N of the second row of g. We hence can define a $\mathbb{Z}$-linear map $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \to M$ by sending $(u,v) \otimes P(X,Y)$ to $\Gamma_1(N)g \otimes x$, where g is any matrix in $SL_2(\mathbb{Z})$ with second row congruent to $(u,v) \bmod N$, and x is the unique element in V_{k-2} such that $P(z,1) =< x, \binom{z}{1}^{\otimes k-2} >$ for every $z \in \mathbb{C}$ (see §1.2 for the definition of the pairing). This map can be extended to a $\mathbb{C}$-linear map

$$\iota_0 : \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \otimes_{\mathbb{Z}} \mathbb{C} \to M.$$

Lemma 2. — *The map ι_0 is an isomorphism.*

Proof. — This is clear from the definition and the fact that the pairing on V_{k-2} is non degenerate. □

We define a right action of $SL_2(\mathbb{Z})$ on $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ as follows:

$$((u,v) \otimes P(X,Y))|[g] = (au+cv, bu+dv) \otimes P(aX+bY, cX+dY),$$

for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Lemma 3.— *The isomorphism ι_0 is compatible with the action of $SL_2(\mathbb{Z})$ in the following sense: we have*

$$\iota_0(\xi\gamma) = \gamma^{-1}\iota_0(\xi)$$

for $\xi \in \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \otimes_{\mathbb{Z}} \mathbb{C}$ and $\gamma \in SL_2(\mathbb{Z})$.

Proof.— If $\iota_0(\xi) = \Gamma_1(N)g\otimes x$, we have $\gamma^{-1}\iota_0(\xi) = \Gamma_1(N)g\gamma\otimes\gamma^{-1}x$. On the other hand, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the second row of $g\gamma$ is congruent to $(au+cv, bu+dv) \bmod N$ and we have $P(az+b, cz+d) =< \gamma^{-1}x, \binom{z}{1}^{\otimes k-2} >$ for all $z \in \mathbb{C}$. The equality $\iota_0(\xi\gamma) = \gamma^{-1}\iota_0(\xi)$ follows. □

Recall from the introduction that $L_k(N)$ is defined as the quotient of $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ by the subspace generated by the elements of the form $x + x|[\sigma]$ and $x + x|[\tau] + x|[\tau^2]$ for $x \in \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$. (This subspace contains also the elements of the form $x - x|[-I]$ since $\sigma^2 = -I$.)

The map ι_0, composed with the projection $M \to M^+$ (with kernel M^-) defines, by passing to the quotient an isomorphism

$$\iota_1 : L_k(N) \otimes_{\mathbb{Z}} \mathbb{C} \to M^+/(M^{+\sigma} + M^{+\tau}).$$

When composing this isomorphism with the isomorphism (7) between $M^+/(M^{+\sigma} + M^{+\tau})$ and $\mathcal{H}_k(\Gamma_1(N))$, we get an isomorphism

$$\iota : L_k(N) \otimes_{\mathbb{Z}} \mathbb{C} \to \mathcal{H}_k(\Gamma_1(N)).$$

5.2. Hecke operators on $L_k(N)$.

For each integer $n \geqslant 1$, we define an operator T_n on $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ by the formula

$$T_n(x) = \sum_{A \in \mathcal{A}_n} x|[A]$$

for $x = (u,v) \otimes P(X,Y)$, where A runs over the finite set $\mathcal{A}_n$ of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ such that $ad - bc = n, a > b \geqslant 0, d > c \geqslant 0$, and where

$$x|[A] = \begin{cases} (ua+vc, ub+vd)\otimes P(aX+bY, cX+dY) & \text{if } (ua+vc, ub+vd) \in C_N, \\ 0 & \text{otherwise.} \end{cases}$$

Remark that $\sum_{A\in\mathcal{A}_n} A$ satisfies condition (8) (see [12, Prop. 20]).

The choice of this sum to define T_n looks a little bit arbitrary. Indeed, if we choose another sum $\sum m_B B$ in $\mathbb{Z}[M_2(\mathbb{Z})]$ (with support in the matrices of determinant n), which satisfies the same condition (8), we do not have $\sum_{A\in\mathcal{A}_n} x|[A] = \sum m_B x|[B]$. However, we have the following proposition.

Proposition 5. — *$\sum_{A\in\mathcal{A}_n} x|[A]$ and $\sum m_B x|[B]$ have the same images in $L_k(N)$.*

The proof is based on the following lemma (which is equivalent to [11, Prop. 4.3]).

Lemma 4. — *Let $\alpha = \sum u_G G \in \mathbb{Z}[SL_2(\mathbb{Z})]$ such that*

$$\sum u_G[G\infty] - u_G[G0] = 0 \quad \textit{in } \mathbb{Z}[\mathbb{P}^1(\mathbb{Q})], \tag{12}$$

then we have $\alpha \in \mathbb{Z}[SL_2(\mathbb{Z})](1+\sigma) + \mathbb{Z}[SL_2(\mathbb{Z})](1+\tau+\tau^2)$.

We prove Proposition 5. Since both $\sum_{A\in\mathcal{A}_n} A$ and $\sum m_B B$ satify (8), we have for every $\beta \in M_2(\mathbb{Z})$ with $\det(\beta)= n$,

$$\sum_{A\in\beta.SL_2(\mathbb{Z})\cap\mathcal{A}_n} [A\infty]-[A0]+ \sum_{B\in\beta.SL_2(\mathbb{Z})} -m_B[B\infty]+m_B[B0] = 0 \quad \text{in } \mathbb{P}^1(\mathbb{Q}).$$

We deduce

$$\sum_{\beta^{-1}A\in SL_2(\mathbb{Z})\cap\beta^{-1}\mathcal{A}_n} [\beta^{-1}A\infty] - [\beta^{-1}A0] + \sum_{\beta^{-1}B\in SL_2(\mathbb{Z})} -m_B[\beta^{-1}B\infty] + m_B[\beta^{-1}B0] = 0 \quad \text{in } \mathbb{P}^1(\mathbb{Q}).$$

Using Lemma 4, we can write therefore

$$\sum_{A\in\mathcal{A}_n} A - \sum m_B B = \sum \beta_i\gamma_i \tag{13}$$

with $\beta_i \in M_2(\mathbb{Z})$, $\det(\beta_i) = n, \gamma_i \in \mathbb{Z}[SL_2(\mathbb{Z})](1+\sigma)+\mathbb{Z}[SL_2(\mathbb{Z})](1+\tau+\tau^2)$. This proves the proposition.

We see from this that the composite map

$$\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \xrightarrow{T_n} \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \to L_k(N)$$

is unchanged if we replace $\sum_{A\in\mathcal{A}_n} A$ by $\sum m_B B$.

PROPOSITION 6. — *The Hecke operator defined on* $\mathbb{Z}[C_N]\otimes_{\mathbb{Z}}\mathbb{Z}[X,Y]_{k-2}$ *defines by passing to the quotient a well-defined map* $T_n : L_k(N) \to L_k(N)$.

Proof. — It suffices to prove that T_n vanishes on $\mathbb{Z}[C_N]\otimes_{\mathbb{Z}}\mathbb{Z}[X,Y]_{k-2}$ $(1+\sigma)$ and $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}(1+\tau+\tau^2)$. Since both $\sum_{A\in\mathcal{A}_n} A$ and $-\sum_{A\in\mathcal{A}_n} \sigma A$ are combinations which satisfy condition (8), we deduce by Lemma 4 that $\sum_{A\in\mathcal{A}_n} A + \sum_{A\in\mathcal{A}_n} \sigma A$ sends $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ to zero in $L_k(N)$. This exactly means that $\sum_{A\in\mathcal{A}_n} A$ vanishes on $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}(1+\sigma)$.

A similar proof holds for $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}(1+\tau+\tau^2)$ since $\sum_{A\in\mathcal{A}_n} A$ and $-\sum_{A\in\mathcal{A}_n} \tau A + \tau^2 A$ both satisfy condition (8). □

For each d prime to N, we define a diamond operator R_d on $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ by

$$R_d((u,v) \otimes P(X,Y)) = (du, dv) \otimes P(X,Y).$$

Since $R_d(x+x|[\sigma]) = R_d(x) + (R_d(x))|[\sigma]$ and $R_d(x+x|[\tau]+x|[\tau^2]) = R_d(x) + (R_d(x))|[\tau] + (R_d(x))|[\tau^2]$ for every $x \in \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$, we deduce that R_d stabilizes the subgroup of $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ generated by the elements of the form $x + x|[\sigma]$ and $x + x|[\tau] + x|[\tau^2]$ for $x \in \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$. We therefore have

PROPOSITION 7. — *The diamond operator defined on* $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ *defines by passing to the quotient a well-defined map* $R_d : L_k(N) \to L_k(N)$.

Remark. — It is clear, not immediately from the definition but from Proposition 5 and Lemma 4, that the Hecke and diamond operators commute on $L_k(N)$.

5.3. Compatibility of Hecke operators.

Proposition 8. — *The operators T_n and R_d on $L_k(N)$ agree through the isomorphism ι with the operators T'_n and R'_d on $\mathcal{H}_k(\Gamma_1(N))$.*

Proof. — When we identify $\mathcal{H}_k(\Gamma_1(N))$ and $M^+/(M^{+\sigma}+M^{+\tau})$, the Hecke operator T'_n gets identified with an operator, still denoted T'_n, on $M^+/(M^{+\sigma}+M^{+\tau})$. By Proposition 3, the map $\phi : M \to M$ defined by

$$\phi(\Gamma_1(N)g \otimes x) = \sum_{A\in\mathcal{A}_n} \sum_{\substack{\Gamma_1(N)h\in\Gamma_1(N)\backslash SL_2(\mathbb{Z}) \\ gA\in\Delta'_n h}} \Gamma_1(N)h \otimes \tilde{A}x$$

maps M^+ to M^+ and defines T'_n by passing to the quotient. If (u,v) (resp. (u',v')) is the reduction mod N of the second row of g (resp. h) and if $A = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$, we remark that the condition $gA \in \Delta'_n h$ is equivalent to $(au+cv, bu+dv) = (u',v')$. If $P(X,Y) \in \mathbb{Z}[X,Y]_{k-2}$ is such that $P(z,1) = < x, \left(\begin{smallmatrix} z \\ 1\end{smallmatrix}\right)^{\otimes k-2} >$ for all $z \in \mathbb{C}$, then $Q(X,Y) = P(aX+bY, cX+dY)$ is such that

$$\begin{aligned} Q(z,1) &= P(az+b, cz+d) \\ &= (cz+d)^{k-2} < x, \begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix}^{\otimes k-2} > \\ &=< x, A\begin{pmatrix} z \\ 1 \end{pmatrix}^{\otimes k-2} > \\ &=< \tilde{A}x, \begin{pmatrix} z \\ 1 \end{pmatrix}^{\otimes k-2} > \end{aligned}$$

for all $z \in \mathbb{C}$. This shows that, by the isomorphism ι_0, ϕ gets identified with the map $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \otimes_{\mathbb{Z}} \mathbb{C} \to \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2} \otimes_{\mathbb{Z}} \mathbb{C}$ deduced from $x \mapsto \sum_{A\in\mathcal{A}_n} x|[A]$ by the extension of scalars. Proposition 8 follows for the Hecke operators.

The case of diamond operators is treated in a similar way, but is simpler. Looking at Proposition 4, and if (u,v) is the reduction mod N of the second row of g, the reduction of the second row of $\sigma_d g$ is congruent to (du, dv). We conclude as in the case of Hecke operators. □

6. Relation between $L_k(N)$ and $\mathcal{S}_k(\Gamma_1(N))$.

Recall that $\mathcal{M}_k(\Gamma_1(N))$ denote the space of modular forms of weight k for $\Gamma_1(N)$, $\mathcal{S}_k(\Gamma_1(N))$ the subspace of cuspforms and $\mathcal{E}_k(\Gamma_1(N))$ the space of Eisenstein series, i.e., the orthogonal complement of $\mathcal{S}_k(\Gamma_1(N))$ in $\mathcal{M}_k(\Gamma_1(N))$ for the Petersson scalar product.

THEOREM 7. — *There exists an isomorphism of complex vector spaces*

$$\mathrm{Hom}_{\mathbb{Z}}(L_k(N),\mathbb{C}) \to \mathcal{S}_k(\Gamma_1(N)) \times \mathrm{Hom}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_1(N)),\mathbb{C}) \\ \times \mathrm{Hom}_{\mathbb{C}}(\mathcal{E}_k(\Gamma_1(N)),\mathbb{C})$$

such that $\mathrm{Hom}(T,1)$ *on the first space agrees with* $T \times \mathrm{Hom}(T,1) \times \mathrm{Hom}(T,1)$ *on the second, with T either a Hecke operator T_n or a diamond operator R_d.*

Proof. — There exists by Proposition 8 an isomorphism

$$L_k(N) \otimes_{\mathbb{Z}} \mathbb{C} \to \mathcal{H}_k(\Gamma_1(N))$$

such that T on the first space agrees with T' on the second. Theorem 2 yields an isomorphism

$$\mathcal{M}_k(\Gamma_1(N)) \times \overline{\mathcal{S}_k(\Gamma_1(N))} \to \mathcal{H}_k(\Gamma_1(N))$$

compatible with the actions of T' on both spaces (where T' acts on $\overline{\mathcal{S}_k(\Gamma_1(N))}$ by $T'(\bar{f}) = \overline{T'f}$).

The Petersson scalar product yields an isomorphism

$$\begin{array}{ccc} \overline{\mathcal{S}_k(\Gamma_1(N))} & \to & \mathrm{Hom}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_1(N)),\mathbb{C}) \\ \bar{g} & \mapsto & \left(f \mapsto < f,g >_{\Gamma_1(N)}\right) \end{array}$$

by which T' on the first space is identified with $\mathrm{Hom}(T,1)$ on the second (see e.g. [16, Prop. 3.39]).

Finally the Atkin-Lehner involution gives an isomorphism

$$W_N : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

which transforms T' in T (see §1.1).

Combining all these isomorphisms, we get an isomorphism

$$L_k(N)\otimes_{\mathbb{Z}}\mathbb{C}\to\mathcal{M}_k(\Gamma_1(N))\times\mathrm{Hom}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_1(N)),\mathbb{C})$$

$$=\mathcal{S}_k(\Gamma_1(N))\times\mathcal{E}_k(\Gamma_1(N))\times\mathrm{Hom}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_1(N)),\mathbb{C})$$

such that $T\otimes 1$ on the first space agrees with $T\times T\times\mathrm{Hom}_{\mathbb{C}}(T,1)$ on the second. The proposition follows by duality. □

7. On the torsion in $L_k(N)$.

Let E be a free $\mathbb{Z}$-module of finite rank and p be a prime number. If E' is a submodule of E, the following conditions are equivalent:

a) E/E' has no (non trivial) p-torsion;

b) the map $E'/pE'\to E/pE$ deduced from the injection $E'\to E$ is injective;

c) the dimension over $\mathbb{F}_p$ of the image of the map $E'/pE'\to E/pE$ is larger than or equal to the rank of E' over $\mathbb{Z}$.

Lemma 5.— *Let E be a free $\mathbb{Z}$-module of finite rank, E_1 and E_2 be two submodules of E and p be a prime number. Assume that E/E_1 and E/E_2 have no p-torsion and denote by $\bar{E}_1$ and $\bar{E}_2$ the images of the maps $E_1/pE_1\to E/pE$, $E_2/pE_2\to E/pE$. The following conditions are equivalent:*

1. *$E/(E_1+E_2)$ has no p-torsion;*
2. *$\dim_{\mathbb{F}_p}(\bar{E}_1\cap\bar{E}_2)\leqslant\mathrm{rk}_{\mathbb{Z}}(E_1\cap E_2)$.*

Proof.— The image of the map $(E_1+E_2)/p(E_1+E_2)\to E/pE$ is $\bar{E}_1+\bar{E}_2$. Its dimension over $\mathbb{F}_p$ is

$$\dim_{\mathbb{F}_p}\bar{E}_1+\dim_{\mathbb{F}_p}\bar{E}_2-\dim_{\mathbb{F}_p}(\bar{E}_1\cap\bar{E}_2).$$

On the other hand, the rank over $\mathbb{Z}$ of E_1+E_2 is

$$\mathrm{rk}_{\mathbb{Z}}E_1+\mathrm{rk}_{\mathbb{Z}}E_2-\mathrm{rk}_{\mathbb{Z}}(E_1\cap E_2).$$

We have $\mathrm{rk}_{\mathbb{Z}}E_1=\dim_{\mathbb{F}_p}\bar{E}_1$, $\mathrm{rk}_{\mathbb{Z}}E_2=\dim_{\mathbb{F}_p}\bar{E}_2$, since E/E_1 and E/E_2 have no p-torsion. The lemma follows from the equivalence of a) and c) for $E'=E_1+E_2$. □

LEMMA 6. — *Let p be an odd prime number. Any polynomial $P \in \mathbb{F}_p[X,Y]$ of degree $\leqslant p$ such that $P(X,Y) = P(aX+bY, cX+dY)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{F}_p)$ is constant.*

Proof. — We can assume that P is homogeneous of some degree $d \neq 0$ with $d \leqslant p$. We have to prove that $P = 0$. If $Q(X) = P(X,1)$ then $Q(X+1) = Q(X)$, hence Q is a polynomial in $X^p - X$. Since $d \leqslant p$, Q is of the form $a(X^p - X) + b$ for some $a, b \in \mathbb{F}_p$. So we have $d = p$ and $P(X,Y) = a(X^p - XY^{p-1}) + bY^p$. Exchanging the roles of X and Y, we see that P must also be a linear combination of X^p and $Y^p - YX^{p-1}$, hence $P = 0$. □

Remark. — When $p = 2$, the lemma is true for degree 0 and 1. The homogeneous polynomials of degree 2 which are invariant under $SL_2(\mathbb{F}_2)$ are the scalar multiples of $X^2 + XY + Y^2$.

PROPOSITION 9. — *Let p be a prime number not dividing N. Assume $k \leqslant p+2$ if $p \neq 2$, and $k \leqslant 3$ if $p = 2$. Then the $\mathbb{Z}$-module $L_k(N)$ has no p-torsion, except in the case where $N = 1$, $p = 2$, $k = 3$.*

Proof. — First we apply Lemma 5 with $E = \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$, $E_1 = E^\sigma$ and $E_2 = E^\tau$ in order to prove that $E/(E^\sigma + E^\tau)$ has no p-torsion. Then $E_1 \cap E_2$ is the set of elements of $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$ fixed under $SL_2(\mathbb{Z})$. If we identify C_N with $\Gamma_1(N)\backslash SL_2(\mathbb{Z})$, $E_1 \cap E_2$ consists of the elements

$$\sum_{g \in \Gamma_1(N)\backslash SL_2(\mathbb{Z})} \Gamma_1(N)g \otimes (P \circ g)$$

where $P \in \mathbb{Z}[X,Y]_{k-2}$ is such that $P \circ \gamma = P$ for all $\gamma \in \Gamma_1(N)$. (We write $P \circ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ for the polynomial $P(aX+bY, cX+dY)$.) Any such polynomial is constant (hence 0 if $k \geqslant 3$). Therefore the rank over $\mathbb{Z}$ of $E_1 \cap E_2$ is 1 if $k = 2$ and 0 if $k \geqslant 3$.

Let $\bar{E}_1, \bar{E}_2$ denote the images of E_1/pE_1 and E_2/pE_2 in $\bar{E} = E/pE$. We have $\bar{E}_1 \subset \bar{E}^\sigma$, $\bar{E}_2 \subset \bar{E}^\tau$, hence $\bar{E}_1 \cap \bar{E}_2$ is contained in the subspace of $\bar{E}$ fixed by $SL_2(\mathbb{Z})$. Exactly as above, we see that the dimension r of this subspace is equal to the dimension of the subspace of $\mathbb{F}_p[X,Y]_{k-2}$ fixed by $\Gamma_1(N)$. Since p is prime to N, the map $\Gamma_1(N) \to SL_2(\mathbb{F}_p)$ is surjective, and it follows from Lemma 6 that $r = 1$ if $k = 2$ and $r = 0$ if $k \geqslant 3$.

We have proved that $\dim_{\mathbb{F}_p}(\bar{E}_1 \cap \bar{E}_2) \leqslant \mathrm{rk}_{\mathbb{Z}}(E_1 \cap E_2)$. By Lemma 5, $E/(E_1 + E_2)$ has no p-torsion.

We now prove that $E^+/(E^{+\sigma} + E^{+\tau})$ has no p-torsion (for $E = \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$). For this, we remark that $E^\sigma = E^{+\sigma}$ since $\sigma^2 = -I$, hence

$$\begin{aligned} E^+ \cap (E^\sigma + E^\tau) &= E^{+\sigma} + (E^+ \cap E^\tau) \\ &= E^{+\sigma} + E^{+\tau}. \end{aligned}$$

This implies that the linear map

$$E^+/(E^{+\sigma} + E^{+\tau}) \to E/(E^\sigma + E^\tau)$$

is injective, hence our assertion.

We now prove the proposition when $N \geqslant 4$. In this case $-I$ (and hence also σ) acts without fixed points on C_N. It follows that any element in E^+ (resp. E^-) is of the form $x + x|[-I]$ (resp. $x - x|[-I]$) for some $x \in E$. Therefore the linear map

$$\begin{array}{ccc} E & \longrightarrow & E^+ \\ x & \longmapsto & x + x|[-I] \end{array}$$

is surjective, and its kernel is contained in the kernel of the canonical surjection $E \to L_k(N)$.

By passing to the quotient, we get an isomorphism from $L_k(N)$ to E^+/A, where A is the subgroup of E^+ generated by the elements of the form $x + x|[\sigma]$ and $x + x|[\tau] + x|[\tau^2]$, where $x \in E^+$.

Since σ acts without fixed points on C_N, the elements of the form $x + x|[\sigma]$ for $x \in E^+$, i.e., of the form $y + y|[\sigma] + y|[\sigma^2] + y|[\sigma^3]$ for $y \in E$, coincide with the elements of $E^\sigma = E^{+\sigma}$. Similarly, since the group of order 6 generated by $-\tau$ acts without fixed points on C_N, the set of elements of the form $x + x|[\tau] + x|[\tau^2]$ with $x \in E^+$ is equal to $E^{+\tau}$. From this we conclude that $L_k(N)$ is isomorphic to $E^+/(E^{+\sigma} + E^{+\tau})$, hence has no p-torsion.

If $N = 3$, σ acts without fixed points on C_3. Similar arguments as above show that $L_k(N)$ becomes isomorphic to $E^+/(E^{+\sigma} + E^{+\tau})$ after tensoring by $\mathbb{Z}[1/3]$. This proves the proposition since $p \neq 3$ in this case.

If $N = 2$, τ acts without fixed points on C_2. Similar arguments as above show that $L_k(N)$ is isomorphic to $E^+/(E^{+\sigma} + E^{+\tau})$ after tensoring by $\mathbb{Z}[1/2]$. This proves the proposition since $p \neq 2$ in this case.

If $N = 1$, the same proof works after tensoring by $\mathbb{Z}[1/6]$, hence for $p \neq 2, 3$. We conclude the proof by a direct (and easy) computation, which shows that $L_2(1) \cong 0$, $L_3(1) \cong \mathbb{Z}/2\mathbb{Z}$, $L_4(1) \cong \mathbb{Z}$ and $L_5(1) \cong \mathbb{Z}/2\mathbb{Z}$. □

Remark. — Since $L_3(1)$ is isomorphic to $\frac{\mathbb{Z}[X,Y]_1}{<X-Y,2X>} \cong \mathbb{Z}/2\mathbb{Z}$ we can look at the action of the Hecke operator T_l (l an odd prime) on the non zero element $\bar{X}$ of $L_3(1) \cong \mathbb{Z}/2\mathbb{Z}$. We deduce that

$$\sum_{A \in \mathcal{A}_l} \bar{X}|[A] = \sum_{A \in \mathcal{A}_l} (a+b)\bar{X} \quad \text{where } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

By [12, Lemma 6, Lemma 7], we can devide $\mathcal{A}_l$ in $l+1$ subsets (each contained in a different right $SL_2(\mathbb{Z})$-coset) of the form

$$\left\{ \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}, \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \ldots, \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \right\}$$

where $\binom{b_i}{d_i} = \binom{a_{i+1}}{c_{i+1}}$ for $0 \leqslant i < n$, and $c_0 = b_n = 0$. For each of this cosets we have $\sum_{i=0}^{n}(a_i + b_i) \equiv a_0 \equiv 1 \bmod 2$ since a_0 is equal to 1 or l. Since, for l an odd prime, $l+1$ is even, we conclude that all T_l act on $L_3(1)$ with eigenvalues zero in characteristic 2.

8. On the representation of $GL_2(\mathbb{F}_p)$ on $\mathbb{F}_p[X,Y]$.

8.1. Lowering the degree.

Let $d \geqslant 0$ be an integer and p be a prime number. Denote U_d for the $\mathbb{F}_p$–vector space of homogeneous functions of degree d on $\mathbb{F}_p^2 - \{(0,0)\}$. There is a natural action of $GL_2(\mathbb{F}_p)$ on U_d given by

$$(f.\alpha)(x,y) = f(ax+by, cx+dy) \quad \text{for } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_p).$$

There is an action of Hecke operators on $\mathbb{Z}[C_N] \otimes U_d$ given by the formula

$$T_n(x) = \sum_{A \in \mathcal{A}_n} x|[A]$$

where

$$x|[A] = \begin{cases} (ua+vc, ub+vd) \otimes f.A & \text{if } (ua+vc, ub+vd) \in C_N, \\ 0 & \text{otherwise,} \end{cases}$$

for $x = (u,v) \otimes f$. Again this choice is an arbitrary choice, but in a similar way as in §5.2, one shows that this operator is well-defined modulo the right action of $(1+\sigma)$ and $(1+\tau+\tau^2)$. The action of a diamond operator is given by

$$R_{d'}((u,v)\otimes f) = (d'u, d'v)\otimes f \quad \text{for } d' \text{ prime to } N,$$

with $(u,v)\in C_N$ and $f\in U_d$. We have the following proposition.

Proposition 10. — *Let $d>p$, then there exists an exact sequence*

$$0 \to \mathbb{F}_p[X,Y]_{d-(p+1)} \overset{u}{\hookrightarrow} \mathbb{F}_p[X,Y]_d \to U_d \to 0.$$

The injection u is given by multiplication by $Q := X^pY - Y^pX$ and we have $u(P)\circ g = \det(g)u(P\circ g)$ for $P\in\mathbb{F}_p[X,Y]_{d-(p+1)}$ and $g\in GL_2(\mathbb{F}_p)$. The map $\mathbb{F}_p[X,Y]_d \to U_d$ is given by

$$P \mapsto ((x,y)\mapsto P(x,y))$$

and is compatible with the action of $GL_2(\mathbb{F}_p)$.

Proof. — Injectivity of u is obvious. A polynomial $R\in\mathbb{F}_p[X,Y]_d$ vanishes on $\mathbb{F}_p^2$ if and only if it is a multiple of all $\mathbb{F}_p$-linear forms, i.e., of $Y\prod_{a\in\mathbb{F}_p}(X-aY) = YX(X^{p-1}-Y^{p-1}) = Q$. This proves that the image of u is the kernel of the map $\mathbb{F}_p[X,Y]_d \to U_d$. Counting dimensions shows that this latter map is surjective.

Comparing the action of $GL_2(\mathbb{F}_p)$ on $\mathbb{F}_p[X,Y]_d$ and U_d we deduce that the second map is compatible with the action of $GL_2(\mathbb{F}_p)$. On the other hand, the polynomial Q is not invariant under $GL_2(\mathbb{F}_p)$. One has $Q\circ g = \det(g)Q$. We deduce that for a polynomial $P\in\mathbb{F}_p[X,Y]_{d-(p+1)}$ we have

$$\begin{aligned} u(P)\circ g = (PQ)\circ g &= (P\circ g)\ (Q\circ g) \\ &= \det(g)\ (P\circ g)\ Q \\ &= \det(g)\ u(P\circ g). \end{aligned}$$

□

8.2. Degree $d\leqslant p-1$.

Suppose that $d\leqslant p-1$.

Proposition 11. — *There exists an exact sequence*

$$0 \to \mathbb{F}_p[X,Y]_d \to U_d \overset{v}{\to} \mathbb{F}_p[X,Y]_{p-1-d} \to 0$$

where the first map is compatible with the action of $GL_2(\mathbb{F}_p)$ *and* $v(f.g) = \det(g)^d v(f) \circ g$ *for* $f \in U_d$ *and* $g \in GL_2(\mathbb{F}_p)$.

Proof. — The first map is

$$P \mapsto ((x,y) \mapsto P(x,y)).$$

This map is compatible with the action of $GL_2(\mathbb{F}_p)$. We have a duality

$$U_d \times U_{p-1-d} \to \mathbb{F}_p$$

defined by

$$(f,f') \mapsto \sum_{(x,y)\neq(0,0)} f(x,y)f'(x,y).$$

We have that $< f.g, f' >=< f, f'.g^{-1} >$ for any $g \in GL_2(\mathbb{F}_p)$. The orthogonal complement of $\mathbb{F}_p[X,Y]_d$, viewed as a subspace of U_d by the first map, with respect to this duality is $\mathbb{F}_p[X,Y]_{p-1-d}$, viewed as a subspace of U_{p-1-d} in a similar way: indeed these two subspaces are orthogonal since $\sum_{(x,y)\in\mathbb{F}_p^2} P(x,y) = 0$ for all $P \in \mathbb{F}_p[X,Y]_{p-1}$ (as one checks easily by taking for P a monomial), and the sum of their dimensions, $d+1$ and $p-d$, is equal to $p+1$, the dimension of U_d. This yields an isomorphism from $U_d/\mathbb{F}_p[X,Y]_d$ to the dual of $\mathbb{F}_p[X,Y]_{p-1-d}$.

On the other hand, as in the pairing on V_k (see §1.2), one deduces from the pairing $< (u,v),(u',v') >= uv' - u'v$ on $\mathbb{F}_p^2$ a pairing on $TS^{p-1-d}(\mathbb{F}_p^2)$, which is non degenerated since $p-1-d \leqslant p-1$. Identifying $\mathbb{F}_p[X,Y]_{p-1-d}$ with the dual of $TS^{p-1-d}(\mathbb{F}_p^2)$ as in §5.1, one gets a duality

$$\mathbb{F}_p[X,Y]_{p-1-d} \times \mathbb{F}_p[X,Y]_{p-1-d} \to \mathbb{F}_p$$

which satisfies $< P \circ g,\ Q > = < P,\ Q \circ \tilde{g} >$, where $P, Q \in \mathbb{F}_p[X,Y]_{p-1-d}$, $g \in GL_2(\mathbb{F}_p)$ and $\tilde{g} = \det(g)g^{-1}$. This yields an isomorphism between the dual of $\mathbb{F}_p[X,Y]_{p-1-d}$ and $\mathbb{F}_p[X,Y]_{p-1-d}$ itself. By composing this isomorphism with the previous one, one gets the surjective map $v : U_d \to \mathbb{F}_p[X,Y]_{p-1-d}$ with kernel $\mathbb{F}_p[X,Y]_d$.

Using the compatibility properties of the previous pairings with the action of $GL_2(\mathbb{F}_p)$, we deduce that $v(f.g) = \det(g)^d v(f) \circ g$ for $f \in U_d$ and $g \in GL_2(\mathbb{F}_p)$. □

9. Proof of the main theorem.

9.1. From characteristic zero to characteristic p.

In this section, F denotes a finite field of characteristic p prime to N. For each prime l not dividing pN, let a_l be an element of F. Let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times$ be a Dirichlet character with values in F such that $\varepsilon(-1) = (-1)^k$. We want to compare the following two conditions:

(C1) There exists a non zero linear map $\mu : L_k(N) \to F$ such that $\mu \circ T_l = a_l \mu$ for all primes l not dividing pN, and $\mu \circ R_d = \varepsilon(d)\mu$ for d prime to N.

(C2) There exists a non zero $f \in \mathcal{S}_k(N, \varepsilon)_F^{\mathrm{mod}}$ (see §4.2 for the definition of this space) such that $T_l f = a_l f$ for all primes $l \not| pN$.

We shall also consider the condition:

(C3) There exist integers $M, M' \geqslant 1$ such that $MM'|N$, integers i, j such that $i + j \equiv k - 1 \bmod p - 1$, a finite extension F' of F, and Dirichlet characters $\varepsilon_1 : (\mathbb{Z}/M\mathbb{Z})^\times \to F'^\times$, $\varepsilon_2 : (\mathbb{Z}/M'\mathbb{Z})^\times \to F'^\times$, such that $\varepsilon_1\varepsilon_2 = \varepsilon$ and $\varepsilon_1(l)l^i + \varepsilon_2(l)l^j = a_l$ for all primes $l \not| pN$.

Note that condition (C3) only depends on $k \bmod p - 1$. We shall prove

Proposition 12. — *If* (C2) *holds, then* (C1) *holds.*

Proposition 13. — *If* (C1) *holds,* (C2) *or* (C3) *holds.*

Proof. — Let us identify F with $R/\mathcal{P}$, where R is the ring of integers of a number field K, and $\mathcal{P}$ a maximal ideal of R containing p. Let V, V_1, V_2, V_3 denote the vector spaces $\mathrm{Hom}_{\mathbb{Z}}(L_k(N), K)$, $\mathcal{S}_k(\Gamma_1(N))_K$, $\mathrm{Hom}_K(\mathcal{S}_k(\Gamma_1(N))_K, K)$ and $\mathrm{Hom}_K(\mathcal{E}_k(\Gamma_1(N))_K, K)$. Let A denote the commutative algebra over R generated by indeterminates T_l (for l prime not dividing pN) and R_d (for d prime to p). We let A act R-linearly on V, V_1, V_2, V_3.

The $A \otimes_R \mathbb{C}$-modules deduced from V and $V_1 \times V_2 \times V_3$ by extending scalars from K to $\mathbb{C}$ are isomorphic by Theorem 7. By Theorem 4, the A-modules V and $V_1 \times V_2 \times V_3$ are isomorphic. Let M, M_1, M_2, M_3 be R-lattices in V, V_1, V_2, V_3 stable by A, and $\bar{M}, \bar{M}_1, \bar{M}_2, \bar{M}_3$ their reductions mod $\mathcal{P}$. Finally, let $\chi : A \to F$ denote the homomorphism of R-algebras which maps T_l to a_l for all primes $l \not| pN$, and R_d to $\varepsilon(d)$ for d prime to N. We denote by $\bar{M}(\chi)$ the set of elements $x \in \bar{M}$ such that $ax = \chi(a)x$ for all $a \in A$. The condition $\bar{M}(\chi) \neq 0$ is independent of the choice of the R-lattice M by Corollary 1, and similar statements hold for M_1, M_2, M_3. Moreover we have $\bar{M}(\chi) \neq 0$ if and only if one of the spaces $\bar{M}_1(\chi), \bar{M}_2(\chi), \bar{M}_3(\chi)$ is different from 0.

We can take for M_1 the R-module $\mathcal{S}_k(\Gamma_1(N))_R$; we then have $\bar{M}_1 = \mathcal{S}_k(\Gamma_1(N))_F$ and the condition $\bar{M}_1(\chi) \neq 0$ is equivalent to (C2).

We can take for M_2 the R-module $\mathrm{Hom}_R(\mathcal{S}_k(\Gamma_1(N))_R, R)$; then $\bar{M}_2$ gets identified with $\mathrm{Hom}_F(\mathcal{S}_k(\Gamma_1(N))_F, F)$ and condition $\bar{M}_2(\chi) \neq 0$ is equivalent to $\bar{M}_1(\chi) \neq 0$, hence to (C2).

We can take for M the R-module $\mathrm{Hom}_{\mathbb{Z}}(L_k(N), R)$. Then $\bar{M}$ gets identified with $\mathrm{Hom}_{\mathbb{Z}}(L_k(N)/L_k(N)_{\mathrm{tors}}, F)$. The condition $\bar{M}(\chi) \neq 0$ implies (C1).

Proposition 12 follows from the four last alineas. We now prove Proposition 13. We distinguish 4 cases:

9.1.1. Case 1: $k \leqslant p+2$ if $p \neq 2$; $k \leqslant 3$ if $p=2$ and $(N,p,k) \neq (1,2,3)$.

In this case $L_k(N)$ has no p-torsion by Proposition 9, and the condition $\bar{M}(\chi) \neq 0$ is equivalent to (C1). Therefore to conclude, it will suffice to show that $\bar{M}_3(\chi) \neq 0$ implies (C3). We can for this extend the scalars and assume that M_3 has a basis in which A acts by upper triangular matrices. The characters $\chi_i : A \to R^\times$ appearing as diagonal entries are described in [13] (they are essential $\varepsilon_1(d)\varepsilon_2(d)$ for R_d and $\sum_{dd'=n} \varepsilon_1(d)\varepsilon_2(d')d'^{k-1}$ for T_n, where $\varepsilon_1, \varepsilon_2$ are the convenient characters) and $\bar{M}_3(\chi) \neq 0$ if and only if χ is the reduction modulo $\mathcal{P}$ of one of the χ_i's. Hence $\bar{M}_3(\chi) \neq 0$ implies (C3).

9.1.2. Case 2: $(N,p,k) = (1,2,3)$.

In this case (C1) is equivalent to say that $a_l = 0$ for all $l \neq 2$ by the remark at the end of §7, and (C3) is equivalent to the same statement. Finally (C2) is never satisfied since $\mathcal{S}_3(\Gamma_1(1))_F^{\mathrm{mod}} = \{0\}$.

9.1.3. Case 3: $(p,k) = (2,4)$.

Remark that we have an isomorphism

$$\begin{array}{ccc} \mathbb{F}_2[X,Y]_1 \oplus \mathbb{F}_2[X,Y]_0 & \to & \mathbb{F}_2[X,Y]_2 \\ (aX+bY, c) & \mapsto & aX^2+bY^2+c(X^2+XY+Y^2) \end{array}$$

with $a, b, c \in \mathbb{F}_2$. This isomorphism is compatible with the right action of $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$. We deduce an isomorphism

$$(\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{F}_2[X,Y]_1) \oplus (\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{F}_2[X,Y]_0) \cong \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{F}_2[X,Y]_2$$

which is compatible with the action of the Hecke operators T_l (with l an odd prime) and diamond operators.

Suppose that (C1) is true for $k = 4$. Then the non zero linear map $\mu : \mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_2 \to F$ induces a non zero linear map on one of the two factors $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{F}_2[X,Y]_1$ or $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{F}_2[X,Y]_0$. Therefore (C1) is satisfied for $k = 2$ or $k = 3$ with the same eigenvalues. Hence by the previous cases, either (C2) is satisfied for $k = 2$ or $k = 3$ and an $f \in \mathcal{S}_2(N, \varepsilon)_F^{\mathrm{mod}}$ or $f \in \mathcal{S}_3(N, \varepsilon)_F^{\mathrm{mod}}$ or (C3) is satisfied for $k = 2$ or $k = 3$. If $N = 1$ (C2) cannot be satisfied since $\mathcal{S}_k(\Gamma_1(1)) = \{0\}$ (and hence $\mathcal{S}_k(\Gamma_1(1))_F = \{0\}$) for $k \leqslant 3$ (see e.g. [8]). If $N > 1$ and (C2) is satisfied, we conclude by replacing f by $A_1 f$ or by $A_1^2 f$ where A_1 is the Hasse invariant in characteristic 2. Indeed, one gets $A_1 f$ or $A_1^2 f \in \mathcal{S}_4(N, \varepsilon)_F^{\mathrm{Katz}} = \mathcal{S}_4(N, \varepsilon)_F^{\mathrm{mod}}$ (see [5, §3.1], [6, Lemma 1.9] and §4.2). This proves the proposition in case $p = 2$ and $k = 4$.

9.1.4. Case 4: general case.

We argue by induction on k. For $N = 1$ and $p = 2$ or $p = 3$ we will prove the stronger statement that (C1) implies (C3). When $k \leqslant p + 2$, Proposition 13 follows from the cases 1, 2 and 3. In case $N = 1$ and $p = 2$ or $p = 3$ (C2) is never satisfied for $k \leqslant 5$.

So we can assume $k > p + 2$. From the exact sequence in Proposition 10 we deduce an exact sequence

$$0 \to \mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{k-p-3} \xrightarrow{u'} \mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{k-2} \to \mathbb{Z}[C_N] \otimes U_{k-2} \to 0.$$

Hecke and diamond operators are compatible with the second map. The first map satisfies

$$u'(T_n x) = \frac{1}{n} T_n(u'(x)) \quad \text{and} \quad u'(R_d x) = R_d(u'(x))$$

for $x \in \mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{k-p-3}$, $n \geqslant 1$ prime to p and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Suppose that (C1) is true for k. Hence, the non zero linear map

$$\mu : \mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{k-2} \to \mathbb{F}_p$$

either

a) has non zero restriction to $\mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{k-p-3}$,

b) factors through $\mathbb{Z}[C_N] \otimes U_{k-2}$.

In case a), we have that (C1) is satisfied for $k-p-1$, with a_l replaced by $b_l = a_l/l$ and same ε. Using the induction hypothesis, we see that we are in one of the two following cases:

- there exists an $f \in \mathcal{S}_{k-p-1}(N,\varepsilon)_F^{\mathrm{mod}}$ such that $T_l f = b_l f$ for l prime to pN, $R_d f = \varepsilon(d) f$ and $(N,p) \neq (1,2)$ or $(1,3)$. In this case, we conclude the proof by $q\frac{df}{dq} \in \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}}$ (see [5, §3.1]) and $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}} = \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$ (see [6, Lemma 1.9] and §4.2). Remark that f can (and has to) be choosen such that $q\frac{df}{dq}$ is non zero. Indeed, otherwise f would be a p^{th} power, i.e., $f = \sum c_n^p q^{np}$ ($c_n \in F$) but, we can then take $\sum c_n^p q^n$ instead.
- there exist integers $M, M' \geqslant 1$ such that $MM'|N$, integers i', j' such that $i' + j' \equiv k' - 1 \bmod p-1$ (with $k' = k-p-1$), a finite extension F' of F, and Dirichlet characters $\varepsilon_1 : (\mathbb{Z}/M\mathbb{Z})^\times \to F'^\times$, $\varepsilon_2 : (\mathbb{Z}/M'\mathbb{Z})^\times \to F'^\times$, such that $\varepsilon_1\varepsilon_2 = \varepsilon$ and $\varepsilon_1(l)l^{i'} + \varepsilon_2(l)l^{j'} = b_l$ for all primes $l \not| pN$. We conclude by taking the same $M, M', \varepsilon_1, \varepsilon_2, F'$ and by $i = i' + 1, j' = j + 1$.

In case b), we remark that U_{k-2} only depends on $k \bmod p-1$. Therefore we find an integer d' with $1 \leqslant d' \leqslant p-1$ such that $d' \equiv k-2 \bmod p-1$ and $U_{d'} = U_{k-2}$. From Proposition 11, we deduce an exact sequence

$$0 \to \mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{d'} \to \mathbb{Z}[C_N] \otimes U_{d'} \xrightarrow{v'} \mathbb{Z}[C_N] \otimes \mathbb{F}_p[X,Y]_{p-1-d'} \to 0.$$

Hecke and diamond operators are compatible with the first map. The second satisfies

$$v'(T_n(x)) = n^{d'} T_n(v'(x)) \quad \text{and} \quad v'(R_d(x)) = R_d(v'(x))$$

for $x \in \mathbb{Z}[C_N] \otimes U_{d'}$, $n \geqslant 1$ prime to pN and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Since we have a non zero map in the middle term of the exact sequence, it is either non zero on the left term, or its factors through the right term.

By cases 1, 2 and 3, we obtain in the first case either a cuspform of weight $d'+2$ with eigenvalues a_l, character ε or that (C3) is satisfied for $d'+2$ and a_l (and hence for k since $d'+2 \equiv k \bmod p-1$). This finishes the proof, since we can multiply the cuspform with an appropriate times the Hasse invariant A_{p-1} in characteristic p, such that we obtain a cuspform of weight k, with the same eigenvalues a_l and same character ε (see [5, §3.1]). Note that we use again $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}} = \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$ since we are in the case $(N,p) \neq (1,2)$ or $(1,3)$ by induction hypothesis.

In the second case, we obtain by Proposition 13 a cuspform of weight $p+1-d'$ with eigenvalues $a_l/l^{d'}$ and character ε or that (C3) is satisfied for $p+1-d'$ and $a_l/l^{d'}$. In case of a modular form of weight $p+1-d'$ there exists, by [6, Prop. 3.3], a modular form of weight $p+1+d'$ with eigenvalues a_l and character ε. We can conclude again by multiplying with the Hasse invariant if necessary (see [5, §3.1]) using the fact that we have $(N,p) \neq (1,2)$ or $(1,3)$ by induction hypothesis, and therefore $\mathcal{S}_k(N,\varepsilon)_F^{\mathrm{Katz}} = \mathcal{S}_k(N,\varepsilon)_F^{\mathrm{mod}}$ (see [6, Lemma 1.9] and §4.2). In the case (C3) is satisfied, we obtain integers $M, M' \geqslant 1$ such that $MM'|N$, integers i', j' such that $i'+j' \equiv p-d' \bmod p-1$, a finite extension F' of F, and Dirichlet characters $\varepsilon_1 : (\mathbb{Z}/M\mathbb{Z})^\times \to F'^\times$, $\varepsilon_2 : (\mathbb{Z}/M'\mathbb{Z})^\times \to F'^\times$, such that $\varepsilon_1\varepsilon_2 = \varepsilon$ and $\varepsilon_1(l)l^{i'} + \varepsilon_2(l)l^{j'} = a_l/l^{d'}$ for all primes $l \not| pN$. We conclude by taking the same $M, M', F', \varepsilon_1, \varepsilon_2$ and by $i = i'+d'$ and $j = j'+d'$. □

9.2. Conclusion.

Let F be a finite field of characteristic p, V a 2-dimensional vector space over F and $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$ a continuous representation. Assume that ρ is absolutely irreducible and odd. Let N, k, and $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to F^\times$ be the conductor, the weight and the character associated by Serre to ρ (see [14, §1, §2]).

We apply the results of §9.1, with $a_l = \mathrm{Tr}\ \rho(\mathrm{Frob}_l)$ for l a prime not dividing pN in order to prove the main theorem. Serre's conjecture in its strong modified form (see §4.2) for ρ is equivalent to condition (C2) of §9.1. Our main conjecture for ρ is equivalent to condition (C1) of §9.1. Condition (C3) would imply that, after extending scalars from F to F', ρ becomes a reducible representation, with semi-simplification isomorphic to $\varepsilon_1\chi_p^i \oplus \varepsilon_2\chi_p^j$, where $\chi_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ is the cyclotomic character. This cannot happen since ρ is assumed to be absolutely irreducible. The main theorem is therefore a consequence of Propositions 12 and 13.

10. Comments.

10.1. An example.

If the strong conjecture of Serre is stated with $\mathcal{S}_k(N,\varepsilon)_F$ instead of $\mathcal{S}_k^{\mathrm{mod}}(N,\varepsilon)_F$ this conjecture is false in characteristic 2 and 3 (see §4.2). Here is a counterexample due to Serre. We take $N=13, k=2$. Let χ be one of the two Dirichlet character mod 13 of order 6. One can check that the dimension of the space $\mathcal{S}_2(13,\chi)$ is equal to 1 (see formulas in [1]). Take g the unique normalized new form of level 13, weight 2 and character χ. Its coefficients lie in $\mathbb{Z}[\rho]$ where $\rho = e^{\pi i/3}$. Reduce it modulo the unique prime ideal of $\mathbb{Z}[\rho]$. One gets a Katz cuspform f of level 13, weight 2 and character ε, where $\varepsilon : (\mathbb{Z}/13\mathbb{Z})^\times \to \mathbb{F}_3^\times$ is the unique character of order 2. The representation ρ_f is absolutely irreducible and its associated triple is $(13,2,\varepsilon)$. However ρ_f does not satisfy the original strong form of Serre's conjecture since $\mathcal{S}_2(13,\varepsilon_0)=0$. One remarks that the character is the problem in this counterexample. However ρ_f does satisfy the conjecture in the modified setting (see §4.2).

Let us examine this example in our setting. We look for a map $\mu : C_{13} \to \mathbb{F}_3$ which factors through $L_2(13)$ and satisfies the conditions of the main conjecture. One remarks first that it suffices to determine $\mu((1,0))$ and $\mu((a,1))$ for $a \in \mathbb{Z}/13\mathbb{Z}$ because R_d acts as the character ε. Because of the relation induced from σ it suffices even to know $\mu((a,1))$ for $a \in \mathbb{Z}/13\mathbb{Z}$.

The reader might find it interesting to write down the relations induced by σ and τ. Remark that τ induces $3\mu((3,1)) = 3\mu((9,1)) = 0$. In Serre's original setting, this would imply that $\mu((3,1)) = \mu((9,1)) = 0$, however in our setting this is an empty condition. Furthermore, we can now write down the action of the Hecke operators (for small primes), diagonalize it and one search for a linear map μ which satisfies the conditions of the main conjecture.

We can define an involution c on C_{13} by $(a,b) \mapsto (a,-b)$. By calculation (by hand) one can find a unique (up to multiplication by an non zero element of $\mathbb{F}_3$) μ^+ (such that $\mu^+ \circ c = \mu^+$) and a μ^- (such that $\mu^- \circ c = -\mu^-$). We obtain

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\mu^+((x,1))$	0	0	0	1	2	2	0	0	1	1	2	0	0
$\mu^-((x,1))$	1	0	1	1	2	0	1	1	0	2	1	1	0

Remark that both $\mu^\pm((3,1))$ and $\mu^\pm((9,1))$ are different from zero.

10.2. General remarks.

One can define in general an involution c on $\mathbb{Z}[C_N] \otimes_{\mathbb{Z}} \mathbb{Z}[X,Y]_{k-2}$, given by $(u,v) \otimes P(X,Y) \mapsto (u,-v) \otimes P(-X,Y)$. By passing to the quotient this gives a complex conjugation c on $L_k(N)$. If there exists a $\mu : L_k(N) \to F$ as in the main conjecture, one can look for μ^+ and μ^- (such that $\mu^\pm \circ c = \pm\mu^\pm$). The unicity of μ^+ (resp. μ^-) up to multiplication by an element of $F^\times$ is an interesting question that we leave for further study.

Remark that $L_k(N)$ also contains information on Eisenstein series (see Theorem 7). Therefore one expects a similar description as the main conjecture for reducible representations, although not exactly the same as the mod 5 representation associated to $X_0(11)$ suggests (see [2, ex. 1]).

The advantages of the main conjecture (with regard to the one of Serre) is that one avoids the introduction of analytic objects (such as modular forms in characteristic 0), and extra choices (choosing a maximal ideal containing p in the ring of algebraic integers, and an embedding of F in its residue field) like in Serre's definition of a modular form in characteristic p, or the heavy algebraic geometric background needed to define Katz modular forms (although we do not give a description of the Katz' case when $k = 1$, see Remark §4.2). Also from a computational point of view, this conjecture is much more easier to test on computers than Serre's original one. Finally, it is our hope that the elements of F appearing in the main conjecture will have a nice Galois theoretic interpretation in terms of ρ.

BIBLIOGRAPHY

[1] H. Cohen, J. Oesterlé, Dimensions des espaces de formes modulaires, Lecture Notes in Mathematics 627, Springer-Verlag 1977, p. 69-78.

[2] H. Darmon, Serre's conjectures, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc. 17, p. 135-153.

[3] P. Deligne, J.-P. Serre, Formes modulaires de poids 1, Ann. Sci. E.N.S., vol. 7 (1974), 507-530.

[4] F. Diamond, J. Im, Modular forms and modular curves, Seminar on Fermat's Last Theorem, CMS conference proceedings 1995, p. 39-134.

[5] B. Edixhoven, The weight in Serre's conjectures on modular forms, Inventiones Mathematicae, vol. 109 (1992), 563-594.

[6] B. Edixhoven, Serre's conjecture, Modular Forms and Fermat's Last Theorem, Springer-Verlag 1997, p. 209-242.

[7] A. HERREMANS, A combinatorial interpretation of Serre's conjecture on modular Galois representations, Ph.D.thesis K.U.Leuven (28th May 2001).

[8] A. KNAPP, Elliptic Curves, Oxford University Press, 1992.

[9] J. MANIN, Parabolic Points and Zeta-Function of Modular Curves, Math. USSR Izvestija, vol. 6 (1972), p. 19-64.

[10] H. MATSUMURA, Commutative algebra, New York, W. A. Benjamin, 1970.

[11] F. MARTIN, Périodes de formes modulaires de poids 1, Thèse de doctorat Paris 7 (20 décembre 2001).

[12] L. MEREL, Universal Fourier expansions of modular forms, Lecture Notes in Mathematics 1585, Springer-Verlag 1994, p. 59-94.

[13] T. MIYAKE, Modular Forms, Springer-Verlag 1989.

[14] J.-P. SERRE, Sur les représentations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$), Duke Mathematical Journal, vol. 54, nr. 1 (1987), 179-230.

[15] J.-P. SERRE, Oeuvres, collected papers, vol. III: 1972–1984, Springer-Verlag 1986.

[16] G. SHIMURA, Introduction to the Arithmetic Theory of Automorphic Functions, Iwana Shoten Publishers and Princeton University Press 1971.

[17] V. SHOKUROV, Shimura integrals of cusp forms, Math. USSR Isvestija, vol. 16 (1981), 603-646.

Manuscrit reçu le 27 juin 2002,
accepté le 12 juin 2003.

Adriaan HERREMANS,
University of Utrecht
Department of Mathematics
PO Box 80010
NL-3508 Utrecht (The Netherlands).
herreman@math.uu.nl