COMPOSITIO MATHEMATICA

ELISABETH PAPIER

Représentations l-adiques

Compositio Mathematica, tome 71, n° 3 (1989), p. 303-362

<http://www.numdam.org/item?id=CM_1989__71_3_303_0>

© Foundation Compositio Mathematica, 1989, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http://http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Compositio Mathematica **71**: 303–362, 1989.
© 1989 *Kluwer Academic Publishers. Printed in the Netherlands.*

Représentations ℓ-adiques

ELISABETH PAPIER
Université de Paris– Sud, Centre d'Orsay Mathématique, Bâtiment 425, C.N.R.S., UA 7521, F-91405 Orsay Cedex, France.

Received 25 May 1986; accepted in revised form 4 January 1989

Introduction

Soit Δ la forme parabolique de poids 12 pour $SL(2, \mathbf{Z})$:

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

Pour tout nombre premier $p \neq 3$, le coefficient de Fourier $\tau(p)$ vérifie la congruence suivante:

$$\begin{cases} \tau(p) \equiv p^{621} + p^{848} \bmod 3^7 \text{ si } p \equiv -1 \bmod 3 \\ \tau(p) \equiv (p^{2079} + p^{2306})\left(1 + 5103 . \dfrac{v^2}{u^2}\right) \bmod 3^8 \text{ si } p \equiv 1 \bmod 3 \end{cases} \quad (*)$$

où u et v sont les entiers positifs définis par l'égalité: $4p = u^2 + 27v^2$.

Une des applications de cet article est de montrer que la congruence précédente est la meilleure possible en un sens qui sera précisé. Cette congruence est liée aux propriétés de la représentation 3-adique attachée à Δ:

$$\rho_{3,\Delta} : \mathrm{Gal}\left(\frac{\bar{\mathbf{Q}}}{\mathbf{Q}}\right) \to \mathrm{GL}(2, \mathbf{Z}_3)$$

continue et non ramifée en dehors de 3 et de l'infini. En particulier, l'image de $\rho_{3,\Delta}$ sera explicitement décrite.

Cette façon d'étudier de telles congruences a été développée par Serre et Swinnerton-Dyer. Par exemple, une version affaiblie de la congruence (*) est démontrée dans [4].

Dans [2], K. A. Ribet et moi généralisions les articles [3] et [4]. Mon but est de compléter les résultats de [2] et de les illustrer par des exemples provenant de formes paraboliques pour $SL(2, \mathbf{Z})$, certains de ces exemples ayant déjà été traités par Swinnerton-Dyer ([4]). Les méthodes employées ici s'inspirent beaucoup de [2], [3] et [4].

Je tiens à remercier particulièrement K. A. Ribet et J-P. Serre pour l'intêret qu'ils ont porté à ce travail et les remarques utiles qu'ils ont formulées.

1. Généralités

(1.1) Soit ℓ un nombre premier impair. Soient $\bar{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$ et $K_\ell \subset \bar{\mathbf{Q}}$ la plus grande extension de $\mathbf{Q}$ non ramifiée en tout nombre premier différent de ℓ, de groupe de Galois $G = \mathrm{Gal}(K_\ell/\mathbf{Q})$.

Soient $K_\ell^{ab} \subset K_\ell$ la plus grande extension abélienne de $\mathbf{Q}$ non ramifiée en dehors de ℓ et de l'infini et $H = \mathrm{Gal}(K_\ell/K_\ell^{ab})$. Soit χ_ℓ le caractère cyclotomique de G dans $\mathbf{Z}_\ell^*$, qui décrit l'action de G sur les racines de l'unité d'ordre une puissance de ℓ. On a la suite exacte suivante:

$$1 \to H \to G \xrightarrow{\chi_\ell} \mathbf{Z}_\ell^* \to 1. \tag{1}$$

Tout caractère continu de G dans un groupe abélien profini A est le composé de χ_ℓ et d'un caractère continu de $\mathbf{Z}_\ell^*$ dans A. Par abus, je noterai parfois de la même manière un caractère continu quelconque de $\mathbf{Z}_l^*$ dans A et le caractère de G obtenu en le composant avec χ_ℓ.

(1.2) Le but principal de cet article est de décrire, à conjugaison près, l'image des morphismes (ρ, χ_ℓ), ρ vérifiant les hypothèses (H.1), (H.2) et (H.3) suivantes:

(H.1) Soient E une extension finie de $\mathbf{Q}_\ell$ et O, λ et $\mathbf{F}$ respectivement l'anneau des entiers, l'idéal maximal et le corps résiduel de E.

Soit $\rho: G \to \mathrm{GL}(2, E)$ une représentation continue et irréductible.

Je note tr et det les fonctions trace et déterminant de ρ, à priori à valeurs dans E. En fait, comme G est compact, ρ est conjuguée dans $\mathrm{GL}(2, E)$ à une représentation à valeurs dans $\mathrm{GL}(2, O)$ et les fonctions tr et det sont à valeurs dans O.

Je suppose qu'il existe deux caractères distincts:

$$\mu, \nu: G \to \mathbf{F}^*$$

tels que, pour tout g dans G:

$$\mathrm{tr}(g) \equiv \mu(g) + \nu(g) \bmod \lambda. \tag{2}$$

La propriété (2) définit alors μ et ν à permutation près. Comme ℓ est impair, l'identité: $2.\det(g) = \mathrm{tr}(g)^2 - \mathrm{tr}(g^2)$, $\forall g \in G$ implique que ρ vérifie aussi:

$$\det \equiv \mu.\nu \bmod \lambda.$$

(H.2) La fonction det est à valeurs dans $\mathbf{Z}_\ell^*$.

(H.3) La représentation ρ vérifie: $(\mu/\nu)^2 = 1$.

(1.3) Dans [2], K. A. Ribet et moi décrivions $(\rho, \chi_\ell)(G)$ dans le cas où ρ vérifie des hypothèses un peu différentes, à savoir (H.1), (H.2) et l'hypothèse suivante:

(H.3. bis) (i) La représentation ρ vérifie: $(\mu/\nu)^2 \neq 1$, (ii) Soit $\mathbf{Q}[\boldsymbol{\mu}_\ell]^+$ le plus grand sous-corps totalement réel de $\mathbf{Q}[\boldsymbol{\mu}_\ell]$ où $\boldsymbol{\mu}_\ell$ est le groupe des racines ℓ-ièmes de l'unité. Soit h^+ le nombre de classes de $\mathbf{Q}[\boldsymbol{\mu}_\ell]^+$. Alors h^+ est premier à ℓ.

La conjecture de Vandiver affirme que l'hypothèse (ii) ci-dessus est toujours vraie. Cette conjecture a été vérifiée numériquement pour tout nombre premier $\ell < 125000$ et aucun contre-exemple n'est connu.

L'hypothèse (H.2) est due à des raisons techiques. On peut toujours se ramener au cas où elle est vérifiée comme je l'explique au point (1.6). En admettant que la conjecture de Vandiver soit vraie, les résultats de [2] et de cet article décrivent donc $(\rho, \chi_\ell)(G)$ pour toute représentation ρ vérifiant (H.1).

(1.4) Je fais encore quelques définitions:
Soit $\omega: \mathbf{Z}_\ell^* \to \mathbf{Z}_\ell^*$ le caractère de Teichmüller, défini par:

$$x \in \mathbf{Z}_\ell^* \to \omega(x) \in \mathbf{Z}_\ell^* \quad \text{tel que:}$$

$$\omega(x) \equiv x \bmod \ell, \quad \omega(x)^{(\ell-1)} = 1.$$

Je note $\langle x \rangle$ le quotient $x/\omega(x)$.

Le caractère ω fournit une décomposition de $\mathbf{Z}_\ell^*$ en produit direct:

$$\mathbf{Z}_\ell^* \xrightarrow{\sim} \boldsymbol{\mu}_{\ell-1} \times (1 + \ell\mathbf{Z}_\ell) \tag{3}$$

par: $x \to (\omega(x), \langle x \rangle)$.

Je note $\tilde{\omega}$ la réduction modulo ℓ:

$$\tilde{\omega}: \mathbf{Z}_\ell^* \to \mathbf{F}_\ell^*.$$

Restreint à $\boldsymbol{\mu}_{\ell-1}$, $\tilde{\omega}$ est un isomorphisme.

Le groupe multiplicatif $(1 + \ell\mathbf{Z}_\ell)$ est isomorphe à $\mathbf{Z}_\ell$.

(1.5) PROPOSITION. *Soit ρ une représentation vérifiant* (H.1). *Il existe alors deux éléments distincts m et n dans $\mathbf{Z}/(\ell-1)\mathbf{Z}$ tels que:*

$$\mu = \tilde{\omega}^m, \quad \nu = \tilde{\omega}^n.$$

Si ρ vérifie de plus (H.3) *alors: $m - n \equiv (\ell-1)/2 \bmod (\ell-1)$.*

DEMONSTRATION. Les caractères μ et ν se factorisent par χ_ℓ. On peut donc les considérer comme des caractères de $\mathbf{Z}_\ell^*$ dans $\mathbf{F}^*$. Pour des raisons de cardinalité, ces caractères sont tous des puissances de $\tilde{\omega}$. Par conséquent, il existe deux éléments m et n dans $\mathbf{Z}/(\ell - 1)\mathbf{Z}$ tels que:

$$\mu = \tilde{\omega}^m, \quad \nu = \tilde{\omega}^n.$$

Ils sont distincts car μ et ν le sont.

La conséquence de l'hypothèse (H.3) est évidente.

(1.6) PROPOSITION. *Soit ρ une représentation vérifiant* (H.1). *Il existe alors un caractère continu δ de G dans O^* tel que la représentation $\rho' = \delta^{-1} \otimes \rho$ vérifie* (H.1) *et* (H.2).

On connaît alors $(\rho, \chi_\ell)(G)$ dès qu'on connaît $(\rho', \chi_\ell)(G)$ puisque:

$$(\rho, \chi_\ell)(G) = \left\{(a, t) \in \frac{GL(2, E) \times \mathbf{Z}_\ell^*}{(\delta(t)^{-1}.a, t)} \in (\rho', \chi_\ell)(G)\right\}.$$

Si ρ vérifie (H.3) où (H.3.bis), il en est de même pour ρ'. Notons que, comme annoncé en (1.1), je considère aussi δ comme un caractère de $\mathbf{Z}_\ell^*$ dans O^*.

DEMONSTRATION. D'après (1.5), la représentation ρ vérifie la congruence suivante:

$$\det(g) \equiv \omega^{m+n}(g) \bmod \lambda, \quad \text{pour tout } g \text{ dans } G.$$

Comme ℓ est impair, il existe un caractère continu unique δ de G dans $(1 + \lambda)$ vérifiant:

$$\delta^2 = \omega^{-(n+m)}.\det.$$

La représentation: $\rho' = \delta^{-1} \otimes \rho$ a pour déterminant ω^{m+n}, à valeurs dans $\mathbf{Z}_\ell^*$.

Il est facile de voir que ρ' vérifie aussi les hypothèses (H.1).

(1.7) Par la suite, g_0 désignera un élément fixé de G tel que $\chi_\ell(g_0)$ engendre $\mathbf{Z}_\ell^*$. Soit G_0 l'adhérence dans G du groupe cyclique engendré par g_0. Par définition, on a: $\chi_\ell(G_0) = \mathbf{Z}_\ell^*$, ce qui implique la décomposition suivante:

$$G = G_0.H. \tag{4}$$

Je fixe aussi γ_0, élément de G_0 vérifiant:

$$\omega^{(\ell-1)/2}(\gamma_0) = -1, \quad \langle \gamma_0 \rangle = 1.$$

(1.8) Dans la section 2, je donne quelques renseignements sur G provenant de la théorie du corps de classes et que j'utiliserai ensuite.

La section 3 est un résumé des principaux résultats de [2], sans démonstration.

Les sections 4, 5 et 7 sont consacrées à la description de $(\rho, \chi_\ell)(G)$ dans le cas où ρ vérifie (H.1), (H.2) et (H.3).

La section 6 consiste en la démonstration d'un résultat auxiliaire qui sera utilisé à la section 7. La méthode de démonstration de ce résultat provient en premier lieu de B. Mazur.

Enfin, les sections 8 et 9 donnent des exemples numériques de représentations vérifiant (H.1), (H.2) et (H.3) ou (H.3.bis) et provenant de formes paraboliques pour $SL(2, \mathbf{Z})$ propres pour l'action des opérateurs de Hecke. Ces exemples utilisent soit les résultats de [2] soit ceux que je démontre ici.

(1.9) Pour tout nombre premier $p \neq \ell$, Frob(p) est une classe de conjugaison d'éléments de G. Par abus, je noterai Frob(p) n'importe quel élément de cette classe. La quantité tr(Frob(p)) est bien définie.

Par densité des éléments de Frobenius, connaître ρ(Frob(p)) pour tout $p \neq \ell$ équivaut à connaitre ρ. Les paragraphes 8 et 9 traitent de représentations dont on connaît surtout la trace sur les éléments de Frobenius. Ce fait explique pourquoi je m'intéresse à de tels éléments en (2.10) et (2.11) ainsi que la remarque suivante:

(1.10) Soit p_0 un nombre premier engendrant topologiquement $\mathbf{Z}_\ell^*$, l'élément $g_0 = \text{Frob}(p_0)$ possède les propriétés demandées en (1.7).

2. Un peu de théorie du corps de classes

Les point (2.1) à (2.6) nous seront utiles pour étudier les représentations ρ vérifiant l'hypothèse (H.3). Les points suivants concernent aussi les représentations vérifiant (H.3.bis). Les points (2.10) et (2.11) nous permettront de traiter les exemples numériques des sections 8 et 9.

(2.1) Soit $k = \mathbf{Q}[\sqrt{\pm\ell}]$ le sous-corps quadratique de $\mathbf{Q}[\mu_\ell]$. Soit G^+ le groupe suivant:

$$G^+ = \text{Gal}\left(\frac{K_\ell}{k}\right) = \text{Ker}(\omega^{(\ell-1)/2}).$$

Notons que, si ρ vérifie (H.1), (H.2) et (H.3), on a aussi:

$$G^+ = \text{Ker}(\mu/\nu).$$

Je note G^- le complémentaire de G^+ dans G:

$$G^- = \left\{ \frac{g \in G}{\omega^{(\ell-1)/2}(g) = -1} \right\} = g_0 . G^+ .$$

Je note aussi G_0^+ et G_0^- les intersections suivantes:

$$G_0^+ = G_0 \cap G^+, \quad G_0^- = G_0 \cap G^- .$$

La décomposition (3) implique:

$$G^+ = G_0^+ . H. \tag{4}$$

Soit $D(G^+)$ l'adhérence dans G du groupe dérivé de G^+, c'est à dire le plus petit sous-groupe fermé de G contenant les commutateurs $g.h.g^{-1}.h^{-1}$, g et h parcourant G^+. C'est un sous-groupe de H distingué dans G, le quotient $H/D(G^+)$ est abélien.

(2.2) Soit N l'union des extensions abéliennes finies de k dans K_ℓ de degré une puissance de ℓ. Le groupe de Galois $Y = \mathrm{Gal}(N/k)$ est un quotient de $G^+/D(G^+)$. La théorie du corps de classes fournit quelques renseignements sur Y.

Le fait principal et bien connu est que le nombre de classes de k est strictement inférieur à ℓ donc premier à ℓ.

INDICATION. Si $k = \mathbf{Q}[\sqrt{-\ell}]$, le nombre de classes de k est lié au nombre de résidus quadratiques de $\mathbf{F}_\ell^*$ compris entre 1 et $(\ell - 1)/2$. Si $k = Q\sqrt{\ell}]$, on montre que tout classe d'idéaux de k contient un idéal entier de norme inférieure à $\sqrt{\ell}/2$ et on conclut par des majorations simples.

Ce fait, qui ne figure pas dans l'hypothèse (H.3) puisqu'il est vérifié pour tout ℓ, est l'analogue de (H.3.bis.ii).

Le groupe de Galois Y est un $\mathbf{Z}_\ell$-module sur lequel G/G^+ agit par conjugaison. Comme $\mathbf{Z}_\ell[G/G^+]$-module, Y est la somme directe de deux sous-modules propres:

$$Y^+ = \left\{ \frac{y \in Y}{g.y = y, \quad \forall g \in \frac{G}{G^+}} \right\},$$

$$Y^- = \left\{ \frac{y \in Y}{g.y = y^{\omega(\ell-1)/2}(g), \quad \forall g \in \frac{G}{G^+}} \right\}.$$

Le nombre de classes de k étant premier à ℓ, la théorie du corps de classes implique que les deux $\mathbf{Z}_\ell$-modules Y^+ et Y^- sont en fait isomorphes à $\mathbf{Z}_\ell$.

Il est clair que Y^+ est le quotient de G^+ par $\mathrm{Ker}(\chi_\ell^{(\ell-1)/2})$. On a donc:

$$\chi_\ell^{(\ell-1)/2}: Y^+ \xrightarrow{\sim} (1 + \ell\mathbf{Z}_\ell).$$

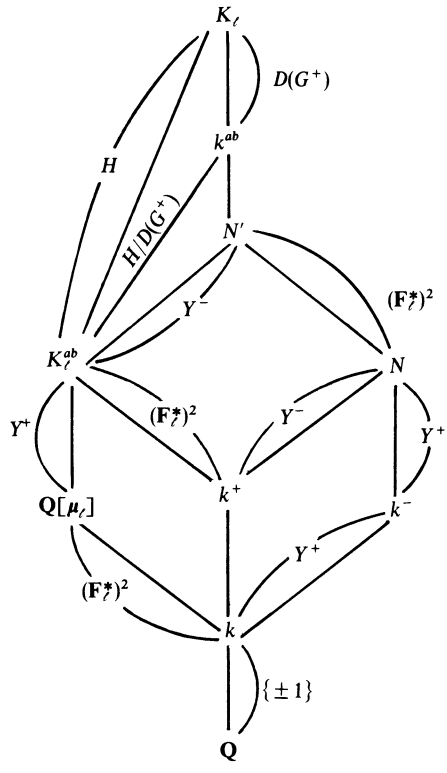
Soient N', k^+, k^- et k^{ab} les corps définis par:

- N' est le compositum $K_\ell^{ab}.N$,
- $Y^+ = \mathrm{Gal}(k^+/k)$, $Y^- = \mathrm{Gal}(k^-/k)$,
- $D(G^+) = \mathrm{Gal}(K_\ell/k^{ab})$.

Ainsi k^{ab} est la plus grande extension abélienne de k incluse dans K_ℓ, elle comprend N et K_ℓ^{ab}.
L'extension N est le compositum $k^+.k^-$ puisque:

$$\mathrm{Gal}\left(\frac{N}{k}\right) = Y = Y^+ \oplus Y^-.$$

On a le diagramme d'extensions suivant:



Il est facile de vérifier à partir de ce diagramme le résultat suivant:

(2.3) PROPOSITION. Le groupe $\mathrm{Gal}(N'/K_\ell^{ab})$ est isomorphe à $\mathbf{Z}_\ell$, l'action par conjugaison de $\mathrm{Gal}(K_\ell^{ab}/\mathbf{Q})$ sur $\mathrm{Gal}(N'/K_\ell^{ab})$ est donnée par le caractère $\omega^{(\ell-1)/2}$. Toute extension finie de K_ℓ^{ab} incluse dans k^{ab} et de degré une puissance de ℓ est incluse dans N'. Tout quotient fini de $H/D(G^+)$ d'ordre une puissance de ℓ est un quotient de $\mathrm{Gal}(N'/K_\ell^{ab})$.

(2.4) Soit h_* un élément de H engendrant le $\mathbf{Z}_\ell$-module $\mathrm{Gal}(N'/K_\ell^{ab})$. Tout quotient fini de $H/D(G^+)$ d'ordre une puissance de ℓ est donc engendré par l'image de h_* (ainsi que tout pro-ℓ-groupe quotient de $H/D(G^+)$).

Je note H_* l'adhérence dans G du groupe cyclique engendré par h_*. On a la décomposition suivante:

$$G = G_0 . H_* . \mathrm{Gal}(K_\ell/N'). \tag{5}$$

(2.5) Soit $\theta_*: \mathrm{Gal}(N'/K_\ell^{ab}) \to \mathbf{Z}_\ell$ le caractère continu vérifiant $\theta_*(h_*) = 1$. D'après le diagramme précédent, on peut considérer θ_* comme un caractère de $\mathrm{Gal}(N'/k)$ puis de G^+ car:

$$\mathrm{Gal}\left(\frac{N'}{k}\right) = Y^+ \oplus Y^- \oplus (\mathbf{F}_\ell^*)^2$$

Il vérifie: $\theta_*(G_0^+) = \{0\}$ car G_0^+ commute à g_0 et l'image de g_0 engendre $\mathrm{Gal}(k/\mathbf{Q})$. Le caractère θ_* vérifie aussi: $\theta_*(H_*) = \mathbf{Z}_\ell$ d'après le choix de h_*.

(2.6) Les caractères χ_ℓ et θ_* permettent d'expliciter la décomposition (5):

Soit g dans G. Il existe g' dans G_0 tel que $\chi_\ell(g) = \chi_\ell(g')$. Posons $h = g'^{-1}.g$. Comme g' est bien défini dans $G_0/G_0 \cap H$ et que θ_* est nul sur $G_0 \cap H$, sous-groupe de G_0^+, la quantité $\theta_*(h)$ est bien définie.

Soit h' dans H_* tel que $\theta_*(h') = \theta_*(h)$. Posons: $k = h'^{-1}.h$. Alors k est dans $\mathrm{Gal}(K_\ell/N')$ et on a: $g = g'.h'.k$.

C'est cette décomposition que j'utiliserai pour décrire les morphismes ρ vérifiant (H.1), (H.2) et (H.3). Je déterminerai $\rho(g_0)$, $\rho(h_*)$ et $\rho(\mathrm{Gal}(K_\ell/N'))$.

(2.7) Dans le cas où ρ vérifie (H.1), (H.2) et (H.3.bis), nous utilisions un résultat semblable.

Soit M l'union des extensions abéliennes finies de $\mathbf{Q}[\mu_\ell]$ dans K_ℓ de degré une puissance de ℓ. Le groupe $X = \mathrm{Gal}(M/\mathbf{Q}[\mu_\ell])$ est un $\mathbf{Z}_\ell$-module sur lequel $\Delta = \mathrm{Gal}(\mathbf{Q}[\mu_\ell]/\mathbf{Q})$ agit par conjugaison. Comme $\mathbf{Z}_\ell[\Delta]$-module, X est la somme directe des sous-modules propres $X(\varepsilon)$ suivants, ε parcourant l'ensemble des

caractères de Δ dans $\mathbf{Z}_\ell^*$:

$$X(\varepsilon) = \left\{ \frac{x \in X}{\delta . x} = \varepsilon(\delta)x, \quad \forall \delta \in \Delta \right\}.$$

Le caractère de Teichmüller ω de G dans $\mathbf{Z}_\ell^*$ a pour noyau $\mathrm{Gal}(K_\ell/\mathbf{Q}[\mu_\ell])$. Notons encore ω le caractère de Δ dans $\mathbf{Z}_\ell^*$ qui s'en déduit. Les différents caractères ε de Δ dans $\mathbf{Z}_\ell^*$ sont les puissances de ω, à exposants dans $\mathbf{Z}/(\ell - 1)\mathbf{Z}$.

(2.8) Soit h^+ le nombre de classes de $\mathbf{Q}[\mu_\ell]^+$. Il est essentiellement bien connu que, si h^+ est premier à ℓ, les différents $X(\varepsilon)$ sont des $\mathbf{Z}_\ell$-modules cycliques.

(2.9) Cas particulier:

$$\varepsilon = \omega^{(\ell-1)/2}$$

Soit k_ε l'extension de $\mathbf{Q}[\mu_\ell]$ définie par $X(\varepsilon) = \mathrm{Gal}(k_\varepsilon/\mathbf{Q}[\mu_\ell])$. Pour cette valeur particulière de ε on peut démontrer que k_ε est le compositum de k^- et $\mathbf{Q}[\mu_\ell]$, ce qui implique: $X(\varepsilon) = Y^-$. Le module $X(\omega^{(\ell-1)/2})$ est donc cyclique pour tout ℓ.

Soit g dans $\mathrm{Gal}(K_\ell/\mathbf{Q}[\mu_\ell]$ dont l'image dans $X(\omega^{(\ell-1)/2})$ engendre ce $\mathbf{Z}_\ell$-module. Soit g' dans G_0^+ vérifiant: $\chi_\ell(g') = \chi_\ell(g)$. Alors l'élément $h_* = g'^{-1}.g$ est dans H et engendre le quotient $\mathrm{Gal}(N'/K_\ell^{ab})$.

(2.10) Les résultats que j'expose ici sont démontrés dans [1]. Notons $F = \mathbf{Q}[\mu_\ell] = \mathbf{Q}[\zeta]$ où ζ est une racine ℓ-ième non triviale de l'unité. Pour tout caractère ε de Δ dans $\mathbf{Z}_\ell^*$, soit $x(\varepsilon)$ le quotient $X(\varepsilon)/\ell X(\varepsilon)$ et soit K_ε l'extension de F incluse dans k_ε définie par: $\mathrm{Gal}(K_\varepsilon/F) = x(\varepsilon)$.

Soit ε un caractère de Δ dans $\mathbf{Z}_\ell^*$ vérifiant:

$$\left(\frac{\varepsilon}{\omega}\right)^{(\ell-1)/2} = 1, \quad x(\varepsilon) = \frac{\mathbf{Z}}{\ell\mathbf{Z}}.$$

Soit alors u_ε un élément de F^* unité en dehors de ℓ et vérifiant:

$$u_\varepsilon \equiv \prod_{\sigma \in \Delta} \sigma(1-\zeta)^{(\varepsilon/\omega)(\sigma)} \bmod (F^*)^\ell.$$

L'extension $F[\sqrt[\ell]{u_\varepsilon}]$ est incluse dans M. L'action de Δ sur son groupe de Galois $\mathrm{Gal}(F[\sqrt[\ell]{u_\varepsilon}]/F)$ se fait par le caractère ε. Enfin ce groupe de Galois est isomorphe à $\mathbf{Z}/\ell\mathbf{Z}$. Il s'agit donc de $x(\varepsilon)$ et:

$$K_\varepsilon = F[\sqrt[\ell]{u_\varepsilon}].$$

Dans cette situation, soit p un nombre premier congru à 1 modulo ℓ, p est totalement décomposé dans F.
L'élément Frob(p) agit trivialement sur K_ε si et seulement si u_ε est une puissance ℓ-ième dans $\mathbf{F}_p^*$. Mais on sait que: $x(\varepsilon) = \mathbf{Z}/\ell\mathbf{Z}$. Donc l'image de Frob($p$) dans $x(\varepsilon)$ engendre $x(\varepsilon)$ si et seulement si Frob(p) n'agit pas trivialement sur K_ε.

(2.11) On en déduit le résultat suivant:

CRITÈRE. Soit ε un caractère de Δ dans $\mathbf{Z}_\ell^*$ vérifiant:

(i) $(\varepsilon/\omega)^{(\ell-1)/2} = 1$
(ii) $X(\varepsilon)$ est un $\mathbf{Z}_\ell$-module cyclique.

Soit u_ε un élément de F^*, unité en dehors de ℓ, tel que:

$$u_\varepsilon \equiv \prod_{\sigma\in\Delta} \sigma(1-\zeta)^{(\varepsilon/\omega)(\sigma)} \bmod (F^*)^\ell.$$

Soit p un nombre premier congru à 1 modulo ℓ.

L'image de Frob(p) dans $X(\varepsilon)$ est un générateur si et seulement si u_ε n'est pas une puissance ℓ-ième dans $\mathbf{F}_p^*$.

(2.12) REMARQUE. L'hypothèse (ii) du critère précédent est vérifiée dès que ε st égal à $\omega^{(\ell-1)/2}$ d'après (2.9). Elle est aussi vérifiée si h^+ est premier à ℓ, d'après (2.8).

3. Image de ρ dans le cas $(\mu/\nu)^2 \neq 1$

Ceci est le résumé des résultats principaux de [2]. Les points (3.1) à (3.5) seront redémontrés par la suite dans le cas où ρ vérifie les hypothèses (H.1), (H.2) et (H.3).

Je commence par supposer que ρ vérifie simplement (H.1).

(3.1) Soit $\mathbf{T}$ la $\mathbf{Z}_\ell$-sous-algèbre de O engendrée par les quantités tr(g), g parcourant G. L'algèbre $\mathbf{T}$ est une $\mathbf{Z}_\ell$-algèbre locale d'idéal maximal $\mathfrak{M} = \mathbf{T} \cap \lambda$. Le corps résiduel $\mathbf{T}/\mathfrak{M}$ est égal à $\mathbf{F}_\ell$.

(3.2) Soit g_0 l'élément de G défini en (1.7). Les caractères μ et ν étant distincts, la matrice $\rho(g_0)$ admet deux valeurs propres r et s distinctes qui sont dans $\mathbf{T}$ et vérifient:

$$r \equiv \mu(g_0), \quad s \equiv \nu(g_0) \bmod \mathfrak{M}.$$

Ces valeurs propres déterminent de façon unique deux caractères continus φ et

ψ de G dans $\mathbf{T}^*$ vérifiant:

$$\varphi(g_0) = r, \quad \psi(g_0) = s,$$

ce qui implique:

$$\varphi . \psi = \det$$
$$\varphi \equiv \mu, \quad \psi \equiv \nu \bmod \mathfrak{M}$$

ou encore: $\mathrm{tr} \equiv \varphi + \psi \bmod \mathfrak{M}$.

Les caractères φ et ψ dépendent du choix de g_0.

(3.3) Soit $\mathfrak{I}$ l'idéal de $\mathbf{T}$ engendré par les quantités $(\mathrm{tr} - \varphi - \psi)(g)$, g parcourant G. Il est clair que $\mathfrak{I}$ est inclus dans $\mathfrak{M}$. L'idéal $\mathfrak{I}$ n'est pas nul car ρ est irréductible. L'idéal $\mathfrak{I}$ ainsi que les caractères $\tilde{\varphi}, \tilde{\psi}: G \to (\mathbf{T}/\mathfrak{I})^*$ déduits de φ et ψ ne dépendent que de la classe d'isomorphisme de ρ.

(3.4) Soient m et n les deux éléments de $\mathbf{Z}/(\ell - 1)\mathbf{Z}$ définis en (1.5). Je suppose désormais que les deux $\mathbf{Z}_\ell$-modules $X(\omega^{m-n})$ et $X(\omega^{n-m})$ sont cycliques. Ceci est le cas si ρ vérifie (H.3) ou (H.3.bis).

Soit g_* un élément de $\mathrm{Gal}(K_\ell/\mathbf{Q}[\mu_\ell])$ dont les projections sur $X(\omega^{m-n})$ et $X(\omega^{n-m})$ engendrent ces deux $\mathbf{Z}_\ell$-modules. Alors $\mathfrak{I}$ est égal à $(\mathrm{tr} - \varphi - \psi)(g_*).\mathbf{T}$.

(3.5) L'idéal $\mathfrak{I}$ étant non nul et principal, il existe une représentation conjuguée de ρ (que je note encore ρ) vérifiant:

$$\rho(G) \subset GL(2, \mathbf{T})$$
$$\rho(g) = \begin{pmatrix} \varphi(g) & 0 \\ 0 & \psi(g) \end{pmatrix}, \text{ pour tout } g \text{ dans } G_0$$
$$\tilde{\rho}(g) = \begin{pmatrix} \tilde{\varphi}(g) & * \\ 0 & \tilde{\psi}(g) \end{pmatrix}, \text{ pour tout } g \text{ dans } G.$$

où $\sim$ désigne la réduction modulo $\mathfrak{I}$.

Comme G est égal à $G_0.H$, il nous reste à déterminer $\rho(H)$ pour connaître $(\rho, \chi_\ell)(G)$.

(3.6) THEOREME A. *Soit ρ vérifiant les hypothèses* (H.1), (H.2) *et* (H.3. bis) *et normalisée comme en* (3.5). *Alors:*

$$\rho(H) = \left\{ \begin{pmatrix} 1 + a & b \\ c & 1 + d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{T}) / a, c, d \in \mathfrak{I} \right\}$$

ou encore:

$$(\rho, \chi_\ell)(G) = \left\{ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, t \right) \in \mathrm{GL}(2, \mathbf{T}) \times \mathbf{Z}_\ell^* \;\middle/\; \begin{array}{l} ad - bc = \det(t) \\ a \equiv \tilde{\varphi}(t), \quad d \equiv \tilde{\psi}(t) \bmod \mathfrak{I} \\ c \in \mathfrak{I} \end{array} \right\}$$

où $\sim$ *désigne la réduction modulo* $\mathfrak{I}$.

COROLLAIRE A. *Soit* ρ *vérifiant* (H.1), (H.2) *et* (*H*.3. bis). *Alors:*

$$(\mathrm{tr}, \chi_\ell)(G) = \{(\tau, t) \in \mathbf{T} \times \mathbf{Z}_\ell^* / \tau \equiv \tilde{\varphi}(t) + \tilde{\psi}(t) \bmod \mathfrak{I}\},$$

où $\sim$ *désigne la réduction modulo* $\mathfrak{I}$.

(3.7) REMARQUE. Soit ρ vérifiant les hypothèses (H.1), (H.2) et (H.3. bis). Alors:

$$\mathbf{T} = \mathbf{Z}_\ell[\mathrm{tr}(g_0), \mathrm{tr}(g_*)].$$

Ce résultat ne figure pas dans [2]. Je démontrerai un résultat analogue dans la proposition (5.12), voir aussi la remarque (5.13).

Connaissant $\det(g_0)$, $\mathrm{tr}(g_0)$ et $\mathrm{tr}(g_*)$ on peut donc déterminer tous les paramètres intervenant dans le Théorème **A** et son corollaire.

4. Quelques objets attachés à ρ

Soit ρ une représentation vérifiant les hypothèses (H.1), (H.2) et (H.3).

(4.1) Soient $\mathbf{T}^+, \mathbf{T}^-$ et $\mathbf{T}$ les $\mathbf{Z}_\ell$-modules engendrés par les quantités $\mathrm{tr}(g), g$ parcourant respectivement G^+, G^- et G.

Les modules $\mathbf{T}^+, \mathbf{T}^-$ et $\mathbf{T}$ sont des sous-modules de O. Il est clair que $\mathbf{T}$ est égal à $\mathbf{T}^+ + \mathbf{T}^-$. Comme Id est dans G^+, on a aussi:

$$\mathbf{Z}_\ell \subset \mathbf{T}^+.$$

(4.2) PROPOSITION.

$\mathbf{T}^+$ *est une* $\mathbf{Z}_\ell$*-algèbre,*

$\mathbf{T}^-$ *est un* $\mathbf{T}^+$*-module,*

$(\mathbf{T}^-)^2$ *est inclus dans* $\mathbf{T}^+$,

$\mathbf{T}$ *est une* $\mathbf{Z}_\ell$*-algèbre.*

DEMONSTRATION. Ces faits découlent de l'identité suivante: $\mathrm{tr}(g)\mathrm{tr}(g') = \mathrm{tr}(gg') + \det(g).\mathrm{tr}(g^{-1}g')$, pour tous g, g' dans G, et du fait que det est à valeurs dans $\mathbf{Z}_\ell$.

(4.3) Il est clair que $\mathbf{T}$ et $\mathbf{T}^+$ sont des $\mathbf{Z}_\ell$-algèbres locales, d'idéaux maximaux respectifs: $\mathfrak{M} = \mathbf{T} \cap \lambda$ et $\mathfrak{M}^+ = \mathbf{T}^+ \cap \lambda = \mathbf{T}^+ \cap \mathfrak{M}$. Comme $\mathbf{Z}_\ell$-modules, $\mathbf{T}$ et $\mathbf{T}^+$ sont libres de rang fini donc complets et séparés par rapport à leurs topologies ℓ-adiques. Ces topologies coïncident respectivement avec les topologies $\mathfrak{M}$-adiques et $\mathfrak{M}^+$-adiques. On a donc:

$$\mathbf{T} \simeq \varprojlim \mathbf{T}/\mathfrak{M}^i$$
$$\mathbf{T}^+ \simeq \varprojlim \mathbf{T}^+/(\mathfrak{M}^+)^i,$$

ce qui permet d'appliquer le lemme de Hensel dans $\mathbf{T}^+$ et $\mathbf{T}$. Regardons les corps résiduels $\mathbf{T}/\mathfrak{M}$ et $\mathbf{T}^+/\mathfrak{M}^+$. D'après (H.1) et (1.5), la représentation ρ vérifie:

$\mathrm{tr}(g) \equiv \omega^m(g) + \omega^n(g) \bmod \mathfrak{M}$, pour tout g dans G, avec m et n dans $\mathbf{Z}/(\ell - 1)\mathbf{Z}$ tels que: $m - n = (\ell - 1)/2$.
Cette congruence implique:

$$\mathbf{T}^+/\mathfrak{M}^+ = \mathbf{T}/\mathfrak{M} = \mathbf{F}_\ell,$$
$$\mathbf{T}^- \subset \mathfrak{M}$$

(4.4) Soit g_0 l'élément de G défini en (1.7). Comme m et n sont distincts, le polynome $X^2 - \mathrm{tr}(g_0).X + \det(g_0)$ a deux racines distinctes dans $\mathbf{T}/\mathfrak{M}$, à savoir $\tilde{\omega}^m(g_0)$ et $\tilde{\omega}^n(g_0)$. D'après le lemme de Hensel, ce polynome admet donc deux racines distinctes r et s qui sont dans $\mathbf{T}$ et vérifient:

$$r \equiv \omega^m(g_0), \quad s \equiv \omega^n(g_0) \bmod \mathfrak{M}.$$

Les racines r et s déterminent de façon unique deux caractères continus φ et ψ de G dans $\mathbf{T}^*$ vérifiant:

$$\varphi(g_0) = r, \psi(g_0) = s.$$

La relation: $\varphi(g_0).\psi(g_0) = r.s = \det(g_0)$ implique: $\varphi.\psi = \det$. Les caractères φ et ψ vérifient aussi:

$$\varphi \equiv \omega^m, \quad \psi \equiv \omega^n \bmod \mathfrak{M},$$

ce qui implique: $\mathrm{tr} \equiv (\varphi + \psi) \bmod \mathfrak{M}$.

Je définis deux autres caractères de G:

$$\varphi' = \omega^{-m}.\varphi, \quad \psi' = \omega^{-n}.\psi.$$

Les caractères φ' et ψ' sont à valeurs dans $1 + \mathfrak{M}$.

(4.5) Quitte à remplacer ρ par une représentation conjuguée, je suppose désormais que ρ vérifie:

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

ce qui implique:

$$\rho(g) = \begin{pmatrix} \varphi(g) & 0 \\ 0 & \psi(g) \end{pmatrix}, \quad \text{pour tout } g \text{ dans } G_0. \tag{6}$$

Etant donné que $G = G_0.H$, il reste à déterminer $\rho(H)$ pour connaître $(\rho, \chi_\ell)(G)$.

En effet, d'après (6):

$$(\rho, \chi_\ell)(G) = \left\{ \left(\begin{pmatrix} \varphi(t) & 0 \\ 0 & \psi(t) \end{pmatrix}.h, t \right) \Big/ t \in \mathbf{Z}_\ell^*, \quad h \in \rho(H) \right\}.$$

(4.6) Le point (6) implique:

$$\mathrm{tr}(g) = \varphi(g) + \psi(g), \quad \text{pour tout } g \text{ dans } G_0.$$

Les caractères φ et ψ vérifient donc:

$$(\varphi + \psi)(g) \in \mathbf{T}^+ \quad \text{pour tout } g \text{ dans } G^+,$$
$$(\varphi + \psi)(g) \in \mathbf{T}^- \quad \text{pour tout } g \text{ dans } G^-,$$

ou encore:

$$(\varphi' + \psi')(g) \in \mathbf{T}^+ \quad \text{pour tout } g \text{ dans } G,$$
$$(\varphi' - \psi')(g) \in \mathbf{T}^- \quad \text{pour tout } g \text{ dans } G.$$

Ces assertions sont dues au fait qu'elles sont vraies pour les éléments de G_0 et que les caractères φ, ψ, φ' et ψ' se factorisent par χ_ℓ.

(4.7) Je définis la fonction η de G dans $\mathbf{T}$ par:

$$\eta(g) = \mathrm{tr}(g) - (\varphi + \psi)(g).$$

Soient $\mathfrak{I}^+, \mathfrak{I}^-$ et $\mathfrak{I}$ les $\mathbf{Z}_\ell$-modules engendrés par les quantités $\eta(g), g$ parcourant respectivement G^+, G^- et G.

Il est clair que $\mathfrak{I}$ est égal à $\mathfrak{I}^+ + \mathfrak{I}^-$.

D'après (4.6), on a les inclusions suivantes:

$$\mathfrak{I}^+ \subset \mathbf{T}^+, \mathfrak{I}^- \subset \mathbf{T}^-, \mathfrak{I} \subset \mathbf{T}.$$

La congruence: $\mathrm{tr}(g) \equiv (\varphi + \psi)(g) \bmod \mathfrak{M}$ pour tout g dans G implique: $\mathfrak{I}^+ \subset \mathfrak{M}^+, \mathfrak{I} \subset \mathfrak{M}$.

(4.8) PROPOSITION:

$\mathfrak{I}^+$ est un idéal de $\mathbf{T}^+$,

$\mathfrak{I}^-$ est un $\mathbf{T}^+$-sous-module de $\mathbf{T}^-$,

$\mathbf{T}^-.\mathfrak{I}^+$ est inclus dans $\mathfrak{I}^-$,

$\mathbf{T}^-.\mathfrak{I}^-$ est inclus dans $\mathfrak{I}^+$,

$\mathfrak{I}$ est un idéal de $\mathbf{T}$.

DEMONSTRATION. Soient g et g' dans G. Il existe alors h' dans G_0 vérifiant: $\chi_\ell(h') = \chi_\ell(g')$. On a l'identité suivante:

$$\mathrm{tr}(g)\eta(g') = (\eta(gg') - \eta(gh')) + \det(g).(\eta(g^{-1}g') - \eta(g^{-1}h')).$$

La proposition découle de cette formule et du fait que det est à valeurs dans $\mathbf{Z}_\ell$.

(4.9) A priori, $\mathfrak{I}^+, \mathfrak{I}^-$ et $\mathfrak{I}$ dépendent de φ et ψ, c'est à dire du choix de g_0. Ils ne dépendent en fait que de la classe d'isomorphisme de ρ comme l'implique la proposition suivante.

PROPOSITION. *Soient α et β deux caractères continus de G dans $\mathbf{T}^*$. Soit $\mathfrak{J}$ un $\mathbf{Z}_\ell$-sous-module de $\mathbf{T}$.*

(a) *Si α, β et $\mathfrak{J}$ vérifient:*

$$\mathfrak{J} \subset \mathbf{T}^+$$

$$\mathrm{tr}(g) - (\alpha + \beta)(g) \in \mathfrak{J} \quad \textit{pour tout } g \textit{ dans } G^+$$

alors $\mathfrak{I}^+$ *est inclus dans* $\mathfrak{J}$ *et* $(\varphi + \psi)(g) - (\alpha + \beta)(g)$ *est dans* $\mathfrak{J}$ *pour tout* g *dans* G^+.

(b) *Si* α, β *et* $\mathfrak{J}$ *vérifient:*

$$\mathfrak{J} \subset \mathbf{T}^-$$

$$\mathrm{tr}(g) - (\alpha + \beta)(g) \in \mathfrak{J} \quad \textit{pour tout } g \textit{ dans } G^-$$

alors $\mathfrak{I}^-$ *est inclus dans* $\mathfrak{J}$ *et* $(\varphi + \psi)(g) - (\alpha + \beta)(g)$ *est dans* $\mathfrak{J}$ *pour tout* g *dans* G^-.

(c) *Si* α, β *et* $\mathfrak{J}$ *vérifient:*

$\mathfrak{J}$ *est un idéal de* $\mathbf{T}$

$$\mathrm{tr}(g) \equiv (\alpha + \beta)(g) \bmod \mathfrak{J} \quad \textit{pour tout } g \textit{ dans } G$$

alors $\mathfrak{I}$ *est inclus dans* $\mathfrak{J}$ *et, à permutation près, on a:*

$$\alpha \equiv \varphi, \quad \beta \equiv \psi \bmod \mathfrak{J}.$$

DEMONSTRATION. Prenons le point (a). On a en particulier, d'après (6):

$(\varphi + \psi)(g) - (\alpha + \beta)(g) \in \mathfrak{J}$ pour tout g dans G_0^+, et ceci est aussi vrai pour tout g dans G^+ car les caractères φ, ψ, α et β se factorisent par χ_ℓ. On en déduit:

$$\eta(g) \in \mathfrak{J} \quad \text{pour tout } g \text{ dans } G^+,$$

ce qui implique que $\mathfrak{I}^+$ est inclus dans $\mathfrak{J}$.

La démonstration du point (b) est identique.

Dans le cadre de (c), les points (a) et (b) impliquent tout d'abord que $\mathfrak{I}^+$ est inclus dans $\mathfrak{J} \cap \mathbf{T}^+$ et $\mathfrak{I}^-$ est inclus dans $\mathfrak{J} \cap \mathbf{T}^-$ donc $\mathfrak{I}$ est inclus dans $\mathfrak{J}$. On sait aussi que:

$(\varphi + \psi)(g) \equiv (\alpha + \beta)(g) \bmod \mathfrak{J}$ pour tout g dans G. L'identité formelle: $2.\det(g) = \mathrm{tr}(g)^2 - \mathrm{tr}(g^2)$ implique alors:

$$\det(g) \equiv \alpha(g).\beta(g) \bmod \mathfrak{J} \quad \text{pour tout } g \text{ dans } G.$$

En appliquant ces deux congruences à g_0, on en déduit, à permutation près:

$$\alpha(g_0) \equiv r, \quad \beta(g_0) \equiv s \bmod \mathfrak{J},$$

car r et s sont distincts mod $\mathfrak{M}$. Comme les caractères φ, ψ, α et β se factorisent par χ_ℓ et que $\chi_\ell(g_0)$ engendre $\mathbf{Z}_\ell^*$, on obtient finalement:

$$\alpha \equiv \varphi, \quad \beta \equiv \psi \bmod \mathfrak{I}.$$

5. Détermination des $\mathbf{Z}_\ell$-modules attachés à ρ

Soit ρ vérifiant (H.1), (H.2) et (H.3) et normalisée de façon à vérifier (6).

Dans ce paragraphe, je vais normaliser ρ une fois encore. La représentation obtenue pourra ne plus être à valeurs dans $GL(2, E)$ c'est pourquoi je considère dès maintenant que les coefficients de ρ sont simplement dans $\bar{\mathbf{Q}}_\ell$.

(5.1) Soient a, b, c et d les fonctions de G dans $\bar{\mathbf{Q}}_\ell$ définies par:

$$\rho(g) = \begin{pmatrix} \varphi(g)(1 + a(g)) & \varphi(g)b(g) \\ \psi(g)c(g) & \psi(g)(1 + d(g)) \end{pmatrix}, \quad \text{pour tout } g \text{ dans } G. \tag{7}$$

D'après (4.5), la fonction $\left(\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right)$ est en fait une fonction de $G_0 \backslash G$ dans $\rho(H)$. Elle coïncide avec ρ sur H.

Etudions plus en détail les fonctions coefficients.

(5.2) PROPOSITION. *Les coefficients de ρ vérifient:*

(i) $(a + d)(g) \in \mathfrak{I}^+$, *pour tout g dans G,*
(ii) $(a - d)(g) \in \mathfrak{I}^-$, *pour tout g dans G,*
(iii) $b(g)c(h) + b(h)c(g) \in \mathfrak{I}^+$, *pour tous g, h dans G,*
(iv) $b(g)c(h) - b(h)c(g) \in \mathfrak{I}^-$, *pour tous g, h dans G.*

DEMONSTRATION. D'après (5.1), il suffit de prouver cette proposition pour les éléments de H puisque $G = G_0 . H$. Soit γ_0 l'élément défini en (1.7). Pour tout h dans H, on a:

$$\eta(h) = (a + d)(h), \quad \eta(\gamma_0 h) = \omega^n(\gamma_0)(a - d)(h).$$

Les points (i) et (ii) découlent donc de la définition de $\mathfrak{I}^+$ et $\mathfrak{I}^-$. Soient g et h deux éléments de H, alors:

$$(a + d)(gh) - (a + d)(g\gamma_0 h \gamma_0^{-1}) = 2[b(g)c(h) + b(h)c(g)]$$

$$(a - d)(gh) - (a - d)(g\gamma_0 h \gamma_0^{-1}) = 2[b(g)c(h) - b(h)c(g)]$$

Ces deux identités impliquent les points (iii) et (iv).

(5.3) Soit h_* un élément de H possédant les propriétés (2.4). D'après (2.3), le commutateur $h' = \gamma_0 h_* \gamma_0^{-1} h_*^{-1}$ est dans H et a même image que h_*^2 dans $\mathrm{Gal}(N'/K_\ell^{ab})$ donc engendre aussi ce $\mathbf{Z}_\ell$-module cyclique. Par ailleurs, il vérifie: $(a-d)(h') = 0$, ce qui permet de faire la définition suivante:

Désormais, h_* désigne un élément de H vérifiant (2.4) et:

$$(a-d)(h_*) = 0. \text{ Je pose: } x = b(h_*)c(h_*) = \left(\mathrm{tr}\frac{(h_*)}{2}\right)^2 - 1.$$

D'après (5.2.iii), x est un élément de $\mathfrak{I}^+$. On a aussi:

$a(h_*) = d(h_*) = \sqrt{1+x} - 1$, où $\sqrt{1+x}$ désigne la racine congrue à 1 modulo $\mathfrak{M}$.

Ceci implique que $a(h_*)$ et $d(h_*)$ sont dans $x.\mathbf{T}^+$.

(5.4) Les formules suivantes me seront utiles.

$$\text{Soient } h = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \text{ et } h' = \begin{pmatrix} 1+a' & b' \\ c' & 1+d' \end{pmatrix} \text{ dans } \rho(H).$$

Je note leur produit:

$$h.h' = \begin{pmatrix} 1+A & B \\ C & 1+D \end{pmatrix},$$

alors:

$$\text{(a) } A + D = \frac{(a+d)(a'+d')}{2} + \frac{(a-d)(a'-d')}{2} + (bc' + b'c) + (a+d) + (a'+d')$$

$$\text{(b) } A - D = \frac{(a+d)(a'-d')}{2} + \frac{(a-d)(a'+d')}{2} + (bc' - b'c) + (a-d) + (a'-d')$$

et pour toute paire (b_0, c_0) dans $\bar{\mathbf{Q}}_\ell$:

$$\text{(c) } b_0 C + c_0 B = (b_0 c + c_0 b) + (b_0 c' + c_0 b') + \frac{(b_0 c + c_0 b)(a'+d')}{2} + \frac{(b_0 c' + c_0 b')(a+d)}{2},$$

$$+\frac{(b_0c - c_0b)(a' - d')}{2} - \frac{(b_0c' - c_0b')(a - d)}{2}$$

La vérification de ces formules est laissée au lecteur.

(5.5) PROPOSITION. (i) *Pour tout couple (b_0, c_0) dans $(b,c)(H)$, la fonction $(b_0c - c_0b)$ induit un morphisme de H dans $\mathfrak{I}^-/\mathbf{T}^-.\mathfrak{I}^+$ stable par conjugaison par G^+.*

(ii) *Pour tout couple (h, h') d'éléments de H, la quantité $b(h)c(h') - b(h')c(h)$ est dans $\mathbf{T}^-.\mathfrak{I}^+$.*

DEMONSTRATION. D'après la formule (5.4.c) et le point (5.2), la fonction $(b_0c - c_0b)$ induit un morphisme de H dans $\mathfrak{I}^-/\mathfrak{I}^+.\mathfrak{I}^-$. Soient g dans G_0^+ et h dans H. Alors:

$$(b_0c - c_0b)(ghg^{-1}) = (b_0c - c_0b)(h) + \frac{(\varphi' - \psi')^2}{2\varphi'\psi'}(g).(b_0c - c_0b)(h)$$

$$+\frac{(\varphi' - \psi')(\varphi' + \psi')}{2\varphi'\psi'}(g).(b_0c + c_0b)(h),$$

ce qui, d'après (4.6), implique:

$$(b_0c - c_0b)(ghg^{-1}) \equiv (b_0c - c_0b)(h) \bmod \mathbf{T}^-.\mathfrak{I}^+.$$

On en déduit le point (i).

Le morphisme de H dans $\mathfrak{I}^-/\mathbf{T}^-.\mathfrak{I}^+$ obtenu a donc, d'après (2.4), comme image un $\mathbf{Z}_\ell$-module cyclique engendré par l'image de h_*. Prenons $(b_0, c_0) = (b, c)(h_*)$. Le morphisme associé à cette valeur est nul sur h_* donc trivial:

$$b(h_*)c(h) - b(h)c(h_*) \in \mathbf{T}^-.\mathfrak{I}^+, \quad \text{pour tout } h \text{ dans } H.$$

Par conséquent, pour toute valeur (b_0, c_0) dans $(b, c)(H)$, le morphisme associé est nul sur h_* donc trivial:

$$b(h)c(h') - b(h')c(h) \in \mathbf{T}^-.\mathfrak{I}^+, \quad \text{pour tout } h, h' \text{ dans } H.$$

(5.6) PROPOSITION. (i) *La fonction $(a - d)$ induit un morphisme de H dans $\mathfrak{I}^-/\mathbf{T}^-\mathfrak{I}^+$ stable par conjugaison par G^+.*

(ii) *Pour tout h dans H, $(a - d)(h)$ est dans $\mathbf{T}^-.\mathfrak{I}^+$.*

DEMONSTRATION. D'après (5.4.b), (5.5) et (5.2), la fonction $(a - d)$ induit un

morphisme de H dans $\mathfrak{I}^-/\mathbf{T}^-.\mathfrak{I}^+$. On a aussi:

$$(a-d)(ghg^{-1}) = (a-d)(h) \quad \text{pour tout } g \text{ dans } G_0^+ \text{ et tout } h \text{ dans } H.$$

Le point (i) est donc démontré.

La normalisation de h_* faite en (5.3) et le point (2.4) impliquent que ce morphisme de H dans $\mathfrak{I}^-/\mathbf{T}^-.\mathfrak{I}^+$ est nul, ce qui démontre le point (ii).

(5.7) PROPOSITION. $\mathfrak{I}^- = \mathbf{T}^-.\mathfrak{I}^+$.

DEMONSTRATION. $\mathfrak{I}^-$ est le $\mathbf{T}^+$-module engendré par les quantités $\eta(g)$, g parcourant G^-. Or, pour tout g dans G^-, on a la formule suivante:

$$\begin{aligned}\eta(g) &= \varphi(g)a(g) + \psi(g)d(g)\\ &= \omega^m(g)[(\varphi' + \psi')(g)(a-d)(g) + (\varphi' - \psi')(g)(a+d)(g)]/2.\end{aligned}$$

On a déjà remarqué en (5.1) que $(a-d)$ est en fait une fonction de $G_0\backslash G$. Comme G est égal à $G_0.H$, le point (5.6 (ii)) est encore vrai pour tout g dans G. La formule précédente implique donc:

$$\eta(g) \in \mathbf{T}^-.\mathfrak{I}^+, \quad \text{pour tout } g \text{ dans } G^-,$$

ou encore: $\mathfrak{I}^-$ est inclus dans $\mathbf{T}^-.\mathfrak{I}^+$.

L'inclusion inverse: $\mathbf{T}^-.\mathfrak{I}^+ \subset \mathfrak{I}^-$ a déjà été démontrée en (4.8)

(5.8) PROPOSITION. (i) *Pour tout couple* (b_0, c_0) *dans* $(b,c)(H)$, *la fonction* $(b_0c + c_0b)$ *induit un morphisme de* H *dans le quotient* $\mathfrak{I}^+/[(\mathbf{T}^-)^2.\mathfrak{I}^+ + (\mathfrak{I}^+)^2]$ *stable par conjugaison par* G^+.

(ii) *Pour tout couple* (h,h') *dans* H, *la quantité* $[b(h)c(h') + b(h')c(h)]$ *est dans* $x.\mathbf{T}^+ + (\mathbf{T}^-)^2.\mathfrak{I}^+ + (\mathfrak{I}^+)^2$.

La démonstration est analogue à celle de la proposition (5.5). La fonction $(b_0c + c_0b)$ induit un morphisme de H dans $\mathfrak{I}^+/(\mathfrak{I}^+)^2$. On a aussi:

$$(b_0c + c_0b)(ghg^{-1}) \equiv (b_0c + c_0b)(h) \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+,$$

pour tout g dans G_0^+ et tout h dans H.

Ceci démontre le point (i).

On en déduit d'abord, pour tout h dans H:

$$[b(h_*)c(h) + c(h_*)b(h)] \in (x.\mathbf{T}^+ + (\mathbf{T}^-)^2.\mathfrak{I}^+ + (\mathfrak{I}^+)^2),$$

puis le point (ii) en faisant varier (b_0, c_0) dans $(b,c)(H)$.

(5.9) PROPOSITION. (i) *La fonction* $(a + d)$ *induit un morphisme de* H *dans* $\mathfrak{I}^+/[x.\mathbf{T}^+ + (\mathbf{T}^-)^2.\mathfrak{I}^+(\mathfrak{I}^-))^2]$ *stable par conjugaison par* G^+.

(ii) *Pour tout* h *dans* H, $(a + d)(h)$ *est dans* $x.\mathbf{T}^+ + (\mathbf{T}^-)^2.\mathfrak{I}^+ + (\mathfrak{I}^+)^2$

DEMONSTRATION. Le point (i) se démontre de la même manière que précédemment. On a vu en (5.3) que $(a + d)(h_*)$ est dans $x.\mathbf{T}^+$, ce qui implique que le morphisme étudié est trivial. On en déduit le point (ii).

(5.10) PROPOSITION. $\mathfrak{I}^+ = x.\mathbf{T}^+$.

DEMONSTRATION: Pour tout g dans G^+, on a la formule suivante:

$$\eta(g) = \omega^m(g)[(\varphi' + \psi')(g)(a + d)(g) + (\varphi' - \psi')(\eta)(a - d)(g)]/2.$$

De la même façon qu'en (5.7), on en déduit:

$$\mathfrak{I}^+ = x.\mathbf{T}^+ + (\mathbf{T}^-)^2.\mathfrak{I}^+ + (\mathfrak{I}^+)^2.$$

Or l'idéal $[(\mathbf{T}^-)^2 + \mathfrak{I}^+]$ est inclus dans $\mathfrak{M}^+$. Le lemme de Nakayama implique finalement: $\mathfrak{I}^+ = x.\mathbf{T}^+$.

(5.11) On a donc identifié $\mathfrak{I}^+$ qui est égal à $x.\mathbf{T}^+$ et $\mathfrak{I}^-$ qui est égal à $\mathbf{T}^-.\mathfrak{I}^+$ ou encore $x.\mathbf{T}^-$. Par conséquent, $\mathfrak{I}$ est égal à $x.\mathbf{T}$ puisque:

$$\mathbf{T} = \mathbf{T}^+ + \mathbf{T}^-, \quad \mathfrak{I} = \mathfrak{I}^+ + \mathfrak{I}^-.$$

La représentation ρ n'étant pas réductible, $\mathfrak{I}$ n'est pas nul ainsi que x (voir la définition de $\mathfrak{I}$).

(5.12) Le but de la proposition suivante est de décrire les $\mathbf{Z}_\ell$-modules définis à la section 4 en fonction de $\mathrm{tr}(g_0)$ et x.

PROPOSITION.

(i) $\mathbf{T}^+ = \mathbf{Z}_\ell[\mathrm{tr}(g_0)^2, x]$

(ii) $\mathbf{T}^- = \mathrm{tr}(g_0).\mathbf{T}^+$

(iii) $\mathbf{T} = \mathbf{Z}_\ell[\mathrm{tr}(g_0), x]$

(iv) $\mathfrak{I}^+ = x.\mathbf{T}^+$

(v) $\mathfrak{I}^- = x.\mathbf{T}^-$

(vi) $\mathfrak{I} = x.\mathbf{T}$.

DEMONSTRATION. Les points (iv), (v) et (vi) ont déjà été vus en (5.11). Le point (iii) découle des points (i) et (ii) puisque: $\mathbf{T} = \mathbf{T}^+ + \mathbf{T}^-$.

Il nous reste à démontrer les points (i) et (ii).

D'après la définition de $\mathfrak{I}^-, \mathbf{T}^-$ est engendré comme $\mathbf{Z}_\ell$-module par $\mathfrak{I}^-$ et les quantités $(\varphi + \psi)(g)$, g parcourant G^- ou encore les quantités $(\varphi' - \psi')(g)$, g parcourant G. Or ces quantités sont des éléments de $\mathrm{tr}(g_0).\mathbf{T}^+$.

En effet, d'après la définition de g_0 et le fait que φ' et ψ' se factorisent par χ_ℓ, il suffit de démontrer que:

$$(\varphi' - \psi')(g_0^n) \in \mathrm{tr}(g_0).\mathbf{T}^+, \quad \text{pour tout } n \text{ dans } \mathbf{Z},$$

et en fait, il suffit de le démontrer pour tout $n \geqslant 1$.

Dans ce cas, on a la formule suivante:

$$(\varphi' - \psi')(g_0^n) = \tfrac{1}{2}(\varphi' - \psi')(g_0) \sum_{k=0}^{n-1} (\varphi' \cdot \psi')(g_0^k)(\varphi' + \psi')(g_0^{n-1-2k})$$

qui implique:

$$(\varphi' - \psi')(G) \subset (\varphi' - \psi')(g_0).\mathbf{T}^+.$$

On a aussi l'identité suivante:

$$\mathrm{tr}(g_0) = \omega^m(g_0)(\varphi' - \psi')(g_0).$$

On a donc démontré:

$$\mathbf{T}^- = \mathrm{tr}(g_0).\mathbf{T}^+ + x.\mathbf{T}^+.$$

Comme x est dans $\mathfrak{M}^+$, on peut appliquer le lemme de Nakayama pour obtenir finalement le point (ii).

D'après la définition de $\mathfrak{I}^+, \mathbf{T}^+$ est engendré comme $\mathbf{Z}_\ell$ — module par $\mathfrak{I}^+$ et les quantités $(\varphi + \psi)(g)$, g parcourant G^+ ou encore les quantités $(\varphi' + \psi')(g)$, g parcourant G. Démontrons que $(\varphi' + \psi')(G)$ est inclus dans $\mathbf{Z}_\ell + (\mathbf{T}^-)^2$.

Les caractères φ' et ψ', de G dans $(1 + \mathfrak{M})$, se factorisent par $\langle \chi_\ell \rangle$ qui a pour image $(1 + \ell \mathbf{Z}_\ell)$. Comme ℓ est impair, pour tout g dans G, il existe donc h dans G tel que:

$$\langle g \rangle = \langle h \rangle^2$$

ce qui implique:

$$\varphi'(g) = \varphi'(h)^2, \quad \psi'(g) = \psi'(h)^2$$

et:

$$(\varphi' + \psi')(g) = 2\varphi'\psi'(h) + (\varphi' - \psi')(h)^2.$$

Comme $\varphi'\psi'$ est à valeurs dans $\mathbf{Z}_\ell$, on a bien démontré que $(\varphi' + \psi')(G)$ est inclus dans $\mathbf{Z}_\ell + (\mathbf{T}^-)^2$, ou encore:

$$\begin{aligned}\mathbf{T}^+ &= \mathbf{Z}_\ell + (\mathbf{T}^-)^2 + \mathfrak{I}^+ \\ &= \mathbf{Z}_\ell + \mathrm{tr}(g_0)^2.\mathbf{T}^+ + x.\mathbf{T}^+ \\ &= \mathbf{Z}_\ell[\mathrm{tr}(g_0)^2, x] + \mathrm{tr}(g_0)^2.\mathbf{T}^+ + x.\mathbf{T}^+.\end{aligned}$$

Or l'idéal de $\mathbf{Z}_\ell[\mathrm{tr}(g_0, x]$ engendré par $\mathrm{tr}(g_0)^2$ et x est inclus dans son idéal maximal. D'après le lemme de Nakayama, on en déduit finalement:

$$\mathbf{T}^+ = \mathbf{Z}_\ell[\mathrm{tr}(g_0)^2, x].$$

La proposition est démontrée.

Connaissant $\mathrm{tr}(g_0)$ et $\mathrm{tr}(h_*)$, on peut donc déterminer tous les $\mathbf{Z}_\ell$-modules définis a la section 4 puisque $\mathrm{tr}(h_*)^2 = 4(1 + x)$. Remarquons que $\mathrm{tr}(g_0)$ et $\det(g_0)$ déterminent aussi les caractères φ et ψ. Tous les objets définis a la section 4 sont donc connus dès qu'on connaît $\mathrm{tr}(g_0)$, $\det(g_0)$ et $\mathrm{tr}(h_*)$.

(5.13) REMARQUE. Revenons au cadre de la section 3 où ρ vérifie les hypothèses (H.1), (H.2) et (H.3.bis). D'après (3.4), $\mathfrak{I}$ est égal à $(\mathrm{tr} - \varphi - \psi)(g_*).\mathbf{T}$ avec g_* défini de façon analogue à h_*. D'après la définition de $\mathfrak{I}$, $\mathbf{T}$ est engendré comme $\mathbf{Z}_\ell$-algèbre par $\mathfrak{I}$ et les quantités $(\varphi + \psi)(g)$, g parcourant G. Les caractères φ et ψ étant définis par le système:

$$\begin{cases}\varphi(g_0) + \psi(g_0) = \mathrm{tr}(g_0) \\ \varphi(g_0).\psi(g_0) = \det(g_0)\end{cases}$$

sont en fait à valeurs dans $\mathbf{Z}_\ell[\mathrm{tr}(g_0)]$. On en déduit:

$$\begin{aligned}\mathbf{T} &= \mathbf{Z}_\ell[\mathrm{tr}(g_0)] + \mathfrak{I} \\ &= \mathbf{Z}_\ell[\mathrm{tr}(g_0), \mathrm{tr}(g_*)] + (\mathrm{tr} - \varphi - \psi)(g_*).\mathbf{T}\end{aligned}$$

ou encore, d'après le lemme de Nakayama:

$$\mathbf{T} = \mathbf{Z}_\ell[\mathrm{tr}(g_0), \mathrm{tr}(g_*)],$$

ce qui était le résultat annoncé en (3.7).

(5.14) On a remarqué en (5.11) que x n'est pas nul. Je note $\sqrt{x}$ une des deux racines carrées de x dans $\bar{\mathbf{Q}}_\ell$.

La représentation ρ est déjà normalisée de façon à vérifier (6) et h_* a été choisi tel que:

$$\rho(h_*) = \begin{pmatrix} \sqrt{1+x} & b(h_*) \\ c(h_*) & \sqrt{1+x} \end{pmatrix},$$

avec

$$b(h_*)c(h_*) = x \quad \text{et} \quad \sqrt{1+x} \equiv 1 \bmod \mathfrak{I}^+.$$

Quitte à conjuger ρ une fois encore, je suppose désormais que ρ vérifie:

$$\begin{cases} \rho(g) = \begin{pmatrix} \varphi(g) & 0 \\ 0 & \psi(f) \end{pmatrix}, \text{ pour tout } g \text{ dans } G_0 \\ \rho(h_*) = \begin{pmatrix} \sqrt{1+x} & \sqrt{x} \\ \sqrt{x} & \sqrt{1+x} \end{pmatrix}. \end{cases} \tag{8}$$

Une fois fixés g_0, h_* et $\sqrt{x}$, cette normalisation est unique. La représentation ρ ainsi normalisée peut ne plus être à valeurs dans $GL(2,E)$. L'intérêt de cette normalisation est qu'elle conduit à une description de ρ en fonction de paramètres qui, eux, ne dépendront plus du choix de g_0 et h_*.

La représentation ρ étant ainsi normalisée, elle vérifie d'après (5.2) et les points suivants:

$$\rho(H) \subset \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \,\middle|\, \begin{matrix} a+d \in \mathfrak{I}^+, & a-d \in \mathfrak{I}^- \\ b+c\in\sqrt{x}.\mathbf{T}^+, & b-c\in\sqrt{x}.\mathbf{T}^- \end{matrix} \right\}$$

Ce groupe étant un pro-ℓ-groupe, on en déduit d'après (2.4):

$$\rho(H) = \rho(H_*) \cdot \rho(D(G^+))$$

ou encore:

$$\rho\left(\mathrm{Gal}\left(\frac{K_\ell}{N'}\right)\right) = \rho(D(G^+)).$$

Je vais d'abord étudier $\rho|_{H_*}$ puis déterminer (au §7) $\rho(D(G^+))$.

(5.15) J'introduis une loi de groupe $*$ sur $\sqrt{x}.\mathbf{T}^+$:

$$a*b = a.\sqrt{1+b^2} + b.\sqrt{1+a^2}$$

où les racines carrées sont prises dans $(1+\mathfrak{I}^+)$.

Cette loi $*$ correspond à la multiplication des matrices de la forme:

$$\begin{pmatrix} \sqrt{1+b^2} & b \\ b & \sqrt{1+b^2} \end{pmatrix}, \quad \text{avec } b \text{ dans } \sqrt{x}.\mathbf{T}^+ \quad \text{et} \quad \sqrt{1+b^2} \text{ dans } (1+\mathfrak{I}^+).$$

Il est facile de voir que $\sqrt{x}.\mathbf{T}^+$ muni de cette loi est bien un groupe abélien en même un $\mathbf{Z}_\ell$-module.

Je note donc $n*a = (\overset{a*\cdots*a}{n \text{ fois}})$ a pour a dans $\sqrt{x}.\mathbf{T}^+$ et n dans $\mathbf{Z}$.

(5.16) Soit θ_* le caractère de G^+ dans $\mathbf{Z}_\ell$ défini en (2.5) et qui vérifie: $\theta_*(h_*) = 1$. La définition de $*$ comme loi de $\mathbf{Z}_\ell$-module sur $\sqrt{x}.\mathbf{T}^+$ correspond à:

$$\rho(h_*)^n = \begin{pmatrix} \sqrt{1+y^2} & y \\ y & \sqrt{1+y^2} \end{pmatrix} \quad \text{avec } y = n*\sqrt{x}, \quad \text{pour tout } n \text{ dans } \mathbf{Z},$$

ce qui implique, par continuité de $*$ et θ_*:

$$\rho(h) = \begin{pmatrix} \sqrt{1+y^2} & y \\ y & \sqrt{1+y^2} \end{pmatrix} \quad \text{avec } y = \theta_*(h)*x, \text{ pour tout } h \text{ dans } H_*. \quad (9)$$

On connaît donc la représentation ρ restreinte à H_*. L'élément h_* étant fixé, la fonction:

$$f_*: h \in H \to \theta_*(h)*\sqrt{x} \in \sqrt{x}.\mathbf{T}^+$$

est définie au signe près, suivant le choix de $\sqrt{x}$. On peut remarquer que f_* (toujours au signe près) ne dépend que du groupe H_* et pas du générateur particulier h_* choisi.

(5.17) PROPOSITION: *La fonction* $(b+c)/2$ *induit un morphisme* f *de* H *dans* $\sqrt{x}.\mathbf{T}^+/\sqrt{x}.(\mathbf{T}^-)^2$. *Pour tout* h *dans* H, $f(h)$ *vérifie:*

$$f(h) \equiv \theta_*(h)*\sqrt{x} \bmod \sqrt{x}.(\mathbf{T}^-)^2$$

ou encore:

$$f \equiv f_* \bmod \sqrt{x}.(\mathbf{T}^-)^2.$$

$\rho(D(G^+))$ est inclus dans le groupe suivant:

$$\mathbf{X} = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \Big/ \begin{matrix} a+d \in (\mathbf{T}^-)^2.\mathfrak{I}^+, & a-d \in \mathfrak{I}^- \\ b+c \in \sqrt{x}.(\mathbf{T}^-)^2, & b-c \in \sqrt{x}.\mathbf{T}^- \end{matrix} \right\}.$$

DEMONSTRATION.

$$\text{Soit } \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \text{ dans } \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell),$$

alors la relation det = 1 peut se réécrire:

$$\left(1 + \frac{a+d}{2}\right)^2 = 1 + \left(\frac{a-d}{2}\right)^2 + \left(\frac{b+c}{2}\right)^2 - \left(\frac{b-c}{2}\right)^2.$$

Les éléments de $\rho(H)$ vérifient donc:

$$\left(1 + \frac{a+d}{2}\right) \equiv \sqrt{1 + \left(\frac{b+c}{2}\right)^2} \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+,$$

où la racine est choisie congrue à 1 modulo $\mathfrak{I}^+$.

$$\text{Soient } \rho(h) = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \text{ et } \rho(h') = \begin{pmatrix} 1+a' & b' \\ c' & 1+d' \end{pmatrix}$$

deux éléments de $\rho(H)$. Le produit

$$\rho(h.h') = \begin{pmatrix} 1+A & B \\ C & 1+D \end{pmatrix}$$

vérifie:

$$(B+C) = (b+c)\left(1 + \frac{a'+d'}{2}\right) + (b'+c')\left(1 + \frac{a+d}{2}\right) + \frac{(b-c)(d'-a')}{2}$$

$$+ \frac{(b'-c')(a-d)}{2},$$

ou encore, d'après ce qui précède:

$$\frac{B+C}{2} \equiv \frac{b+c}{2} * \frac{b'+c'}{2} \bmod \sqrt{x}.(\mathbf{T}^-)^2.\mathfrak{I}^+.$$

Soient g dans G_0^+ et h dans H. Alors:

$$\frac{b+c}{2}(ghg^{-1}) = \frac{b+c}{2}(h) + \frac{(\varphi'-\psi')^2}{2\varphi'\psi'}(g).\frac{b+c}{2}(h)$$
$$+ \frac{(\varphi'-\psi')(\varphi'+\psi')}{2\varphi'\psi'}(g).\frac{b-c}{2}(h).$$

Ceci implique que $b + c/2$ induit un morphisme f de H dans $\sqrt{x}.\mathbf{T}^+\sqrt{x}.(\mathbf{T}^-)^2$ stable par conjugaison par G^+. D'après (2.4) et (2.5), ce morphisme se factorise par θ_*. On a donc:

$$f(h) \equiv \theta_*(h) * \sqrt{x} \bmod \sqrt{x}.(\mathbf{T}^-)^2, \quad \text{pour tout } h \text{ dans } H$$

puisque:

$$f(h_*) \equiv \sqrt{x} \bmod \sqrt{x}.(\mathbf{T}^-)^2.$$

Le morphisme f est nul sur $D(G^+)$. Les éléments de $\rho(D(G^+))$ vérifient donc:

$$b + c \in \sqrt{x}.(\mathbf{T}^-)^2$$

puis:

$$\left(\frac{1+(a+d)}{2}\right) \equiv 1 \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+,$$

c'est à dire que $\rho(D(G^+))$ est inclus dans X.
Il est facile de voir que X est un groupe, je le démontrerai d'ailleurs à la section 6. Le but principal des sections 6 et 7 sera de démontrer que $\rho(D(G^+))$ est égal à X.

(5.18) Soit X le sous-groupe fermé de $\sqrt{x}.\mathbf{T}^+$ pour la loi $*$ engendré par $\sqrt{x}$ et $\sqrt{x}.(\mathbf{T}^-)^2$. Soit $\tilde{X} = X/\sqrt{x}.(\mathbf{T}^-)^2$.

La normalisation de ρ efffectuée en (8) dépend du choix de la paire (g_0, h_*) et de la constante $\sqrt{x}$ au signe près. A priori, il en est de même pour X, $\tilde{X}$ et le morphisme $f: H \to \tilde{X}$ défini en (5.16). En fait, il n'en est rien.

(5.19) PROPOSITION. *Les groupes X et $\tilde{X}$ sont canoniques ainsi que le morphisme $f: H \to \tilde{X}$ (au signe près).*

DEMONSTRATION: Soit h un élément de H vérifiant (2.4). La quantité $\theta_*(h)$ est donc dans $\mathbf{Z}_\ell^*$. Soit $y = (\mathrm{tr}(h)/2)^2 - 1$. On a la congruence suivante:

$$y \equiv f(h)^2 \bmod (\mathbf{T}^-)^2 . \mathfrak{I}^+$$

puisque: $\det(h) = 1$.
On a aussi:

$$f(h) \equiv \theta_* h) * \sqrt{x} \bmod \sqrt{x} . (\mathbf{T}^-)^2$$

d'où:

$$f(h) \equiv \theta_*(h) . \sqrt{x} \bmod \sqrt{x} . \mathfrak{M}^+$$

et:

$$y \equiv x . \theta_*(h)^2 \bmod \mathfrak{M}^+ . \mathfrak{I}^+,$$

ce qui implique que y/x est un carré dans $(\mathbf{T}^+)^*$ donc:

$$\sqrt{y} . \mathbf{T}^+ = \sqrt{x} . \mathbf{T}^+ .$$

Le $\mathbf{T}^+$-module $\sqrt{x} . \mathbf{T}^+$ est donc canonique, il est égal à $\sqrt{((\mathrm{tr}(h)/2)^2 - 1)} . \mathbf{T}^+$ pour tout h vérifiant (2.4).

Par conséquent $\sqrt{x} . (\mathbf{T}^-)^2$ est aussi canonique.

Soient (g', h') une autre paire possédant les propriétés voulues et $f': H \to \sqrt{x} . \mathbf{T}^+ / \sqrt{x} . (\mathbf{T}^-)^2$, le morphisme qu'elle définit. La relation:

$(\mathrm{tr}(h/2)^2 - 1) \equiv f(h)^2 \equiv f'(h)^2 \bmod (\mathbf{T}^-)^2 . \mathfrak{I}^+$, pour tout h dans H implique que:

$$f'(h_*) = \varepsilon f(h_*) \quad \text{avec} \quad \varepsilon = \pm 1$$

et, comme f' et f se factorisent par θ_*: $f' = \varepsilon f$.

Le morphisme f est donc canonique, au signe près, ainsi que son image qui est $\tilde{X}$. Comme $\tilde{X}$ et $\sqrt{x} . (\mathbf{T}^-)^2$ sont canoniques, X l'est aussi.

(5.20) Si A est un $\mathbf{T}^+$-module, je noterai $X . A$ le $\mathbf{T}^+$-module $\sqrt{x} . A$, qui est canonique dès que A l'est (par exemple $X . \mathbf{T}^+$ désigne $\sqrt{x} . \mathbf{T}^+$).

(5.21) REMARQUE. Le morphisme f est défini sur H. En fait, d'après (5.1), on peut considérer f comme une fonction de $G_0^+\backslash G^+$ dans $\tilde{X}$. Or f est nulle sur $\mathrm{Gal}(K_\ell/N')$ et $G_0^+ . \mathrm{Gal}(K_\ell/N')$ est le groupe $\mathrm{Ker}(\theta_*)$, distingué dans G^+. Ceci signifie que f est naturellement un morphisme de G^+ dans $\tilde{X}$, canonique au signe près. La formule: $f(g) \equiv \theta_*(g) * \sqrt{x} \bmod X.(\mathbf{T}^-)^2$ est encore valable pour tout g dans G^+.

(5.22) Le fait que f soit canonique (au signe près) a une conséquence importante:

PROPOSITION. *La fonction:* $\widetilde{(\varphi+\psi)}: G^+ \to \mathbf{T}^+/(\mathbf{T}^-)^2.\mathfrak{I}^+$, *réduction de* $(\varphi+\psi)$, *est canonique.*

On a déjà vu en (4.9) que la fonction $(\varphi+\psi)$ induit deux fonctions canoniques de G^+ dans $\mathbf{T}^+/\mathfrak{I}^+$ et de G^- dans $\mathbf{T}^-/\mathfrak{I}^-$.

DEMONSTRATION. Soit g dans G^+, on a la formule suivante:

$$\mathrm{tr}(g) = (\varphi+\psi)(g)\left(1+\frac{a+d}{2}\right)(g) + (\varphi-\psi)(g)(a-d)(g)/2,$$

d'où:

$$\mathrm{tr}(g) \equiv (\varphi+\psi)(g).\sqrt{1+\left(\frac{b+c}{2}\right)^2}(g) \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+,$$

ou encore, d'après la remarque (5.21):

$$\mathrm{tr}(g) \equiv (\varphi+\psi)(g).\sqrt{1+f(g)^2} \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+.$$

Comme tr et f^2 sont canoniques, il en est de même pour:

$$\widetilde{(\varphi+\psi)}: G^+ \to \mathbf{T}^+/(\mathbf{T}^-)^2.\mathfrak{I}^+.$$

6. À propos de groupes de matrices

(6.1) Soient X et Y les ensembles suivants:

$$\mathrm{X} = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in SL(2, \bar{\mathbf{Q}}_\ell) \,\middle/\, \begin{matrix} a+d \in \mathbf{T}^-.\mathfrak{I}^-, & a-d \in \mathfrak{I}^- \\ b+c \in X.(\mathbf{T}^-)^2, & b-c \in X.\mathbf{T}^- \end{matrix} \right\}$$

$$\mathrm{Y} = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in SL(2, \bar{\mathbf{Q}}_\ell) \,\middle/\, \begin{matrix} a+d \in \mathbf{T}^-.\mathfrak{I}^-, & a-d \in (\mathbf{T}^-)^2.\mathfrak{I}^- \\ b+c \in X.\mathbf{T}^-.\mathfrak{I}^-, & b-c \in X.(\mathbf{T}^-)^2.\mathfrak{I}^- \end{matrix} \right\}$$

THEOREME. (i) X *et* Y *sont des sous-groupes de* $\mathrm{SL}(2, \bar{\mathbf{Q}}_\ell)$. Y *est l'adhérence du groupe dérivé de* X. *La fonction* $(a-d, b+c, b-c)$ *induit un isomorphisme:*

$$\frac{\mathrm{X}}{\mathrm{Y}} \xrightarrow{\sim} \frac{\mathfrak{I}^-}{(\mathbf{T}^-)^2.\mathfrak{I}^-} \times \frac{X.(\mathbf{T}^-)^2}{X.(\mathbf{T}^-)^2.\mathfrak{I}^+} \times \frac{X.\mathbf{T}^-}{X.(\mathbf{T}^-)^2.\mathfrak{I}^-}$$

(ii) *Soit* G *un sous-groupe fermé d* X *tel que* $\mathrm{X} = \mathrm{G}.\mathrm{Y}$. *Alors* G *est égal à* X.

Il est facile de voir que ce résultat n'est qu'un cas particulier du Théorème (6.3) suivant:

(6.2) Soient A^-, B^+ et B^- des $\mathbf{T}^+$-sous-modules de $\bar{\mathbf{Q}}_\ell$ vérifiant:

$$(A^-)^3 \subset B^+.B^- \subset A^- \subset \mathbf{T}^-,$$
$$(B^+)^3 \subset A^-.B^- \subset B^+ \subset \underline{X}.\mathbf{T}^+,$$
$$(B^-)^3 \subset A^-.B^+ \subset B^- \subset \underline{X}.\mathbf{T}^-.$$

Je pose:

$$A^+ = (A^-)^2 + (B^+)^2 + (B^-)^2.$$

Ainsi A^+ est un idéal de $\mathbf{T}^+$.

Soient X et Y les ensembles suivants:

$$\mathrm{X} = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \,\middle/\, \begin{matrix} a+d \in A^+, & a-d \in A^- \\ b+c \in B^+, & b-c \in B^- \end{matrix} \right\},$$

$$\mathrm{Y} = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \,\middle/\, \begin{matrix} a+d \in A^+, & a-d \in B^+.B^- \\ b+c \in A^-.B^-, & b-c \in A^-.B^- \end{matrix} \right\}.$$

(6.3) THEOREME. *Sous les hypothèses* (6.2), X *et* Y *sont des sous-groupes de* $\mathrm{SL}(2, \bar{\mathbf{Q}}_\ell)$, Y *est l'adhérence du groupe dérivé de* X. *La fonction:* $(a-d, b+c, b-c)$ *induit un isomorphisme:*

$$\frac{\mathrm{X}}{\mathrm{Y}} \xrightarrow{\sim} \frac{A^-}{B^+.B^-} \times \frac{B^+}{A^-.B^-} \times \frac{B^-}{A^-.B^+}.$$

Soit G *un sous-groupe fermé de* X *tel que:* $\mathrm{X} = \mathrm{G}.\mathrm{Y}$. *Alors* G *est égal à* X.

Je démontrerai le théorème (6.3) en plusieurs étapes. Commençons par quelques définitions supplémentaires.

(6.4) Soient $(A_n^-)_{n\geqslant 1}$, $(B_n^+)_{n\geqslant 1}$ et $(B_n^-)_{n\geqslant 1}$ les $\mathbf{T}^+$-sous-modules de $\bar{\mathbf{Q}}_\ell$ suivants:

$$A_1^- = A^-, \quad B_1^+ = B^+, \quad B_1^- = B^-,$$

et, pour tout $n \geqslant 1$:

$$A_{n+1}^- = B_1^+ . B_n^- + B_1^- . B_n^+,$$
$$B_{n+1}^+ = A_1^- . B_n^- + A_n^- . B_1^-,$$
$$B_{n+1}^- = A_1^- . B_n^+ + A_n^- . B_1^+.$$

Soient

$$L = \left\{ u \in \frac{\mathrm{M}(2, \bar{\mathbf{Q}}_\ell)}{\mathrm{tr}(u)} = 0 \right\}$$

et $\theta : \mathrm{M}(2, \bar{\mathbf{Q}}_\ell) \to L$ défini par $\theta(u) = u - \mathrm{tr}(u)/2.\mathrm{Id}$. Je définis encore pour tout $n \geqslant 1$:

$$L_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \frac{L}{a-d} \in A_n^-, \quad b + c \in B_n^+, \quad b - c \in B_n^- \right\}$$

$$H_n = \left\{ (1+u) \in \frac{\mathrm{SL}(2, \bar{\mathbf{Q}}_\ell)}{\mathrm{tr}(u)} \in A^+, \theta(u) \in L_n \right\}$$

(6.5) Les propriétés suivantes sont évidentes:
Pour tout $n \geqslant 1$, A_n^-, B_n^+ et B_n^- sont des $\mathbf{T}^+$-sous-modules de $\bar{\mathbf{Q}}_\ell$, ils vérifient:

$$A_n^- \subset \mathbf{T}^-, \quad B_n^+ \subset X.\mathbf{T}^+, \quad B_n^- \subset X.\mathbf{T}^-.$$

Les différents $L_n, n \geqslant 1$, et L sont des sous-groupes de $\mathrm{M}(2, \bar{\mathbf{Q}}_\ell)$. θ est un morphisme surjectif.

On a aussi les égalités suivantes:

$$H_1 = \mathrm{X}, \quad H_2 = \mathrm{Y}.$$

(6.6) L'hypothèse (6.2) implique que L_2 est inclus dans L_1. D'après la définition par récurrence des modules A_n^-, B_n^+ et B_n^- pour tout $n \geqslant 1$, on voit facilement que, pour tout entier $n \geqslant 1$, l'inclusion: $L_{n+1} \subset L_n$ implique: $L_{n+2} \subset L_{n+1}$. La proposition suivante est alors évidente.

PROPOSITION. *Les $(L_n)_{n\geqslant 1}$ forment une suite décroissante de sous-groupes de*

$\mathrm{M}(2, \bar{\mathbf{Q}}_\ell)$. *Pour tout* $n \geqslant 1$, *la fonction* $(a - d, b + c, b - c)$ *induit un isomorphisme:*

$$\psi_n : L_n/L_{n+1} \xrightarrow{\sim} A_n^-/A_{n+1}^- \times B_n^+/B_{n+1}^+ \times B_n^-/B_{n+1}^-.$$

Par conséquent, les différents $(H_n)_{n \geqslant 1}$ *forment une suite décroissante de sous-ensembles de* $\mathrm{SL}(2, \bar{\mathbf{Q}}_\ell)$.

Je note, pour tout $n \geqslant 1$, φ_n le morphisme canonique suivant:

$$\varphi_n : L_n \to L_n/L_{n+1}.$$

(6.7) Les formules suivantes résultent d'un petit calcul laissé au lecteur:

LEMME:

Soient $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $v = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ *deux éléments de* L.

Posons $uv = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. *Alors:*

$$2(A + D) = (a - d)(a' - d') + (b + c)(b' + c') - (b - c)(b' - c'),$$
$$2(A - D) = (b - c)(b' + c') - (b + c)(b' - c'),$$
$$2(B + C) = (b' - c')(a - d) - (b - c)(a' - d'),$$
$$2(B - C) = (b + c)(a' - d') - (b' + c')(a - d).$$

On a aussi la relation suivante: $\theta(uv + vu) = 0$.

Ces formules permettent de démontrer le point suivant:

(6.8) LEMME:

(a) *Soient* u *et* v *dans* L_1, *alors* $\mathrm{tr}(uv)$ *est dans* A^+.

(b) *Soit* $n \geqslant 1$ *quelconque, soient* u *dans* $\mathrm{M}(2, \bar{\mathbf{Q}}_\ell)$ *et* v *dans* L_n. *Alors:*
   (i) *Si* u *est dans* L_1, $\theta(uv)$ *et* $\theta(vu)$ *sont dans* L_{n+1}.
   (ii) *Si* u *est dans* L_2, $\theta(uv)$ *et* $\theta(vu)$ *sont dans* L_{n+2}.
   (iii) *Si* u *est de la forme* $a.Id$ *avec* a *dans* A^+, uv *est dans* L_{n+1} *(et est égal à* vu*).*

DEMONSTRATION. Utilisons (6.7). Le point (a) découle de l'identité

$$A^+ = (A^-)^2 + (B^+)^2 + (B^-)^2.$$

Le point (b) (i) résulte de la définition par récurrence des modules

$$A_{n+1}^-, B_{n+1}^+ \text{ et } B_{n+1}^-.$$

Le point ((b)(ii)) est équivalent au système suivant:

$$\begin{cases} B_2^+ . B_n^- + B_2^- . B_n^+ \subset A_{n+2}^-, \\ B_2^- . A_n^- + B_n^- . A_2^- \subset B_{n+2}^+, \\ B_2^+ . A_n^- + B_n^+ . A_2^- \subset B_{n+2}^-. \end{cases}$$

En exprimant d'une part les modules d'indice $(n+2)$ en fonction des modules d'indice n et de A^-, B^+ et B^- et d'autre part les modules d'indice 2 en fonction de A^-, B^+ et B^-, on constate que ce système d'inclusions est vérifié pour tout $n \geqslant 1$. L'assertion ((b)(iii)) est équivalente au système suivant:

$$(S_n) \begin{cases} A^+ . A_n^- \subset A_{n+1}^- \\ A^+ . B_n^+ \subset B_{n+1}^+ \\ A^+ . B_n^- \subset B_{n+1}^- \end{cases}$$

Le système (S_1) est vérifié d'après les hypothèses (6.2) et, en utilisant les définitions par récurrence des divers $\mathbf{T}^+$-modules concernés, on voit que, pour tout $n \geqslant 1$, si (S_n) est vrai, (S_{n+1}) l'est aussi.

(6.9) Je déduis d'abord de (6.8) le résultat suivant:

PROPOSITION. *Pour tout $n \geqslant 1$, H_n est un groupe, H_{n+1} est un sous-groupe distingué de H_n et l'application suivante:*

$$f_n : (1+u) \in H_n \to \psi_n(\theta u) \in L_n / L_{n+1}$$

est un morphisme surjectif de noyau, H_{n+1}.

DEMONSTRATION. Soit $n \geqslant 1$ quelconque. Soient $(1+u)$ un élément de H_n et $(1+v) = (1+u)^{-1}$ dans $\mathrm{SL}(2, \bar{\mathbf{Q}}_\ell)$. Alors:

$$\begin{cases} \mathrm{tr}(v) = \mathrm{tr}(u) \\ \theta(v) = -\theta(u) \end{cases}$$

donc $(1+v)$ est aussi dans H_n.

Soient $(1+u)$ et $(1+v)$ deux éléments de H_n, je pose:

$$(1+w) = (1+u)(1+v).$$

Alors:

$$\mathrm{tr}(w) = \mathrm{tr}(u) + \mathrm{tr}(v) + \mathrm{tr}(u).\mathrm{tr}(v)/2 + \mathrm{tr}(\theta u . \theta v),$$
$$\theta(w) = \theta(u) + \theta(v) + \mathrm{tr}(u).\theta(v)/2 + \mathrm{tr}(v).\theta(u)/2 + \theta(\theta u . \theta v).$$

On en déduit, en utilisant (6.8):

$$\mathrm{tr}(w) \in A^+,$$
$$\theta(w) - \theta(u) - \theta(v) \in L_{n+1} \quad \text{d'ou} \quad \theta(w) \in L_n.$$

Ceci implique que $(1 + w)$ est dans H_n et que f_n est un morphisme. Il est facile de voir que $\mathrm{Ker}(f_n)$ est H_{n+1}, par conséquent H_{n+1} est un sous-groupe distingué de H_n.

Soit $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ un élément de L_n. On a la formule suivante:

$$4.\det(u) = (b - c)^2 - (b + c)^2 - (a - d)^2,$$

ce qui implique d'après (6.2): $\det(u) \in A^+$.

Comme on peut appliquer le lemme de Hensel dans $\mathbf{T}^+$ et que A^+ est inclus dans $\mathfrak{M}^+$, la quantité $(1 - \det(u))$ admet une racine carrée dans $(1 + A^+)$, que je note $\sqrt{1 - \det(u)}$. Posons:

$$1 + v = \sqrt{1 - \det(u)}.\mathrm{Id} + u,$$

alors:

$$\begin{cases} \det(1 + v) = 1, \\ \mathrm{tr}(v) \in A^+, \\ \theta(v) = u, \end{cases}$$

donc $(1 + v)$ est dans H_n et on voit que f_n est surjective, ce qui achève la démonstration.

Je vais maintenant m'intéresser à divers commutateurs.

(6.10) Soient u et v deux éléments de L. Je note $[u, v] = uv - vu$. C'est encore un élément de L.

PROPOSITION et DEFINITION. Soit $n \geqslant 1$ un entier quelconque. Soient u un élément de L_1 et v un élément de L_n.

(i) $[u, v]$ est dans L_{n+1},
(ii) $\varphi_{n+1}([u, v])$ ne dépend que de $\varphi_1(u)$ et $\varphi_n(v)$,
(iii) pour toute paire $(\tilde{u}, \tilde{v})$ dans $L_1/L_2 \times L_n/L_{n+1}$, je définis $[\tilde{u}, \tilde{v}]_n$ dans L_{n+1}/L_{n+2} par:

$$[\tilde{u}, \tilde{v}]_n = \varphi_{n+1}(u, v])$$

où (u, v) est une paire quelconque dans $L_1 \times L_n$ relevant $(\tilde{u}, \tilde{v})$. D'après (ii), ceci a un sens.

Les éléments $[\tilde{u}, \tilde{v}]_n$, $\tilde{u}$ parcourant L_1/L_2 et $\tilde{v}$ parcourant L_n/L_{n+1}, engendrent le groupe L_{n+1}/L_{n+2}.

DEMONSTRATION. Les points (6.8.b)(i) et (ii)) impliquent, pour tout $n \geqslant 1$ et j dans $\{1, 2\}$:

$$u \in L_j, \quad v \in L_n \to [u,v] \in L_{j+n},$$

on en déduit facilement les points (i) et (ii).

La troisième assertion est évidente à partir des formules (6.7) et de la définition des modules A^-_{n+1}, B^+_{n+1} et B^-_{n+1}.

(6.11) PROPOSITION. (i) *Soit $n \geqslant 1$ un entier quelconque. Soient h_1 et h_n deux éléments respectivement de H_1 et H_n. Je pose:*

$$g = h_1 . h_n . h_1^{-1} . h_n^{-1}.$$

Alors g est dans H_{n+1} et vérifie:

$$f_{n+1}(g) = [f_1(h_1), f_n(h_n)]_n.$$

(ii) *Pour tout $n \geqslant 1$, H_n est distingué dans H_1.*

DEMONSTRATION. Le point (ii) découle de (i) puisque:

$$h_1 . h_n . h_1^{-1} = g . h_n$$

et que H_n est un groupe contenant H_{n+1}. Démontrons (i):

Posons:

$$h_1 = 1 + u,$$
$$h_n = 1 + v,$$
$$g = 1 + w,$$

et:

$$h_1^{-1} . h_n^{-1} = 1 + t.$$

Tout d'abord, g est dans le groupe H_1, ce qui implique:

$$\mathrm{tr}(w) \in A^+.$$

On a aussi la formule suivante: $w = [\theta u, \theta v](1 + t)$ d'où:

$$\theta(w) = \theta([\theta u, \theta v]t) + [\theta u, \theta v].$$

D'après (6.10), l'élément $[\theta u, \theta v]$ est dans L_{n+1}. On en déduit alors, en utilisant (6.8(b)(i)) et (iii) que $\theta([\theta u, \theta v]t)$ est dans L_{n+2}. On a donc:

$$\theta(w) \in L_{n+1},$$
$$\theta(w) - [\theta u, \theta v] \in L_{n+2}.$$

Ceci implique que g est un élément de H_{n+1} et vérifie, d'après (6.10):

$$f_{n+1}(g) = [f_1(h_1), f_n(h_n)]_n.$$

On peut maintenant démontrer le théorème (6.3).

Tout d'abord, les égalités $X = H_1, Y = H_2$ impliquent que X est un groupe, Y un sous-groupe distingué de X et que la fonction: $(a - d, b + c, b - c)$ induit un isomorphisme:

$$X/Y \xrightarrow{\sim} A^-/B^+.B^- \times B^+/A^-.B^- \times B^-/A^-.B^+.$$

Il s'agit de l'assertion (6.9) appliquée au cas $n = 1$, l'isomorphie provient de l'étude de $\psi_1 \circ f_1$. Comme Y est fermé et que le quotient X/Y est abélien, Y contient l'adhérence du groupe dérivé de X.

Pour tout sous-groupe fermé G de X, je note $D(G)$ l'adhérence du groupe dérivé de G, qui est incluse dans $G \cap Y$, et pour tout $n \geqslant 1$ je pose:

$$G_n = G \cap H_n \quad \text{d'où} \quad G_1 = G$$
$$D(G)_n = D(G) \cap H_n \quad \text{d'où} \quad D(G)_2 = D(G)$$
$$\text{et} \quad D(G)_n \subset G_n \quad \text{pour tout } n \geqslant 2.$$

(6.12) PROPOSITION. *Soit* G *un sous-groupe fermé de* X *vérifiant:*

$$X = G.Y.$$

Alors:

(i) $G_n/G_{n+1} = \dfrac{D(G)_n}{D(G)_{n+1}} = \dfrac{H_n}{H_{n+1}}$ *pour tout* $n \geqslant 2$

(ii) $Y = D(G).H_n$ *pour tout* $n \geqslant 2$.

DEMONSTRATION. Les inclusions suivantes sont évidentes:

$$\frac{D(G)_n}{D(G)_{n+1}} \subset \frac{G_n}{G_{n+1}} \subset \frac{H_n}{H_{n+1}} \quad \text{pour tout } n \geqslant 2.$$

L'hypothèse $X = G.Y$ peut encore s'écrire: $f_1(G_1) = L_1/L_2$. Soit n un entier $\geqslant 1$ tel que: $f_n(G_n) = L_n/L_{n+1}$.

Le groupe $D(G)$ contient les commutateurs $g_1 . g_n . g_1^{-1} . g_n^{-1}$, g_1 parcourant G_1 et g_n parcourant G_n. D'après (6.11), ces commutateurs sont dans $D(G)_{n+1}$ et on a:

$$f_{n+1}(g_1 . g_n . g_1^{-1} . g_n^{-1}) = [f_1(g_1), f_n(g_n)]_n,$$

donc le groupe $f_{n+1}(D(G)_{n+1})$ contient les éléments $[u, v]_n$, u et v parcourant respectivement $f_1(G_1)$ et $f_n(G_n)$. D'après (6.10.(iii)) les hypothèses:

$$f_n(G_1) = \frac{L_1}{L_2}, f_n(G_n) = \frac{L_n}{L_{n+1}}$$

impliquent donc:

$$f_{n+1}(D(G)_{n+1}) = \frac{L_{n+1}}{L_{n+2}} = f_{n+1}(G_{n+1})$$

ou encore:

$$\frac{D(G)_{n+1}}{D(G)_{n+2}} = \frac{G_{n+1}}{G_{n+2}} = \frac{H_{n+1}}{H_{n+2}}.$$

Le point (i) est donc démontré par récurrence sur n. Le point (ii) est alors évident.

(6.13) REMARQUE.

$$\bigcap_{n \geqslant 1} L_n = \{0\}, \bigcap_{n \geqslant 1} H_n = \{1\}.$$

En effet, soit $\mathfrak{M}$ l'idéal maximal de $\mathbf{T}$. Il est facile de vérifier que, pour tout $n \geqslant 1$, on a:

$$L_n \subset \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{M}(2, \bar{\mathbf{Q}}_\ell)/a, d \in \mathfrak{M}^{E(n/2)}, \quad b, c \in X . \mathfrak{M}^{E(n/2)} \right\}.$$

Le fait que $\bigcap_{n \geqslant 1} \mathfrak{M}^n = \{0\}$ implique la remarque.

(6.14) PROPOSITION. *Soit* G *un sous-groupe fermé de* X *vérifiant:* $X = G.Y$. *Alors* $D(G)$ *est égal à* Y.

DEMONSTRATION. On a déjà démontré en (6.12):

$$Y = D(G).H_n, \quad \forall n \geqslant 2.$$

Comme $D(G)$ est un groupe fermé, on en déduit, d'après (6.13), que $D(G)$ est égal à Y.

En appliquant cette proposition à $G = X$, on voit que Y est l'adhérence du groupe dérivé de X. Si G est à priori quelconque, les égalités $X = G.Y$ et $Y = D(G)$ impliquent $X = G.D(G) = G$. Le théorème (6.3) est démontré.

7. Image de ρ dans le cas $(\mu/\nu)^2 = 1$

Soit ρ vérifiant (H.1), (H.2) et (H.3) et normalisée de façon à vérifier (8). Soient X et Y les ensembles définis en (6.1). Le résultat principal de ce paragraphe est le suivant: $\rho(D(G^+)) = X$.

On sait déjà d'après (5.17) que $\rho(D(G^+))$ est inclus dans X. D'après (6.1), il suffit d'étudier l'image de $\rho(D(G^+))$ dans le quotient X/Y et de montrer que $X = \rho(D(G^+)).Y$ pour conclure.

Le groupe $D(G^+)$ est distingué dans G. On en déduit les trois points suivants:

(7.1) Soient γ_0 l'élément défini en (1.7) et

$$h = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \quad \text{dans } \rho(D(G^+)).$$

Alors l'élément

$$\rho(\gamma_0)h_\rho(\gamma_0)^{-1} = \begin{pmatrix} 1+a & -b \\ -c & 1+d \end{pmatrix}$$

est encore dans $\rho(D(G^+))$.

(7.2) Soient g dans G_0^+ et

$$h = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \quad \text{dans } \rho(D(G^+)).$$

Alors la matrice suivante est encore dans $\rho(D(G^+))$:

$$\rho(g)h\rho(g)^{-1} = \begin{pmatrix} 1+a & (\varphi/\psi)(g)b \\ (\psi/\varphi)(g)c & 1+d \end{pmatrix}.$$

(7.3) Soit

$$h = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \quad \text{dans } \rho(D(G^+)).$$

Alors l'élément:

$$\rho(h_*)h\rho(h_*)^{-1} = \begin{pmatrix} 1+A & B \\ C & 1+D \end{pmatrix}$$

est encore dans $\rho(D(G^+))$ et vérifie:

$$A + D = a + d,$$
$$A - D = (a-d)(1+2x) + 2\sqrt{x}.\sqrt{1+x}.(b-c),$$
$$B + C = b + c,$$
$$B - C = (b-c)(1+2x) - 2\sqrt{x}.\sqrt{1+x}.(a-d).$$

(7.4) Soient f_1, f_2 et f_3 les morphismes déduits des fonctions coefficients $(a-d)$, $(b+c)$ et $(b-c)$ qui décrivent l'image de $\rho(D(G^+))$ dans X/Y:

$$f_1 : \rho(D(G^+)) \to \mathfrak{I}^-/(\mathbf{T}^-)^2.\mathfrak{I}^-$$
$$f_2 : \rho(D(G^+)) \to \sqrt{x}.(\mathbf{T}^-)^2/\sqrt{x}.(\mathbf{T}^-)^2.\mathfrak{I}^+$$
$$f_3 : \rho(D(G^+)) \to \sqrt{x}.\mathbf{T}^-/\sqrt{x}.(\mathbf{T}^-)^2.\mathfrak{I}^-$$

Les points précédents permettent de démontrer la proposition suivante:

PROPOSITION. *Le morphisme (f_1, f_2, f_3) est surjectif.*

DEMONSTRATION. Il est clair que $\mathrm{Im}(f_1, f_2, f_3)$ est un $\mathbf{Z}_\ell$-module. Le point (7.1) implique:

$$\mathrm{Im}(f_1, f_2, f_3) = \mathrm{Im}(f_1) \times \mathrm{Im}(f_2, f_3).$$

En tenant compte de ceci, le point (7.3) implique:

$f_3(\mathrm{Ker} f_2)$ est un $\mathbf{Z}_\ell[x]$-module, $\sqrt{x}.\mathrm{Im}(f_3) \subset \mathrm{Im}(f_1)$.

Utilisons une variante du point (7.2): soient $g = \gamma_0 . g_0$, qui est dans G_0^+, h quelconque dans $\rho(D(G^+))$ et $k = \rho(g).h.\rho(g)^{-2}.h.\rho(g)$ Alors:

$$f_2(k) = (\varphi/\omega + \psi/\varphi)(g).f_2(h),$$
$$f_3(k) = (\varphi/\psi + \psi/\varphi)(g).f_3(h),$$

et:

$$(\varphi/\psi + \psi/\varphi)(g) = 2 - \frac{\mathrm{tr}(g_0)^2}{\det(g_0)}.$$

Ceci montre que $\mathrm{Im}(f_2)$ et $f_3(\mathrm{Ker}\, f_2)$ sont des $\mathbf{Z}_\ell[\mathrm{tr}(g_0)^2]$-modules.

D'après (5.12), $\mathrm{Im}(f_2)$ et $f_3(\mathrm{Ker}\, f_2)$ sont des $\mathbf{T}^+$-modules puisque:

$$\mathbf{T}^+ = \mathbf{Z}_\ell[\mathrm{tr}(g_0)^2, x] = \mathbf{Z}_\ell[\mathrm{tr}(g_0)^2] + \mathfrak{I}^+.$$

Considérons le produit $k' = \rho(g.h_*.g^{-2}.h_*^{-1}.g)$ où $g = \gamma_0 . g_0$. Cette matrice k' est dans $\rho(D(G^+))$ et vérifie:

$$(b + c)(k') = 0$$
$$(b - c)(k') = 2\sqrt{x}.\sqrt{1+x}.\mathrm{tr}(g_0).\omega^m(\gamma_0).\frac{(\varphi + \psi)(g)}{\det(g)},$$

ce qui montre que: $f_3(\mathrm{Ker}\, f_2) = \sqrt{x}.\mathbf{T}^-/\sqrt{x}.(\mathbf{T}^-)^2.\mathfrak{I}^-$ donc:

f_3 est surjectif,

$\mathrm{Im}(f_2, f_3) = \mathrm{Im}(f_2) \times \mathrm{Im}(f_3)$.

L'inclusion $\sqrt{x}.\mathrm{Im}\,(f_3) \subset \mathrm{Im}(f_1)$ implique que f_1 est aussi surjectif. Il nous reste à voir que f_2 est surjectif, ce qui est immédiat car le commutateur $k'' = \rho(\gamma_0 . g_0 . h_* . g_0^{-1} . \gamma_0^{-1} . h_*^{-1})$ est dans $\rho(D(G^+))$ et vérifie:

$$(b + c)(k'') = -\sqrt{x}.\sqrt{1+x}.\frac{\mathrm{tr}(g_0)^2}{\det(g_0)}.$$

Il s'agit d'un générateur du $\mathbf{T}^+$-module $\sqrt{x}.(\mathbf{T}^-)^2$.

(7.5) Le point (7.4) équivaut à $\mathbf{X} = \rho(D(G^+))$. Or $\rho(D(G^+))$ est un groupe fermé. On en déduit immédiatement, en utilisant (6.1), le résultat suivant:

THEOREME B1. *Soit* ρ *vérifiant* (H.1), (H.2) *et* (H.3) *et normalisée de façon*

à vérifier (8). *Alors:*

$$\rho(D(G^+)) = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \,\middle/\, \begin{array}{ll} a+d \in (\mathbf{T}^-)^2.\mathfrak{I}^+, & a-d \in \mathfrak{I}^- \\ b+c \in X.(\mathbf{T}^-)^2, & b-c \in X.\mathbf{T}^- \end{array} \right\}$$

Connaissant ρ restreint à H_*, on en déduit $(\rho, f)(H)$:

THEOREME B2. *Sous les mêmes hypothèses,* $(\rho, f)(H)$ *est égal à:*

$$\left\{ \left(\begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix}, y \right) \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \times \tilde{X} \,\middle/\, \begin{array}{l} a+d \in \mathfrak{I}^+, \quad a-d \in \mathfrak{I}^- \\ \frac{1}{2}(b+c) \in X, \quad b-c \in X.\mathbf{T}^-, \\ b+c \equiv 2y \bmod X.(\mathbf{T}^-)^2, \\ a+d \equiv 2(\sqrt{1+y^2}-1) \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+ \end{array} \right\}$$

DEMONSTRATION. Il est clair d'après (5.14) et (5.17) que $(\rho, f)(H)$ est inclus dans ce groupe. Notons que la propriété:

$$1 + (a+d)/2 \equiv \sqrt{1+y^2} \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+$$

est automatiquement vérifiée dès que les autres le sont puisque:

$$(1+a)(1+d) - bc = 1$$

ou encore: $(2+a+d)^2 = 4 + (b+c)^2 + (a-d)^2 - (b-c)^2$.

On sait aussi que $f(H)$ est égal à $\tilde{X}$. D'après la définition de f et le fait que $(\rho, f)(H)$ contient $\rho(D(G^+)) \times \{0\}$, le Théorème B2 est une conséquence de B1.

(7.6) Puisque G^+ est égal à $G_0^+.H$, on peut maintenant décrire le groupe $(\rho, f, \chi_\ell)(G^+)$:

THEOREME B3. *Sous les mêmes hypothèses,* $(\rho, f, \chi_\ell)(G^+)$ *est égal à:*

$$\left\{ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, y, t \right) \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \times \tilde{X} \times (\mathbf{Z}_\ell^*)^2 \,\middle/\, \begin{array}{l} ad - bc = \det(t), b - c \in X.\mathbf{T}^- \\ a - d \equiv (\widetilde{\varphi - \psi})(t) \bmod \mathfrak{I}^- \\ b + c \equiv (\widetilde{\varphi + \psi})(t) y \bmod X.(\mathbf{T}^-)^2 \\ a + d \equiv (\widetilde{\varphi + \psi})(t)\sqrt{1+y^2} \\ \qquad \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+ \end{array} \right\}$$

où $(\widetilde{\varphi + \psi})$ *et* $(\widetilde{\varphi - \psi})$ *désignent les réductions respectivement modulo* $(\mathbf{T}^-)^2.\mathfrak{I}^+$ *et* $\mathfrak{I}^-$.

DEMONSTRATION. Il est clair que:

$$(\rho, f, \chi_\ell)(G_0^+) = \left\{\left(\begin{pmatrix} \varphi(t) & 0 \\ 0 & \psi(t) \end{pmatrix}, 0, t\right) \middle/ t \in (\mathbf{Z}_\ell^*)^2\right\}.$$

Ce théorème est alors une conséquence immédiate de B2 et de la décomposition $G^+ = G_0^+ . H$.

COROLLAIRE B3. *Soit* ρ *vérifiant les hypothèses* (H.1), (H.2) *et* (H.3). *Alors* $(\mathrm{tr}, f, \chi_\ell)(G^+)$ *est égal à:*

$$\{(\tau, y, t) \in \mathbf{T}^+ \times \tilde{X} \times (\mathbf{Z}_\ell^*)^2/\tau \equiv (\varphi + \psi)(t) . \sqrt{1 + y^2} \bmod (\mathbf{T}^-)^2 . \mathfrak{I}^+\}.$$

DEMONSTRATION. Ceci est une conséquence évidente du Théorème B3 si ρ vérifie aussi (8). Or il existe toujours une représentation conjugée de ρ vérifiant (8) et la fonction $(\mathrm{tr}, f, \chi_\ell)$ est indépendante de la conjugaison effectuée.

REMARQUE. La fonction $(\varphi + \psi)$ fournit, par réduction, deux fonctions canoniques respectivement de G^+ dans $\mathbf{T}^+/(\mathbf{T}^-)^2 . \mathfrak{I}^+$ et de G^- dans $\mathbf{T}^-/\mathfrak{I}^-$ (cf. (5.22)). On en déduit que $(\varphi - \psi)$ donne, par réduction, deux fonctions respectivement de G^+ dans $\mathbf{T}^-/\mathfrak{I}^-$ et de G^- dans $\mathbf{T}^+/(\mathbf{T}^-)^2 . \mathfrak{I}^+$ qui sont canoniques au signe près. En effet, pour tout g dans G, on a la formule suivante:

$$(\varphi - \psi)(g) = \omega^{-m}(\gamma) . (\varphi + \psi)(\gamma . g),$$

où γ est un élément quelconque de G^- vérifiant $\langle \gamma \rangle = 1$.

La formule précédente ne dépend que du choix de m, la paire (m, n) étant canonique.

THEOREME B4. *Soit* ρ *vérifiant* (H.1), (H.2) *et* (H.3) *et normalisée de façon à vérifier* (8). *Alors* $(\rho, \chi_\ell)(G)$ *est égal à:*

$$\left\{\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, t\right) \in \mathrm{SL}(2, \bar{\mathbf{Q}}_\ell) \times \mathbf{Z}_\ell^* \;\middle|\; \begin{array}{l} ad - bc = \det(t) \\ a + \varepsilon d \equiv (\varphi + \varepsilon\psi)(t) \bmod \mathfrak{I}^+ \\ a - \varepsilon d \equiv (\varphi - \varepsilon\psi)(t) \bmod \mathfrak{I}^- \\ b - \varepsilon c \equiv 0 \bmod X . \mathbf{T}^- \\ \dfrac{(b + \varepsilon c)}{(\varphi + \varepsilon\psi)(t)} \in X \\ \text{où } \varepsilon = \omega^{(\ell-1)/2}(t) \end{array}\right\}$$

DEMONSTRATION. Ce théorème est une conséquence directe du Théorème

B3, sachant que: $G = G^+ \cup \gamma_0 . G^+$ avec:

$$\chi_\ell(\gamma_0) = \omega(\gamma_0),$$
$$\omega^{(\ell-1)12}(\gamma_0) = -1,$$
$$\rho(\gamma_0) = \begin{pmatrix} \varphi(\gamma_0) & 0 \\ 0 & \psi(\gamma_0) \end{pmatrix}.$$

COROLLAIRE B4. *Soit ρ vérifiant les hypothèses* (H.1), (H.2) *et* (H.3). *Alors* $(\mathrm{tr}, \chi_\ell)(G^-)$ *est égal à*:

$$\{(\tau, t) \in \mathbf{T}^- \times \mathbf{Z}_\ell^* / t^{(\ell-1)/2} \equiv -1 \bmod \ell, \tau \equiv (\varphi + \psi)(t) \bmod \mathfrak{I}^-\}.$$

Ce corollaire est évident si ρ vérifie aussi (8). Or il existe toujours une représentation conjuguée de ρ vérifiant (8) et la fonction (tr, χ_ℓ) est indépendante de la conjugaison effectuée.

Notons que les paramètres qui interviennent dans les Théorèmes B1 à B4 et leurs corollaires dépendent uniquement de la classe d'isomorphisme de ρ.

8. Application au calcul d'une représentation donnée

Le but de ce paragraphe est de montrer comment utiliser de façon concrète les Théorèmes A et B et, en particulier, d'expliquer comment ont été calculés les exemples numériques du paragraphe 9.

(8.1) Soit f une forme parabolique pour $\mathrm{SL}(2, \mathbf{Z})$, de poids k, propre pour l'action des opérateurs de Hecke et normalisée:

$$f(z) = \sum_{n \geq 1} a_n . q^n \quad \text{où} \quad q = e^{2i\pi z} \quad \text{et} \quad a_1 = 1.$$

Soit O_f l'anneau des entiers du corps des coefficients de f, $\mathbf{Q}[\ldots, a_n, \ldots]$, extension finie de $\mathbf{Q}$. Les coefficients a_n sont dans O_f.

Soient ℓ un nombre premier impair et λ un idéal premier de O_f au dessus de ℓ. Soit O_λ le complété de O_f en λ, de corps résiduel $\mathbf{F}_\lambda$.

THEOREME (Serre, Deligne). *Il existe une représentation continue*:

$$\rho_{\lambda, f}: \mathrm{Gal}(K_\ell / \mathbf{Q}) \to GL(2, 0_\lambda)$$

vérifiant:

(i) $\det = \chi_\ell^{k-1}$
(ii) $\mathrm{tr}(\mathrm{Frob}(p)) = a_p$ pour tout nombre premier $p \neq \ell$.

(8.2) La théorie des formes modulaires modulo ℓ permet de déterminer s'il existe m et n dans $\mathbf{Z}/(\ell - 1)\mathbf{Z}$ tels que $\rho_{\lambda,f}$ vérifie:

$$\mathrm{tr} \equiv \omega^m + \omega^n \bmod \lambda.$$

Notons en particulier le résultat suivant:

PROPOSITION. *S'il existe m et n tels que:* $\mathrm{tr} \equiv \omega^m + \omega^n \bmod \lambda$, *$\ell$ vérifie:*

- *soit* $\ell \leqslant k - 5$
- *soit ℓ divise le numérateur du k-ième nombre de Bernouilli* b_k.

(8.3) *Théorie des formes modulaires modulo* $\ell (\ell \neq 2, 3)$.
Le but de ce paragraphe est d'esquisser cette théorie due à Serre et Swinnerton-Dyer et de démontrer la proposition (8.2). *Cette proposition est une légère amélioration d'un résultat bien connu. Pour un exposé plus complet de cette théorie, voir* [3].

Pour tout poids k, soit M_k l'ensemble des formes modulaires pour SL(2, **Z**) de poids k à coefficients de Fourier dans **Q** entiers en ℓ. Soit $\tilde{M}_k$ l'image de M_k dans $\mathbf{F}_\ell[[q]]$ obtenue par réduction modulo ℓ des coefficients de Fourier. Notons que:

$$\tilde{M}_k = \frac{M_k}{\ell M_k}.$$

Si f est un élément de M_k, je note $\tilde{f}$ son image dans $\tilde{M}_k$.

Soit $\tilde{M} = \Sigma_{k \geqslant 0} \tilde{M}_k$ la sous-algèbre de $\mathbf{F}_\ell[[q]]$ engendrée par les $\tilde{M}_k$. Cette somme n'est pas directe.

Pour tout $k \geqslant 4$ pair, soient G_k et E_k les séries d'Eisenstein suivantes:

$$G_k = \frac{-b_k}{2k} + \sum_{n \geqslant 1} \sigma_{k-1}(n) \cdot q^n,$$

$$E_k = -\left(\frac{2k}{b_k}\right) \cdot G_k = 1 - \left(\frac{2k}{b_k}\right) \cdot \sum_{n \geqslant 1} \sigma_{k-1}(n) \cdot q^n,$$

où b_k est le $k$ième nombre de Bernouilli et $\sigma_{k-1}(n) = \Sigma_{d|n; d \geqslant 1} d^{k-1}$. Les séries G_k et E_k sont des formes modulaires pour SL(2, **Z**) de poids k.

LEMME (Von Staudt, Kummer). (i) *Si* $(\ell - 1) | k$ *alors* $b_k \equiv -1 \bmod \ell$, (ii) *Si*

$(\ell - 1) \nmid k$ alors b_k/k est entier en ℓ et sa classe résiduelle modulo ℓ ne dépend que de celle de k modulo $(\ell - 1)$.

Ce lemme implique:

(i) $E_{\ell-1} \in M_{\ell-1}$ et $\tilde{E}_{\ell-1} = 1$,
(ii) Si $(\ell - 1) \nmid k$ alors G_k est dans M_k.

Donc, pour tout poids k, la multiplication par $\tilde{E}_{\ell-1}$ est une injection canonique de $\tilde{M}_k$ dans $\tilde{M}_{k+\ell-1}$. On voit que $\tilde{M}$ n'est pas une somme directe.

Soit $\tilde{f}$ dans $\tilde{M}_k \otimes \bar{\mathbf{F}}_\ell$ non nulle. On définit sa filtration

$$\omega(\tilde{f}) = \inf\{j / \tilde{f} \in \tilde{M}_j \otimes \bar{\mathbf{F}}_\ell\}.$$

Elle vérifie:

$$\omega(\tilde{f}) \equiv k \bmod (\ell - 1).$$

On introduit aussi un opérateur θ agissant sur les différents M_k:

$$\theta = q \cdot \frac{d}{dq}, \quad f = \sum_{n \geq 0} a_n \cdot q^n \to \theta(f) = \sum_{n \geq 1} n a_n \cdot q^n.$$

L'opérateur θ agit, par passage au quotient, sur $\tilde{M}$ puis $\tilde{M} \otimes \bar{\mathbf{F}}_\ell$. Il envoie $\tilde{M}_k$ dans $\tilde{M}_{k+\ell-1}$ pour tout poids k. θ vérifie aussi:

$\omega(\theta \tilde{f}) \leqslant \omega(\tilde{f}) + \ell + 1$ avec égalité si et seulement si ℓ ne divise pas $\omega(\tilde{f})$, ceci pour tout poids k et tout élément $\tilde{f}$ de $\tilde{M}_k \otimes \bar{\mathbf{F}}_\ell$, en particulier $\theta(\tilde{f}) \neq 0$ si $\omega(\tilde{f}) \not\equiv 0 \bmod \ell$.

Démontrons maintenant la proposition (8.2). Je reprends la situation (8.1).

Soit f une forme parabolique pour $\mathrm{SL}(2, \mathbf{Z})$ de poids k, propre pour l'action des opérateurs de Hecke et normalisée. Soit λ un idéal premier de O_f divisant ℓ. La réduction $\tilde{f}$ de f mod λ est un élément de $\tilde{M}_k \otimes \bar{\mathbf{F}}_\ell$. Je suppose que la représentation associée vérifie la congruence:

$$\mathrm{tr}(g) \equiv \omega^m(g) + \omega^n(g) \bmod \lambda, \forall g \in \mathrm{Gal}(K_\ell/\mathbf{Q})$$

ou encore, en prenant $g = \mathrm{Frob}(p)$:

$$a_p \equiv p^m + p^n \bmod \lambda \quad \text{pour tout nombre premier} \quad p \neq \ell,$$

avec m et n dans $\mathbf{Z}/(\ell - 1)\mathbf{Z}$. Puisque $\det = \chi_\ell^{k-1}$, les nombres m et n vérifient:

$m + n \equiv k - 1 \bmod(\ell - 1)$, ce qui, par parité, implique que m et n sont distincts. La représentation $\rho_{\lambda,f}$ vérifie donc (H.1), (H.2) et (H.3) ou (H.3. bis.(i)).

Je choisis des représentants de m et n dans $\{0, \ldots, \ell - 2\}$ que je note encore m et n et qui vérifient:

$0 \leqslant m < n \leqslant \ell - 2$ (m et n étant précédemment déterminés à l'ordre près).

Par multiplicativité des coefficients, f vérifie la congruence suivante:

$a_j \equiv j^m . \sigma_{n-m}(j) \bmod \lambda$ pour tout entier j premier à ℓ.

Si ℓ est égal à 3, il vérifie $\ell \leqslant k - 5$ car $k \geqslant 12$. Supposons donc $\ell \geqslant 5$. On peut utiliser la théorie esquissée plus haut. La congruence précédente implique:

$$\theta(\tilde{f}) = \theta^{m+1}(\tilde{G}_{n-m+1})$$

à deux exceptions près:

- $n - m + 1 = 2$ car je n'ai pas défini G_2 on a alors: $\theta(\tilde{f}) = \theta^{m+1}(\tilde{G}^{\ell+1})$
- $n - m + 1 = \ell - 1$ car $G_{\ell-1}$ n'est pas dans $M_{\ell-1}$ cette égalité implique: $m = 0$, $n = \ell - 2$ d'où $a_p \equiv 1 + 1/p \bmod \lambda$, $\forall p \neq \ell$ ou encore: $\theta(\tilde{f}) = \theta^{\ell-1}(\tilde{G}_{\ell+1})$.

(1) Cas $m = 0$, $n \neq (\ell - 2)$. On a donc:

$$n \equiv k - 1 \bmod(\ell - 1)$$
$$\theta(\tilde{f}) = \theta(\tilde{G}_k)$$

Ceci implique:

soit $\tilde{f} = \tilde{G}_k$;

soit $\omega(\tilde{f} - \tilde{G}_k) \equiv 0 \bmod \ell$, mais on a aussi:

$\omega(\tilde{f} - \tilde{G}_k) \equiv k \equiv n + 1 \bmod(\ell - 1)$ d'où:

$\omega(\tilde{f} - \tilde{G}_k) \equiv \ell(n + 1) \bmod \ell(\ell - 1)$ et, par choix de n:

$\omega(\tilde{f} - \tilde{G}_k) \geqslant \ell(n + 1) \geqslant 2\ell$ mais aussi: $\omega(\tilde{f} - \tilde{G}_k) \leqslant k$.

Ceci est impossible si $\ell > k/2$.

L'inégalité $\ell \leqslant k/2$ implique $\ell \leqslant k - 5$ car k est supérieur ou égal à 12.

Si ℓ est supérieur à $k - 5$, on est donc dans le cas: $\tilde{f} = \tilde{G}_k$, ce qui implique, en regardant le terme constant, que ℓ divise le numérateur de b_k.

(2) Cas $m = 0$, $n = (\ell - 2)$ et cas $m \neq 0$, $n = m + 1$.
On a alors: $\theta(\tilde{\mathcal{F}}) = \theta^a(\tilde{G}_{\ell+1})$ avec

$$a = m + 1 \quad \text{si} \quad m \neq 0 \quad \text{et} \quad n = m + 1$$

et

$$a = \ell - 1 \quad \text{si} \quad m = 0 \quad \text{et} \quad n = \ell - 2.$$

Dans ces deux cas, a vérifie:

$$2 \leqslant a \leqslant \ell - 1.$$

On a aussi: $\omega(\tilde{G}_{\ell+1}) = \ell + 1$ car $\tilde{M}_2 = \{0\}$, ce qui implique par récurrence:

$$\omega(\theta^a \tilde{G}^{\ell+1}) = (a + 1)(\ell + 1) \text{ car } a \leqslant \ell - 1.$$

On obtient donc:

$$k \geqslant a(\ell + 1) \geqslant 2(\ell + 1),$$

ou encore:

$$\ell \leqslant k/2 - 1 \leqslant k - 5 \text{ car } k \geqslant 12.$$

(3) Cas $m \neq 0$, $n \neq m + 1$. Il s'agit du cas général: $\theta(\tilde{\mathcal{F}}) = \theta^{m+1}(\tilde{G}_{n-m+1})$.
On a: $4 \leqslant n - m + 1 \leqslant (\ell - 3)$ et, par conséquent: $\omega(\tilde{G}_{n-m+1}) = n - m + 1$ d'où:

$$\omega(\theta\tilde{\mathcal{F}}) = \omega(\theta^{m+1}\tilde{G}_{n-m+1}) = (n - m + 1) + (\ell + 1)(m + 1),$$

en calculant cette dernière filtration par récurrence. On obtient l'inégalité suivante:

$$k \geqslant (n - m + 1) + m(\ell + 1) \geqslant 4 + (\ell + 1),$$

ou encore: $\ell \leqslant k - 5$.

En rassemblant ces résultats on voit que, si ℓ est supérieur à $k - 5$, ℓ divise le numérateur de b_k. La proposition (8.2) est démontrée.

(8.4) Reprenons la situation (8.1) et supposons désormais qu'il existe m et n dans

$\mathbf{Z}/(\ell-1)\mathbf{Z}$ tels que $\rho_{\lambda,\ell}$ vérifie:

$$\mathrm{tr} \equiv \omega^n + \omega^n \bmod \lambda.$$

Je suppose aussi que le nombre premier ℓ vérifie: $(h^+, \ell) = 1$ (hypothèse (H.3. bis.(ii))). Suivant la valeur de $(m-n)$, les Théorèmes A ou B décrivent l'image de $\rho_{\lambda,\ell}$. J'explique ici comment calculer explicitement les paramètres intervenant dans ces théorèmes.

Soit p_0 un nombre premier engendrant topologiquement $\mathbf{Z}_\ell^*$. On peut choisir g_0 égal à $\mathrm{Frob}(p_0)$. Les caractères φ et ψ sont alors déterminés par les équations:

$$\varphi(p_0) + \psi(p_0) = a_{p_0}$$
$$\varphi(p_0) \cdot \psi(p_0) = p_0^{k-1}.$$

Les réductions mod λ de φ et ψ sont ω^n et ω^n. Connaissant m et n, on sait s'il faudra utiliser les Théorèmes A ou B.

D'après (2.7) et (2.8), il existe g_* dans $\mathrm{Gal}(K_\ell/\mathbf{Q}[\mu_\ell])$ dont les images dans $X(\omega^{m-n})$ et $X(\omega^{n-m})$ engendrent ces deux $\mathbf{Z}_\ell$-modules cycliques. Par densité des éléments de Frobenius, il existe un nombre premier p_* congru à 1 modulo ℓ tel que $g_* = \mathrm{Frob}(p_*)$ convienne. Le critère (2.11) permet d'exhiber un tel p_*. Notons que les deux caractères ω^{m-n} et ω^{n-m} vérifient l'hypothèse:

$$(\varepsilon/\omega)^{(\ell-1)/2} = 1$$

car k est pair, ℓ impair et: $m + n \equiv k - 1 \bmod(\ell - 1)$. Connaissant a_{p_*}, on peut calculer tous les autres paramètres.

Cas du théorème A:
L'algèbre $\mathbf{T}$ est la $\mathbf{Z}_\ell$-algèbre engendrée par les quantités a_{p_0} et a_{p_*}.

L'idéal $\mathfrak{I}$ est égal à $(a_{p_*} - \varphi(p_*) - \psi(p_*)) \cdot \mathbf{T}$.

Les caractères φ et ψ ont été calculés plus haut et det est égal à χ_ℓ^{k-1}.

Cas des théorèmes B:
Soit h_* un élément de H possédant les propriétés demandées en (5.3). Soit H_* le sous-groupe fermé de H engendré par h_*. Il existe alors g dans G_0 et h dans H_* tels que $h^{-1} \cdot g^{-1} \cdot \mathrm{Frob}(p_*)$ soit dans $\mathrm{Gal}(K_\ell/N')$. Ceci implique:

$$\begin{cases} \chi_\ell(g) = p_* \\ \theta_*(h) = \theta_*(\mathrm{Frob}(p_*)). \end{cases}$$

En particulier, h engendre aussi H_*. On peut donc supposer que h_* est égal à h. La

décomposition: $\mathrm{Frob}(p_*) \in g.h_*.\mathrm{Gal}(K_\ell/N')$ implique aussi:

$$a_{p_*} \equiv (\varphi + \psi)(p_*).\sqrt{1+x} \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+.$$

On connaît donc x modulo $(\mathbf{T}^-)^2.\mathfrak{I}^+$.

Ce degré de précision suffit pour déterminer les modules suivants:

$$\mathbf{T}^+ = \mathbf{Z}_\ell[a_{p_0}^2, x],$$
$$\mathbf{T}^- = a_{p_0}.\mathbf{T}^+,$$
$$\mathbf{T} = \mathbf{Z}_\ell[a_{p_0}, x],$$
$$\mathfrak{I}^+ = x.\mathbf{T}^+,$$
$$\mathfrak{I}^- = x.\mathbf{T}^-,$$
$$\mathfrak{I} = x.\mathbf{T}.$$

On peut aussi déterminer X qui est le sous-groupe fermé de $\sqrt{x}.\mathbf{T}^+$ (pour la loi $*$) engendré par $\sqrt{x}$ et $\sqrt{x}.(\mathbf{T}^-)^2$.

Enfin f est le morphisme de G^+ dans $\tilde{X}$ (ce dernier groupe étant muni de la loi $*$) qui se factorise par θ_* (cf. (2.5)) et vérifie:

$$f(\mathrm{Frob}(p_*)) \equiv \sqrt{x} \bmod X.(\mathbf{T}^-)^2.$$

Ceci détermine f au signe près.

Les caractères φ et ψ ont déjà été calculés et det est égal à χ_ℓ^{k-1}.

Connaissant deux coefficients de Fourier particuliers de f, il est donc possible de calculer explicitement les paramètres intervenant dans les Théorèmes *A* ou *B*.

(8.5) REMARQUE. Le fait que ρ provienne d'une forme parabolique a été relativement peu utilisé. La méthode précédente s'applique à tout nombre premier ℓ vérifiant $(h^+, \ell) = 1$ et à toute représentation ρ vérifiant (H.1) et (H.2) et dont on connaît:

- le déterminant,
- $\mathrm{tr}(\mathrm{Frob}(p))$ pour tout nombre premier $p \neq \ell$.

Il suffit alors de calculer explicitement deux quantités $\mathrm{tr}(\mathrm{Frob}(p))$ particulières pour obtenir une version explicite des Théorèmes A ou B appliqués à ρ.

(8.6) *Congruences vérifiées par les coefficients de Fourier de f*: Je reprends la situation (8.1) et suppose que $\rho_{\lambda,f}$ vérifie (H.1). Les coefficients de Fourier de f vérifient:

$$a_p \equiv \varphi(p) + \psi(p) \bmod \mathfrak{I}, \forall p \neq \ell \text{ premier}.$$

D'après la définition de φ, ψ et $\mathfrak{I}$ et par densité des éléments de Frobenius, cette congruence est la plus précise possible de ce type.

Dans le cas où $(\mu/\nu)^2$ est trivial, f vérifie de plus:

$$a_p \equiv (\varphi + \psi)(p) \begin{cases} \text{dans } \mathbf{T}^+/\mathfrak{I}^+ & \text{si } p \text{ est un carré modulo } \ell \\ \text{dans } \mathbf{T}^-/\mathfrak{I}^- & \text{si } p \text{ n'est pas un carré mod} \ell. \end{cases}$$

Ces deux congruences sont, elles aussi, les plus précises de ce type.

Les coefficients a_p, p carré modulo ℓ, vérifient une congruence d'un type plus compliqué:

$$a_p \equiv (\varphi + \psi)(p).\sqrt{1 + f^2(\mathrm{Frob}(p))} \bmod (\mathbf{T}^-)^2.\mathfrak{I}^+.$$

9. Exemples numériques

Dans ce paragraphe, f désigne une forme parabolique pour SL(2, **Z**) propre pour l'action des opérateurs de Hecke et de poids k compris entre 12 et 38, 36 excepté. De plus, f est normalisée:

$$f(z) = \sum_{n \geq 1} a_n.q^n \quad \text{où} \quad q = 2^{2i\pi z} \quad \text{et} \quad a_1 = 1.$$

La forme f est alors essentiellement unique. Plus précisément f est unique si k est inférieur strictement à 24 ou égal à 26. Dans le cas contraire, il existe deux formes f conjuguées par $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ ce qui permet de les confondre.

Le nombre ℓ parcourt l'ensemble des nombres premiers impairs inférieurs à $k - 5$ (cette hypothèse étant justifiée par la Proposition (8.2)). Si k est inférieur à 24 ou égal à 26, il existe alors une unique représentation $\rho_{\ell,f}$ associée au couple (f, ℓ) (cf (8.1)). Dans le cas contraire, ℓ est décomposé dans l'anneau des entiers de f, à une exception près ($k = 28, \ell = 3$). A chacun des deux idéaux λ relevant ℓ, on peut associer une représentation $\rho_{\lambda,f}$ déterminée par le triplet $(k, \ell, \sqrt{d} \bmod \lambda)$ où le corps des coefficients de f est égal à $\mathbf{Q}[\sqrt{d}]$.

Le cas ($k = 28, \ell = 3$) est traité séparément.

Les tables qui suivent permettent de déterminer l'image de ρ dans les cas où elle vérifie les hypothèses de cet article, ce qui d'après (8.4) revient à supposer:

(H.4) Il existe m et n dans $\mathbf{Z}/(\ell - 1)\mathbf{Z}$ tels que

$$a_p \equiv p^m + p^n \bmod \lambda \text{ pour tout } p \neq \ell, \text{ premier.}$$

En effet, comme ℓ est inférieur ou égal à 33, l'hypothèse (H.3.bis.ii) est toujours vérifiée.

Les tables doivent se lire comme suit:

- k et ℓ sont bien indiqués
- j'indique la valeur de $\sqrt{d} \bmod \lambda$ si nécessaire
- j'indique ensuite si (H.4) est vérifiée, ce qui suit concerne le cas où (H.4) est vraie
- je donne le type de théorème qui se rapporte à ρ (A ou B)
- je donne un générateur de l'idéal $\mathfrak{I}$
- si on est dans le cas B, je donne un générateur de $\mathbf{T}^-$
- je donne le nombre test p_* qui sert à déterminer l'idéal $\mathfrak{I}$
- dans le cas B, je donne la variable x modulo $(\mathbf{T}^-)^2.\mathfrak{I}^+$
- j'indique enfin les caractères φ et ψ sous la forme $\varphi = \chi_\ell^M$, $\psi = \chi_\ell^N$, ces caractères étant à valeurs dans:
  - $(\mathbf{T}/\mathfrak{I})^*$ si on est dans le cas A
  - $(\mathbf{T}/(\mathbf{T}^-)^2.\mathfrak{I})^*$ si on est dans le cas B

Dans le cas *B*, il nous faut faire quelques remarques supplémentaires: puisque $\mathbf{T}$ est égal à $\mathbf{Z}_\ell$ on en déduit:

- $\mathbf{T}^+ = \mathbf{T}$
- $\mathfrak{I}^+ = \mathfrak{I}$

La donnée de la paire (p_*, x) permet de déterminer le morphisme f au signe près (cf. (5.21)), f vérifie $f(\mathrm{Frob}(p_*)) = \sqrt{x}$).

Poids 12:				$f = \Delta$			
ℓ	TH.	$\mathfrak{I}$	$\mathbf{T}^-$	p_*	x	$\varphi - M$	$\psi - N$
3	B	729	3	7	729 × 5	2079	2306
5	A	125	—	11	—	70	41
7	B	7	7	29	7 × 36	136	169

Regardons ainsi la forme Δ modulo 3 et les résultats annoncés dans l'introduction. Le morphisme f de G^+ dans $\sqrt{x}.\mathbf{Z}_3/9\sqrt{x}.\mathbf{Z}_3$ défini par:

$$f(\mathrm{Frob}(7)) = \sqrt{x} \text{ où } x = 729 \times 5 = 3645$$

vérifie:

$$\tfrac{1}{2} f^2(\mathrm{Frob}(p)) = 5103v^2/u^2 \text{ pour tout } p \text{ premier} \equiv 1 \bmod 3$$

où u et v sont les entiers positifs définis par l'égalité:

$$4p = u^2 + 27.v^2$$

(La vérification de ce fait est un petit exercice de théorie du corps de classes).

Ceci étant, les congruences annoncées dans l'introduction sont des conséquences directes des corollaires **B.3** et **B.4**.

Poids 16:				$f = \Delta.E_4$			
ℓ	TH.	$\mathfrak{I}$	$\mathbf{T}^-$	p_*	x	$\varphi - M$	$\psi - N$
3	B	243	27	7	243 × 434	5187	112926
5	A	25	—	11	—	18	17
7	A	343	—	29	—	224	85
11	A	11	—	23	—	4	1

Poids 18:				$f = \Delta.E_6$			
ℓ	TH.	$\mathfrak{I}$	$\mathbf{T}^-$	p_*	x	$\varphi - M$	$\psi - N$
3	B	243	3	7	243 × 7	117	1358
5	A	125	—	11	—	95	22
7	B	7	7	29	7 × 3	58	253
11	B	11	11	23	11 × 50	236	991
13	A	13	—	53	—	4	1

Poids 20:				$f = \Delta.E_4^2$			
ℓ	TH.	$\mathfrak{I}$	$\mathbf{T}^-$	p_*	x	$\varphi - M$	$\psi - N$
3	B	243	3	7	243 × 7	207	1270
5	A	25	—	11	—	6	13
7	B	7	7	29	7 × 16	143	170
11	A	11	—	23	—	8	1
13	A	13	—	53	—	6	1

Poids 22:				$f = \Delta.E_4E_6$			
ℓ	TH.	$\mathfrak{I}$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	B	729	9	7	729 × 55	34995	4392
5	A	25	—	11	—	7	14
7	A	49	—	29	—	26	37
11	(H.4) non vérifiée						
13	A	13	—	53	—	8	1
17	A	17	—	103	—	4	1

Poids 24:		$f = \Delta.E_6^2 + (1572 + 12\sqrt{d}).\Delta^2$ où $d = 144169$						
ℓ	$\sqrt{d}$	TH.	$\mathfrak{I}$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	1	B	243	3	7	243 × 8	531	950
3	2	B	729	3	7	729 × 2	3695	702
5	2	A	125	—	11	—	43	80
5	3	A	25	—	11	—	14	9
7	5	A	343	—	29	—	63	254
7	2	B	7	49	29	7 × 2161	11782	2647
11	5	A	1331	—	67	—	1012	221
11	6	(H.4) non vérifiée						
13	8	A	13	—	53	—	10	1
13	5	(H.4) non vérifiée						
17	3	A	17	—	103	—	6	1
17	14	(H.4) non vérifiée						
19	4	A	19	—	191	—	4	1
19	15	(H.4) non vérifiée						

Poids 26:				$f = \Delta.E_4^2.E_6$			
ℓ	TH.	$\Im$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	B	243	3	7	243 × 8	171	1312
5	A	25	—	11	—	19	6
7	B	7	49	29	7 × 1539	5903	8528
11	A	11	—	23	—	4	1
13	(H.4) non vérifiée						
17	A	17	—	103	—	8	1
19	A	19	—	191	—	6	1

Poids 28:					$f = \Delta.E_6^2.E_4 + (-3348 + 108\sqrt{d}).\Delta^2.E_4$ où $d = 18209$			
ℓ	$\sqrt{d}$	TH.	$\Im$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	voir plus bas							
5	2	A	625	—	11	—	302	225
5	3	A	25	—	11	—	11	16
7	3	A	49	—	29	—	38	31
7	4	B	7	49	29	7 × 381	11469	2964
11	2	A	11	—	23	—	5	2
11	9	B	11	11	23	11 × 117	1126	111
13	3	A	2197	—	53	—	1742	313
13	10	(H.4) non vérifiée						
17	11	A	17	—	103	—	10	1
17	6	(H.4) non vérifiée						
19	8	A	19	—	191	—	8	1
19	11	(H.4) non vérifiée						
23	4	A	23	—	47	—	4	1
23	19	(H.4) non vérifiée						

Cas du poids 28, $\ell = 3$:

Le nombre 18209 n'est pas un carré modulo 3. Ainsi la représentation $\rho_{\ell,f}$ a pour corps des coefficients l'extension quadratique non ramifiée de $\mathbf{Q}_\ell$. La représentation $\rho_{\ell,f}$ vérifie les hypothèses des divers théorèmes **B**. Les caractéristiques de cette représentation sont:

$\mathrm{O} = \mathbf{Z}_\ell \oplus \sqrt{d}.\mathbf{Z}_\ell$ (où $\ell = 3$ et $d = 18209$)
anneau des entiers du corps des fractions de **T**,

$\mathbf{T}^+ = \mathbf{Z}_\ell \oplus 243.\sqrt{d}.\mathbf{Z}_\ell$,

$\mathbf{T}^- = (9 + 1350\sqrt{d}).\mathbf{T}^+$,

$\mathbf{T} = \mathbf{Z}_\ell \oplus 27.\sqrt{d}.\mathbf{Z}_\ell$,

$\mathfrak{I}^+ = (243 + 20412.\sqrt{d}).\mathbf{T}^+$.

Notons alors que $3^{14}.\mathrm{O}$ est inclus dans $(\mathbf{T}^-)^2.\mathfrak{I}^+$ et $\mathfrak{I}^-$.

Posons $p_0 = 2$, générateur topologique de $\mathbf{Z}_\ell^*$. Il vérifie:

$$\mathrm{tr}(\mathrm{Frob}(2)) = -4140 + 108.\sqrt{d}$$

ce qui permet de calculer φ et ψ:

$$\varphi(2) \equiv 4491971 + 3241431.\sqrt{d} \bmod 3^{14}.\mathrm{O},$$
$$\psi(2) \equiv 286858 + 1541646.\sqrt{d} \bmod 3^{14}.\mathrm{O}.$$

On connaît ainsi φ et ψ avec le degré de précision nécessité par les théorèmes B.

Choisissons $p_* = 7$. Il vérifie:

$$\mathrm{tr}(\mathrm{Frob}(7)) = -87695981800 + 809077248.\sqrt{d},$$

ce qui permet de calculer la constante x associée:

$$x \equiv 2333772 + 1942785.\sqrt{d} \bmod 3^{14}.\mathrm{O}.$$

On peut alors utiliser explicitement les théorèmes B pour décrire l'image de $\rho_{\ell,f}$.

Par exemple, précisons le morphisme f:

On peut constater que $\mathfrak{I}^+$ est inclus dans $(\mathbf{T}^-)^2$ ce qui implique que la loi de groupe sur $\tilde{X}$ est simplement l'addition. Le sous-groupe de $\mathbf{T}^+/(\mathbf{T}^-)^2$ engendré par 1 étant égal à $\mathbf{Z}/3^8.\mathbf{Z}$, le groupe $\tilde{X}$ est égal à $\sqrt{x}.\mathbf{Z}/3^8.\sqrt{x}.\mathbf{Z}$.

Pour tout nombre premier p congru à 1 modulo 3, il existe un couple unique d'entiers positifs (u, v) vérifiant:

$$4p = u^2 + 27.v^2.$$

Posons $g(p) = u + 3.\sqrt{-3}.v.$

La quantité $g(p)/\overline{g(p)}$ est dans $1 + 3.\sqrt{-3}.\mathrm{O}$.

Le logarithme 3-adique est un isomorphisme de $1 + 3.\sqrt{-3}.\mathrm{O}$ dans $3.\sqrt{-3}.\mathrm{O}$.

Notons F l'application suivante:

$$F(g(p)) = \log\left(\frac{g(p)}{\overline{g(p)}}\right) \bmod 3^9.\sqrt{-3}.$$

Elle définit un morphisme de G^+ dans $3.\sqrt{-3}.\mathbf{Z}/3^9.\sqrt{-3}.\mathbf{Z}$ ayant le comportement voulu pour la conjugaison par G/G^+. On en déduit:

$$f(\mathrm{Frob}(p)) = \sqrt{x}.\left(\frac{F(g(p))}{F(g(7))}\right).$$

Les coefficients de Fourier de f vérifient donc la congruence suivante:

$$a_p \equiv (\varphi + \psi)(p).\sqrt{1 + x\frac{F(g(p))^2}{F(g(7))^2}} \bmod (\mathbf{T}^-)^2.I^+,$$

pour tout nombre premier $p \equiv 1 \bmod 3$.

Poids 30: $f = \Delta.E_6^3 + (5856 + 96\sqrt{d}).\Delta^2.E_6$ où $d = 51349$								
ℓ	$\sqrt{d}$	TH.	$\mathfrak{I}$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	1	B	243	3	7	243 × 8	281	1206
3	2	B	2187	3	7	2187 × 5	9153	3998
5	2	A	25	—	11	—	11	18
5	3	A	3125	—	11	—	125	2404
7	5	A	49	—	29	—	39	32
7	2	B	49	7	29	49 × 20	1498	589
11	1	A	11	—	23	—	8	1
11	10	B	11	11	23	11 × 100	357	882
13	8	A	13	—	53	—	4	1
13	5	(H.4) non vérifiée						
17	3	A	17	—	103	—	12	1
17	14	(H.4) non vérifiée						
19	12	B	19	19	191	19 × 79	1054	5473
19	7	(H.4) non vérifiée						
23	6	A	23	—	47	—	6	1
23	17	(H.4) non vérifiée						

Poids 32: $f = \Delta . E_6^2 . E_4^2 + (20532 + 12\sqrt{d}) . \Delta^2 . E_4^2$ où $d = 18295489$								
ℓ	$\sqrt{d}$	TH.	$\Im$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	1	B	243	3	7	243 × 8	481	1008
3	2	B	2187	3	7	2187 × 5	4941	8212
5	3	A	125	—	11	—	10	21
5	2	A	25	—	11	—	19	12
7	3	A	343	—	29	—	112	213
7	4	B	7	7	29	7 × 17	281	44
11	6	A	11	—	23	—	9	2
11	5	(H.4) non vérifiée						
13	2	A	13	—	53	—	5	2
13	11	A	13	—	53	—	6	1
17	15	A	17	—	103	—	14	1
17	2	(H.4) non vérifiée						
19	16	A	19	—	191	—	12	1
19	3	(H.4) non vérifiée						
23	1	A	23	—	47	—	8	1
23	22	(H.4) non vérifiée						

Poids 34: $f=\Delta.E_6^3.E_4+(-59544+72\sqrt{d}).\Delta^2.E_6.E_4$ où $d=2356201$								
ℓ	$\sqrt{d}$	TH.	$\mathfrak{I}$	$\mathbf{T}^-$	p_*	x	$\varphi-M$	$\psi-N$
3	1	B	2187	9	7	2187 × 19	3429	114702
3	2	B	243	81	7	243 × 194	466077	596838
5	1	A	125	—	11	—	43	90
5	4	A	125	—	11	—	45	88
7	1	A	49	—	29	—	8	25
7	6	B	7	7	29	7 × 2	129	198
11	10	A	121	—	67	—	42	101
11	1	(H.4) non vérifiée						
13	4	A	13	—	53	—	7	2
13	9	A	13	—	53	—	8	1
17	1	(H.4) non vérifiée						
17	16	(H.4) non vérifiée						
19	7	A	19	—	191	—	14	1
19	12	(H.4) non vérifiée						
23	14	A	23	—	47	—	10	1
23	9	(H.4) non vérifiée						
29	26	A	29	—	59	—	4	1
29	3	(H.4) non vérifiée						

Poids 38: $f = \Delta.E_6^3.E_4^2 + (-96144 + 48\sqrt{d}).\Delta^2.E_6.E_4^2$ où $d = 63737521$								
ℓ	$\sqrt{d}$	TH.	$\Im$	T^-	p_*	x	$\varphi - M$	$\psi - N$
3	1	B	243	3	7	243 × 1	19	18
3	2	B	243	3	7	243 × 1	1395	100
5	1	A	125	—	11	—	65	72
5	4	A	125	—	11	—	82	55
7	6	A	49	—	29	—	10	27
7	1	B	49	7	29	49 × 1	1211	884
11	10	A	11	—	23	—	5	2
11	1	B	11	11	23	11 × 30	586	661
13	4	A	13	—	53	—	11	2
13	9	(H.4) non vérifiée						
17	13	A	17	—	103	—	4	1
17	4	(H.4) non vérifiée						
19	8	(H.4) non vérifiée						
19	11	(H.4) non vérifiée						
23	6	A	23	—	47	—	14	1
23	17	(H.4) non vérifiée						
29	4	A	29	—	59	—	8	1
29	25	(H.4) non vérifiée						
31	23	A	31	—	311	—	6	1
31	8	(H.4) non vérifiée						

Références

1. E. Papier, *Thèse de 3ème cycle*, Paris (1981).
2. E. Papier et K.A. Ribet, Eisenstein ideals and λ-adic representations, *Journal of the faculty of Science*, Univ. of Tokyo, Sec. IA Vol. 28, n° 3, February, 1982.
3. H.P.F. Swinnerton-Dyer, On ℓ-adic representations and congruences for coefficients of modular forms, *Lecture Notes in Math.* 350, Springer.
4. H.P.F. Swinnerton-Dyer, On ℓ-adic representations and congruences for coefficients of modular forms (II), *Lecture Notes in Math.* 601, Springer.